KURT F. READING
PAUL J. SOBEL | URTON L. ANDERSON
MICHAEL J. HEAD | SRIDHAR RAMAMOORTI
MARK SALAMASICK | CRIS RIDDLE

MANUEL D'AUDIT INTERNE

AMÉLIORER L'EFFICACITÉ DE LA GOUVERNANCE, DU CONTRÔLE INTERNE ET DU MANAGEMENT DES RISQUES



Copyright © 2015 Eyrolles.

ifaci
Institut français de l'audit et du contrôle internes
EYROLLES
The IIA Research Foundation

MANUEL D'AUDIT INTERNE

AMÉLIORER L'EFFICACITÉ DE LA GOUVERNANCE, DU CONTRÔLE INTERNE ET DU MANAGEMENT DES RISQUES

Le Manuel d'audit interne est l'ouvrage international de référence sur le métier d'auditeur interne. Élaboré sous l'égide de la fondation pour la recherche de l'IIA, il est le fruit de la collaboration de professeurs et de praticiens. Cette adaptation aux contextes européen et français réalisée par l'IFACI en fait un outil idéal pour les auditeurs internes, les étudiants en audit interne et leurs enseignants.

Ce manuel est organisé en deux sections, « Concepts fondamentaux de l'audit interne » et « Conduire une mission d'audit interne ». Il reflète les dernières évolutions de la profession, en particulier dans les domaines suivants :

- Normes internationales de l'audit interne
- Gouvernance, contrôle interne et gestion des risques
- Éléments clés liés aux systèmes d'information et références aux guides GTAG diffusés par l'IIA et l'IFACI
- Risques de fraude
- Valeur ajoutée de l'audit interne, notamment par des missions de conseil et des points de vue pertinents
- Coordination avec les autres prestataires internes et externes d'assurance

Les objectifs d'efficacité et d'amélioration de la valeur ajoutée fixés par les organisations ne peuvent être atteints sans les meilleures compétences, tout spécialement dans les métiers de l'audit. Cette adaptation française de la troisième édition du *Manuel* a pour objectif de contribuer efficacement à la professionnalisation des pratiques.

L'IFACI (www.ifaci.com) rassemble plus de 5 600 professionnels de l'audit et du contrôle internes. Il favorise la diffusion des meilleures pratiques professionnelles. Il est le partenaire privilégié des organisations publiques et privées de toutes tailles souhaitant améliorer l'efficacité de leurs dispositifs de gouvernance, de maîtrise des risques et de contrôle interne. L'IFACI est affilié à l'IIA (*The Institute of Internal Auditors*), qui bénéficie d'un réseau de 180 000 adhérents.

www.editions-eyrolles.com

Couverture : Studio Eyrolles
© Éditions Eyrolles/ Faceout Studio

Code éditeur : G56210
Code ISBN : 978-2-212-56210-1

Copyright © 2015 Eyrolles.

SOMMAIRE

SECTION 1 :
CONCEPTS FONDAMENTAUX DE L'AUDIT INTERNE

Chapitre 1 – Introduction à l'audit interne

Chapitre 2 – Le cadre de référence international des pratiques professionnelles : des lignes directrices incontournables pour l'audit interne

Chapitre 3 – La gouvernance

Chapitre 4 – La gestion des risques

Chapitre 5 – Les processus et les risques

Chapitre 6 – Le contrôle interne

Chapitre 7 – Les risques et les contrôles des systèmes d'information

Chapitre 8 – Les risques de fraude et d'actes illégaux

Chapitre 9 – La gestion de l'audit interne

Chapitre 10 – Les preuves d'audit et les papiers de travail

Chapitre 11 – L'échantillonnage en audit

SECTION 2 :
CONDUIRE UNE MISSON D'AUDIT INTERNE

Chapitre 12 – Introduction au processus d'audit

Chapitre 13 – Le déroulement de la mission d'assurance

Chapitre 14 – La communication des résultats d'une mission d'assurance et les procédures de suivi

Chapitre 15 – La mission de conseil

Copyright © 2015 Eyrolles.

CHEZ LE MÊME ÉDITEUR





Copyright © 2015 Eyrolles.

MANUEL D'AUDIT INTERNE

Copyright © 2015 Eyrolles.

Groupe Eyrolles
61, bd Saint-Germain
75240 Paris Cedex 05
www.editions-eyrolles.com

Copyright © 2013 by *Institute of Internal Auditors Research Foundation ("IIARF")* strictly reserved. No parts of this material may be reproduced in any form without the written permission of IIARF.

Permission has been obtained from the copyright holder, IIARF to publish this translation, which is the same in all material respects, as the original unless approved as changed. No parts of this document may be reproduced, stored in any retrieval system, or transmitted in any form, or by any means electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of IIARF.

3e édition

Copyright © 2013 par la Fondation pour la recherche de l'*Institute of Internal Auditors* (*Institute of Internal Auditors Research Foundation*, IIARF). Tous droits réservés.

Publié par la Fondation pour la recherche de l'*Institute of Internal Auditors*

247 Maitland Avenue

Altamonte Springs, Floride 32701-4201

Aucune partie de cette publication ne peut être reproduite, stockée dans un système de consultation ou transmise sous quelque forme que ce soit, ni par aucun moyen (électronique, mécanique, reprographie, enregistrement ou autre) sans autorisation écrite préalable de l'éditeur.

Limite de responsabilité : L'IIARF publie ce document à titre informatif et pédagogique. Cette publication entend donner des informations, mais ne se substitue en aucun cas à un conseil juridique ou comptable. L'IIARF ne fournit pas ce type de service et ne garantit, par la publication de ce document, aucun résultat juridique ou comptable. En cas de problèmes juridiques ou comptables, il convient de recourir à l'assistance de professionnels.

Le Cadre de référence international des pratiques professionnelles de l'audit interne (CRIPP) de l'*Institute of Internal Auditors* (IIA) comprend l'ensemble des lignes directrices existantes et émergentes destinées à la profession. Le CRIPP donne des lignes directrices aux auditeurs internes, et balise le développement de l'audit interne au plan international.

L'IIA et l'IIARF collaborent avec des chercheurs du monde entier, qui réalisent des études utiles sur les problématiques du monde des affaires. Une grande partie de leurs rapports finaux provient de recherches financées par l'IIARF, menées pour le compte de celle-ci et de la profession d'audit interne. Les opinions, les interprétations et les points de vue formulés sont le fruit d'un consensus parmi les chercheurs, et ne reflètent pas nécessairement ni ne représentent la position officielle ou les règles de l'IIA ou l'IIARF.

Copyright © 2015 Eyrolles.

En application de la loi du 11 mars 1957, il est interdit de reproduire intégralement ou partiellement le présent ouvrage, sur quelque support que ce soit, sans autorisation de l'éditeur ou du Centre français d'exploitation du droit de copie, 20, rue des Grands-Augustins, 75006 Paris.

© Groupe Eyrolles, 2015
ISBN : 978-2-212-56210-1



MANUEL D'AUDIT INTERNE

Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques

Kurt F. Reding, PhD, CIA, CPA, CMA
Paul J. Sobel, CIA, CRMA
Urton L. Anderson, PhD, CIA, CFSA, CCEP
Michael J. Head, CIA, CPA, CISA, CMA
Sridhar Ramamoorti, PhD, CIA, CFSA, CGAP, CRMA
Mark Salamasick, CIA, CISA, CRMA, CSP
Cris Riddle, MA, CIA, CRMA

Commandité en partie par
The Institute of Internal Auditors Chicago Chapter

Copyright © 2015 Eyrolles.

The IIA Research Foundation

EYROLLES

ifaci
institut français de l'audit et du contrôle internes

Copyright © 2015 Eyrolles.

SOMMAIRE

Préambule ..... **XV**

Préface ..... **XVII**

Remerciements ..... **XXI**

À propos des auteurs ..... **XXIII**

SECTION 1 : CONCEPTS FONDAMENTAUX DE L'AUDIT INTERNE



CHAPITRE 1

INTRODUCTION À L'AUDIT INTERNE

Définition de l'audit interne 1-3

Relation entre l'audit et la comptabilité 1-10

Activités d'assurance menées dans le cadre des audits financiers 1-10

La profession d'audit interne 1-12

L'institut des auditeurs internes 1-16

Compétences nécessaires pour exceller dans l'audit interne 1-20

Les carrières dans l'audit interne 1-25

Résumé 1-27

Questions de révision 1-28

Questions à choix multiples 1-30

Thèmes de discussion 1-32

Études de cas 1-33



CHAPITRE 2

LE CADRE DE RÉFÉRENCE INTERNATIONAL DES PRATIQUES PROFESSIONNELLES : DES LIGNES DIRECTRICES INCONTOURNABLES POUR L'AUDIT INTERNE

Historique des lignes directrices à l'intention des professionnels de l'audit interne 2-2

Le cadre de référence international des pratiques professionnelles 2-5

Copyright © 2015 Eyrolles.

SOMMAIRE

Dispositions obligatoires 2-7

Dispositions fortement recommandées 2-32

Actualisation du cadre de référence international des pratiques professionnelles 2-36

Normes publiées par d'autres organisations 2-41

Résumé 2-45

Questions de révision 2-46

Questions à choix multiples 2-48

Thèmes de discussion 2-51

Études de cas 2-53



CHAPITRE 3

LA GOUVERNANCE

Concepts liés à la gouvernance 3-3

L'évolution de la gouvernance 3-20

Opportunités pour un point de vue de l'audit interne .. 3-20

Résumé 3-22

Annexes 3-24

Questions de révision 3-30

Questions à choix multiples 3-32

Thèmes de discussion 3-33

Études de cas 3-35



CHAPITRE 4

LA GESTION DES RISQUES

Présentation de la gestion des risques 4-3

Le cadre de référence relatif au management des risques de l'entreprise élaboré par le COSO 4-5

Norme ISO 31000:2009, management du risque – Principes et lignes directrices 4-20

Le rôle de l'audit interne dans le management des risques de l'entreprise 4-24

Copyright © 2015 Eyrolles.

SOMMAIRE

Impact du management des risques de l'entreprise sur l'assurance apportée par l'audit interne 4-28

Opportunités pour un point de vue de l'audit interne 4-30

Résumé 4-30

Questions de révision 4-32

Questions à choix multiples 4-34

Thèmes de discussion 4-37

Études de cas 4-39



CHAPITRE 5

LES PROCESSUS ET LES RISQUES

Les processus opérationnels 5-2

Description écrite des processus opérationnels 5-10

Risques opérationnels 5-11

Externalisation de processus opérationnels 5-26

Opportunités pour un point de vue de l'audit interne 5-29

Résumé 5-30

Annexe 5-31

Questions de révision 5-35

Questions à choix multiples 5-36

Thèmes de discussion 5-39

Études de cas 5-40



CHAPITRE 6

LE CONTRÔLE INTERNE

Cadres de référence 6-2

Définition du contrôle interne 6-9

Les objectifs, les composantes et les principes du contrôle interne 6-10

Rôles et responsabilités en matière de contrôle interne 6-23

Limites du contrôle interne 6-26

Copyright © 2015 Eyrolles.

SOMMAIRE

Les différentes approches du contrôle interne 6-30
Typologie des contrôles 6-32
Évaluation du système de contrôle interne – Présentation 6-37
Opportunités pour un point de vue de l'audit interne .. 6-39
Résumé 6-39
Questions de révision 6-41
Questions à choix multiples 6-43
Thèmes de discussion 6-46
Étude de cas 6-47



CHAPITRE 7

LES RISQUES ET LES CONTRÔLES DES SYSTÈMES D'INFORMATION

Principales composantes des systèmes d'information 7-5
Opportunités et risques SI 7-10
Gouvernance des SI 7-14
La gestion des risques SI 7-15
Contrôles des SI 7-18
Conséquences des SI pour les auditeurs internes 7-25
Principales sources de lignes directrices relatives à l'audit des SI 7-30
Opportunités pour un point de vue de l'audit interne .. 7-32
Résumé 7-32
Questions de révision 7-35
Questions à choix multiples 7-37
Thèmes de discussion 7-39
Étude de cas 7-42

Copyright © 2015 Eyrolles.

SOMMAIRE



CHAPITRE 8

LES RISQUES DE FRAUDE ET D'ACTES ILLÉGAUX

La fraude dans les organisations aujourd'hui 8-2

Définitions de la fraude 8-7

Le triangle de la fraude 8-12

Les grands principes de la gestion du risque de fraude 8-14

La gouvernance du programme de gestion du risque de fraude 8-19

Évaluation des risques de fraude 8-23

Traitement des actes illégaux 8-29

Prévention de la fraude 8-31

Détection de la fraude 8-35

Enquêtes et actions correctives 8-37

Comprendre les fraudeurs 8-40

Conséquences pour les auditeurs internes et d'autres collaborateurs 8-42

Opportunités pour un point de vue de l'audit interne .. 8-48

Résumé 8-48

Questions de révision 8-50

Questions à choix multiples 8-52

Thèmes de discussion 8-55

Études de cas 8-57



CHAPITRE 9

LA GESTION DE L'AUDIT INTERNE

Quelle place pour l'audit interne au sein de l'organisation ? 9-3

Planification 9-9

Communication et approbation 9-11

Gestion des ressources 9-12

Règles et procédures 9-17

Copyright © 2015 Eyrolles.

SOMMAIRE

Coordination des travaux d'assurance 9-18
Rapports au conseil et à la direction générale 9-21
La gouvernance 9-23
La gestion des risques 9-25
Contrôle 9-28
Assurance qualité et programmes d'amélioration 9-29
Les indicateurs de performance pour l'audit interne 9-34
La place de la technologie dans le processus d'audit interne 9-35
Opportunités pour un point de vue de l'audit interne 9-39
Résumé 9-39
Questions de révision 9-40
Questions à choix multiples 9-42
Thèmes de discussion 9-45
Étude de cas 9-46



CHAPITRE 10

LES PREUVES D'AUDIT ET LES PAPIERS DE TRAVAIL

Preuves d'audit 10-1
Les procédures d'audit 10-5
Papiers de travail 10-17
Résumé 10-21
Questions de révision 10-22
Questions à choix multiples 10-24
Thèmes de discussion 10-27



CHAPITRE 11

L'ÉCHANTILLONNAGE EN AUDIT

Introduction à l'échantillonnage en audit 11-2
Échantillonnage statistique dans les tests des contrôles 11-5

Copyright © 2015 Eyrolles.

SOMMAIRE

Échantillonnage non statistique dans les tests des contrôles 11-18

Échantillonnage statistique dans l'échantillonnage par unités monétaires 11-21

Résumé 11-24

Questions de révision 11-27

Questions à choix multiples 11-28

Thèmes de discussion 11-31

Étude de cas 11-33

SECTION 2 : CONDUIRE UNE MISSON D'AUDIT INTERNE



CHAPITRE 12 INTRODUCTION AU PROCESSUS D'AUDIT

Catégories de missions d'audit interne 12-3

Présentation du déroulement de la mission d'assurance 12-5

Le déroulement de la mission de conseil 12-15

Résumé 12-16

Questions de révision 12-17

Questions à choix multiples 12-18

Thèmes de discussion 12-21

Étude de cas 12-23



CHAPITRE 13 LE DÉROULEMENT DE LA MISSION D'ASSURANCE

Déterminer les objectifs et le périmètre de la mission ... 13-4

Comprendre l'audité 13-10

Repérer et évaluer les risques 13-27

Identifier les contrôles clés 13-35

Évaluer l'adéquation de la conception des contrôles . 13-37

Établir un plan des tests 13-39

Copyright © 2015 Eyrolles.

SOMMAIRE

Élaborer un programme de travail 13-42
Allouer des ressources à la mission 13-45
Réaliser des tests pour collecter des preuves 13-48
Évaluer les preuves rassemblées et en tirer des conclusions 13-50
Faire des observations et formuler des recommandations 13-53
Opportunités pour un point de vue de l'audit interne 13-57
Résumé 13-57
Questions de révision 13-61
Questions à choix multiples 13-63
Thèmes de discussion 13-66
Étude de cas 13-69



CHAPITRE 14

LA COMMUNICATION DES RÉSULTATS D'UNE MISSION D'ASSURANCE ET LES PROCÉDURES DE SUIVI

L'obligation de communication des résultats d'une mission 14-3
Processus d'évaluation des observations et de remontée de l'information 14-6
Procéder à des communications intermédiaires et préliminaires 14-18
Rédiger le rapport définitif de la mission 14-20
Diffusion des communications finales formelles et informelles 14-27
Surveillance et suivi 14-32
Autres types de missions 14-34
Résumé 14-35
Questions de révision 14-37
Questions à choix multiples 14-38
Thèmes de discussion 14-41
Études de cas 14-44

Copyright © 2015 Eyrolles.

SOMMAIRE



CHAPITRE 15

LA MISSION DE CONSEIL

Apporter un point de vue dans le cadre de missions de conseil 15-5

Différenciation entre les activités d'assurance et de conseil 15-6

Types d'activités de conseil 15-9

Sélectionner les missions de conseil à réaliser 15-12

Le déroulement de la mission de conseil 15-16

Papiers de travail d'une mission de conseil 15-25

Évolution de l'environnement des activités de conseil 15-26

Capacités nécessaires 15-27

Opportunités pour un point de vue de l'audit interne 15-29

Résumé 15-30

Questions de révision 15-31

Questions à choix multiples 15-32

Thèmes de discussion 15-34

Études de cas 15-35

Références **1**

Glossaire **9**

Annexes **23**

ANNEXE A
Code de Déontologie de l'***Institute of Internal Auditors*** ***23***

ANNEXE B
Normes internationales pour la pratique professionnelle de l'audit interne ***25***

Index **45**

Copyright © 2015 Eyrolles.

Copyright © 2015 Eyrolles.

PRÉAMBULE

Les objectifs d'efficacité et d'amélioration de la valeur ajoutée, fixés par les organisations ne peuvent être atteints sans les meilleures compétences, tout spécialement dans nos métiers.

La professionnalisation des acteurs de l'audit et du contrôle internes est l'une des raisons d'être de l'IFACI. C'est donc tout naturellement que, lorsque la fondation pour la recherche de l'IIA a décidé de réunir un groupe d'experts pour mettre à jour ce manuel d'audit interne, l'IFACI a immédiatement souhaité l'adapter aux contextes européen et francophone, avec le concours de professionnels et d'universitaires.

Je suis convaincu que cet ouvrage didactique, comportant de nombreux exemples d'application et illustrations, permettra aux étudiants et aux professionnels d'appréhender plus précisément le monde passionnant mais complexe et exigeant de l'audit interne.

Farid ARACTINGI
Président de l'IFACI

Copyright © 2015 Eyrolles.

Copyright © 2015 Eyrolles.

PRÉFACE

Nous sommes heureux de vous présenter la 3e édition de ce manuel auquel d'importantes modifications ont été apportées. Certaines d'entre elles résultent de l'actualisation d'ouvrages de référence pour la profession, tels que le Cadre de référence international des pratiques professionnelles de l'audit interne de l'IIA (*The Institute of Internal Auditors*) et le « Référentiel intégré de contrôle interne – Principes de mise en œuvre et de pilotage » du COSO (*Committee of Sponsoring Organizations of the Treadway Commission*).

Comme dans les éditions précédentes, les auteurs apportent aux étudiants les connaissances fondamentales et un aperçu des compétences qui leur seront nécessaires pour réussir en tant que professionnels de l'audit interne débutants. Ce manuel est principalement destiné aux étudiants de premier et deuxième cycles qui suivent des cours d'initiation à l'audit interne. Nous sommes néanmoins persuadés que cette édition constituera également un outil de formation et de référence pour les professionnels de l'audit interne.

PRINCIPALES MODIFICATIONS DE LA 3E ÉDITION

Cette 3e édition du Manuel de l'audit interne comporte d'importantes modifications :

- Le chapitre 1, *Introduction à l'audit interne*, présente la proposition de valeur de l'audit interne et notamment l'opportunité qu'ont les fonctions d'audit interne de créer de la valeur ajoutée pour leur organisation en donnant leur point de vue (*Insight*). Tout au long du manuel, ce concept est développé à travers des encadrés sur les points de vue liés aux sujets traités dans les chapitres en question.
- Le chapitre 2, *Le cadre de référence international des pratiques professionnelles : des lignes directrices incontournables pour l'audit interne*, comprend désormais une analyse de la relation entre la proposition de valeur et le CRIPP. Ce chapitre a également été actualisé pour refléter la procédure actuelle de mise à jour des lignes directrices professionnelles, y compris les comités impliqués et le processus de sélection, de rédaction, de publication et de révision de ces mises à jour.
- Le chapitre 3, *La gouvernance*, introduit le modèle des trois lignes de maîtrise. Il donne des lignes directrices sur la manière dont ce modèle peut être utilisé pour comprendre les différents niveaux d'assurance donnée au sein d'une organisation, et pour les structurer efficacement, en vue de contribuer à une gouvernance solide.
- Le chapitre 4, *La gestion des risques*, comprend désormais une analyse de la norme ISO 31000:2009, *Management du risque – principes et lignes directrices* (norme ISO 31000).
- Le chapitre 6, *Le contrôle interne*, a été révisé pour refléter l'actualisation du nouveau « Référentiel intégré de contrôle interne – Principes de mise en œuvre et de pilotage » du COSO.
- Le chapitre 7, *Les risques et les contrôles des systèmes d'information*, couvre désormais les évolutions liées aux réseaux sociaux, au Big Data, au *cloud computing* et au BYOD (*Bring Your Own Device* ou AVOP) : « Prenez vos appareils personnels ». Ce chapitre

Copyright © 2015 Eyrolles.

présente également les nouveaux Guides pratiques d'audit des technologies de l'information (GTAG) du CRIPP, ainsi que le COBIT® 5 récemment publié par l'ISACA.

- Le chapitre 8, auparavant intitulé *Risques de fraude et contrôles*, est désormais intitulé *Les risques de fraude et d'actes illégaux*. Ce chapitre analyse la distinction entre la fraude et les actes illégaux, ainsi que les risques et les modalités de traitement associées à chacun de ces risques.
- Le chapitre 9, *La gestion de l'audit interne*, poursuit l'analyse de la coordination des services d'assurance initiée dans le chapitre 3, au regard de la gestion de la fonction d'audit interne.
- Le chapitre 15, *La mission de conseil*, examine la proposition de valeur de l'audit interne en mettant l'accent sur les points de vue que la fonction peut apporter dans le cadre de missions de conseil.
- Les questions de révision ont été approfondies afin de couvrir plus en détail les concepts majeurs traités dans chaque chapitre, y compris les nouveautés. Des questions à choix multiples et des thèmes de discussion supplémentaires ont été ajoutés dans certains chapitres.

CONTENU ET STRUCTURE DU MANUEL

Le manuel comprend toujours les éléments clés suivants :

- développement des processus de gouvernance d'entreprise, de management des risques et de contrôle interne ;
- approche d'audit interne fondée sur les risques et axée sur les processus et les contrôles ;
- intégration des risques et des contrôles liés aux SI et à la fraude ;
- alignement avec le CRIPP et la préparation pour la certification CIA (*Certified Internal Auditor*) ;
- rappel de termes clés en marge de chaque chapitre afin de renforcer les principaux concepts.

Les chapitres 1 à 11, constituant la section « Concepts fondamentaux de l'audit interne », couvrent des thèmes que tous les auditeurs doivent connaître et comprendre. Les chapitres 12 à 15 de la section « Conduire une mission d'audit interne » portent sur les phases de planification, d'exécution et de communication des missions d'assurance et de conseil.

Chaque fin de chapitre inclut des questions de révision, des questions à choix multiple, des thèmes de discussion, des études de cas à réaliser. Les questions et les études de cas sont le fruit du travail des auteurs, sauf indication contraire, ou ont été adaptées à partir des modèles d'examen pour la certification CIA*.

* Modèles d'examen publiés par l'IIA en 1998 puis en 2004.

Copyright © 2015 Eyrolles.

Le glossaire contient les définitions des termes clés employés dans l'ensemble du manuel. Le Code de déontologie et les *Normes* de l'IIA sont respectivement joints en Annexe A et en Annexe B.

OUTILS ADDITIONNELS

Les outils additionnels suivants sont mis à la disposition des enseignants en version originale, sur demande formulée par courrier électronique (iiatextbook@theiia.org).

- **Manuel de réponses.** Le manuel de réponses, rédigé par les auteurs du manuel, contient les réponses aux questions et aux études de cas figurant à chaque fin de chapitre.
- **Encadrés.** Chacun des encadrés présentés dans le manuel a été reproduit à l'intention des enseignants qui souhaitent s'en servir comme supports visuels et/ou polycopiés.
- **Modèles.** Des modèles ont été élaborés pour chaque chapitre. Les enseignants peuvent s'en servir comme point de départ pour préparer leurs propres présentations.
- **Exemples de sujets d'examen.** Les auteurs ont rédigé des exemples de sujets d'examen afin de donner aux enseignants une base pour préparer les sujets les plus appropriés pour leurs cours.
- **Projet d'audit interne.** Urton Anderson et Mark Salamasick expliquent comment ils ont réussi à intégrer des projets d'audit interne concrets à leur programme de formation *Internal Auditing Education Partnership* (IAEP).

Copyright © 2015 Eyrolles.

Copyright © 2015 Eyrolles.

REMERCIEMENTS

Nous souhaitons remercier les organisations et les personnes suivantes pour les contributions qu'elles ont apportées au présent manuel.

Pour la version originale en anglais (États-Unis).

Les auteurs remercient les organisations et les personnes qui ont utilisé les éditions précédentes de ce manuel, notamment les enseignants et leurs étudiants.

Ils remercient tout particulièrement Jeffrey E. Perkins, CIA, CRMA, CPA, CISSP, CISA, CISM, Vice President, Internal Audit, TransUnion Corp. En sa qualité de membre du Conseil d'administration de la Fondation pour la recherche de l'IIA et de *Trustee Champion* du manuel, Jeff a revu de manière approfondie chacun des chapitres actualisés de cette 3e édition. Il a formulé des observations pertinentes qui nous ont permis de produire un manuel de qualité qui, selon nous, sera utile pour les étudiants.

- La Fondation pour la recherche de l'IIA, pour avoir financé la rédaction du manuel original.
- L'IIA, pour avoir donné l'autorisation d'y inclure le Cadre de référence international des pratiques professionnelles de l'audit interne et d'autres instruments, notamment les questions issues des modèles d'examen pour la certification CIA (*Certified Internal Auditor*) et des anciens examens CIA.
- ACL Services Ltd., pour avoir contribué à l'élaboration de la version pédagogique du logiciel d'audit ACL contenu dans le DVD-ROM joint à la version originale du manuel.
- Audimation Services Inc., pour avoir contribué à l'élaboration du logiciel d'audit IDEA contenu dans le DVD-ROM joint à la version originale du manuel.
- Michael Gowell, General Manager et Vice President CCH® TeamMate, pour avoir permis d'offrir une expérience pratique du logiciel TeamMate aux étudiants qui utilisent ce manuel.
- Dan W. Youse, CPA, CITP, CFP, Vice President, Operations, Wolters Kluwer, pour avoir contribué, au nom de Wolters Kluwer, à l'élaboration du logiciel TeamMate contenu dans le DVD-ROM joint à la version originale du manuel.
- Melissa Ewing et Karen Peary, Wolters Kluwer, pour avoir élaboré les études de cas et les exercices TeamMate contenus dans le manuel et dans le DVD-ROM joint à la version originale du manuel.
- Patrick Rodriguez et David Carr, Wolters Kluwer, pour avoir créé et fourni les vidéos de démonstration TeamMate contenues dans le DVD-ROM joint à la version originale du manuel.
- The Institute of Internal Auditors (Royaume-Uni et Irlande), The IT Governance Institute, The Committee of Sponsoring Organizations of the Treadway Commission (COSO), The American Institute of Certified Public Accountants (AICPA), et l'Université du Texas à Austin, pour avoir permis de copier et/ou d'adapter des informations exclusives.

Copyright © 2015 Eyrolles.

REMERCIEMENTS

- Lillian McAnally, *Content Development Manager*, Fondation pour la recherche de l'IIA, pour avoir coordonné et dirigé le projet, et pour avoir géré le processus de fabrication final de l'ouvrage.
- Lee Ann Campbell, Senior Publications Editor, Fondation pour la recherche de l'IIA, pour avoir révisé l'intégralité du manuel, y compris les études de cas supplémentaires contenues dans le DVD-ROM joint à la version originale du manuel.
- Faceout Studio, pour avoir conçu la couverture du manuel.
- Rule & Renco, pour avoir géré tous les aspects relatifs à la conception intérieure et à la composition du manuel.

Pour la traduction française et son adaptation francophone.

- **Louis Vaurs**, Président d'honneur de l'IFACI, pour avoir coordonné le projet d'adaptation.
- **Béatrice Bon-Michel** (professeur, CNAM), **Vianney Dumont** (directeur de l'audit interne, MAIF), **Sébastien Lepers** (commissaire principal, Ministère de la défense), **Jacques Renard** (consultant en management et audit interne) pour avoir adapté l'ouvrage original aux contextes européen et francophone, mais aussi activement participé à la révision de l'ensemble de l'ouvrage.
- **Béatrice Ki-Zerbo**, IFACI, pour avoir assuré l'homogénéité de la rédaction et la relecture finale de l'ouvrage.
- **Julie Ferré,** IFACI, pour avoir assuré le suivi de la relation avec l'éditeur.
- **Philippe Mocquard,** IFACI, pour avoir révisé le manuel dans son ensemble.

Copyright © 2015 Eyrolles.

À PROPOS DES AUTEURS

Kurt F. Reding, PhD, CIA, CPA, CMA
Grant Thornton *Faculty Fellow*
Clinical Assistant Professor of Accounting
W. Frank Barton School of Business
Université de Wichita

Kurt a été membre du Conseil d'administration de l'IIA, ainsi que du *North American Board*, du *Board of Research and Education Advisors*, et de l'*Academic Relations Committee*. Il a également été membre du *Board of Governors* du Chapitre de Wichita de l'IIA, et membre de droit du *Board of Governors* du Chapitre de Kansas City de l'IIA. Il intervient régulièrement lors de conférences et de séminaires organisés par l'IIA.

En 2003, il a reçu le prix Leon R. Radde de l'IIA, qui récompense le meilleur formateur de l'année (*Leon R. Radde Educator of the Year Award*). Il a en outre reçu, pour ses écrits, le prix John B. Thurston de l'IIA, ainsi que la *Lybrand Gold Medal* de l'*Institute of Management Accountants*, les deux récompenses les plus prestigieuses décernées chaque année par ces organisations. Il est coauteur de deux autres ouvrages publiés par l'IIA : *Enterprise Risk Management: Achieving and Sustaining Success* et *Introduction to Auditing: Logic, Principles, and Techniques*. Il a publié plusieurs articles dans les revues *Internal Auditor*, *Internal Auditing*, *Managerial Auditing Journal*, *Management Accounting Quarterly*, *Strategic Finance*, et bien d'autres.

Kurt a plus de 25 ans d'expérience en tant que professionnel de l'audit et formateur. Il est titulaire d'un PhD en comptabilité de l'Université du Tennessee. Il est membre de l'*Institute of Internal Auditors*, l'*American Institute of Certified Public Accountants*, l'*Institute of Management Accountants*, et l'*American Accounting Association*.

Paul J. Sobel, CIA, CRMA
Vice President, Chief Audit Executive
Georgia-Pacific LLC

Paul est vice-président et responsable de l'audit interne chez Georgia-Pacific, LLC, une entreprise privée du secteur des biens de consommation et produits forestiers située à Atlanta (Géorgie). Auparavant, il était responsable de l'audit interne pour trois entreprises publiques : Mirant Corporation, une entreprise du secteur de l'énergie située à Atlanta (Géorgie) ; Aquila, Inc., une entreprise du secteur de l'énergie située à Kansas City (Missouri) ; et les activités d'édition d'Harcourt General à Orlando (Floride). Au sein de ces entreprises, il dirigeait les activités d'audit interne sur le plan mondial et fournissait des services de conseil concernant les programmes de gestion des risques, de conformité et de contrôle interne. Il a également été *Audit Manager* chez PepsiCo, *Senior Manager* de l'activité *Business Risk Consulting* et *Experienced Manager* de l'activité *Financial Statement Assurance* chez Arthur Andersen.

Copyright © 2015 Eyrolles.

À PROPOS DES AUTEURS

Paul intervient régulièrement sur les thèmes de la gouvernance, de la gestion des risques et de l'audit interne. Il a publié un ouvrage intitulé *Auditor's Risk Management Guide: Integrating Auditing and ERM*. Il est par ailleurs coauteur des deux premières éditions du manuel commandité par l'IIARF, intitulé *Internal Auditing: Assurance and Consulting Services*. Son troisième ouvrage, intitulé *Enterprise Risk Management : Achieving and Sustaining Success*, a été publié en août 2012. Il est enfin reconnu pour ses articles publiés dans les revues *Internal Auditor* et *Management Accounting Quarterly*.

Paul est aujourd'hui membre du Conseil d'administration de l'IIA. Il a été Président du Conseil de juillet 2013 à juillet 2014. Par le passé, il a occupé la fonction de vice-président à plusieurs reprises, et a également agi en qualité de président de l'IIARF. En 2010, il a été *Program Chair* de la Conférence internationale de l'IIA qui s'est déroulée à Atlanta, un rôle qu'il a tenu de nouveau en 2013 dans le cadre de la Conférence internationale qui a eu lieu à Orlando. En 2012, Paul figurait parmi les *100 personnalités les plus influentes dans le domaine financier*, dont la liste a été publiée dans la revue *Treasury & Risk*. Il a également été membre du *Standing Advisory Group* du PCAOB, et représentant de l'IIA auprès de la *Pathways Commission*, qui a élaboré des recommandations pour améliorer l'avenir des formations comptables aux États-Unis.

Copyright © 2015 Eyrolles.

À PROPOS DES AUTEURS

Urton L. Anderson, PhD, CIA, CCSA, CGAP, CFSA, CCEP
Clark W. Thompson, Jr., *Professor in Accounting Education*
Chair, Department of Accounting
McCombs School of Business
Université du Texas à Austin

Urton a rejoint le département de comptabilité en 1984. À McCombs, il a été directeur du département et vice-doyen du premier cycle. Urton a obtenu son PhD à l'Université du Minnesota en 1985. Ses recherches couvraient diverses problématiques d'audit interne et externe, notamment la gouvernance d'entreprise, la conformité, la gestion des risques d'entreprise et le contrôle interne. Il est auteur de quatre ouvrages, dont plusieurs ont été traduits en français, en espagnol, en chinois et en japonais. Urton est particulièrement engagé dans les activités de l'*Institute of Internal Auditors* (IIA). Il a été membre et Président du *Board of Regents* de l'IIA, et Président de l'*Internal Auditing Standards Board* à deux reprises (2002-2003 et 2007-2010). En 1997, il a reçu le prix Leon R. Radde de l'IIA, qui récompense le meilleur formateur de l'année (*Leon R. Radde Educator of the Year*). En reconnaissance de ses contributions exceptionnelles dans le domaine de l'audit interne, l'IIA lui a décerné le prix *Bradford Cadmus Memorial* en juin 2006. Il est actuellement Président du *Committee of Research and Education Advisors* de l'IIA et membre du Conseil d'administration de la Fondation pour la recherche de l'IIA (*IIA Research Foundation*, IIARF). Urton est membre du Conseil d'administration de l'*Health Care Compliance Association* et de l'*Advisory Board* de la *Society of Corporate Compliance and Ethics*. Entre 2011 et 2012, Urton a occupé la fonction d'*Academic Fellow* au sein de l'*Office of the Chief Accountant* de la *Securities and Exchange Commission* aux États-Unis.

Copyright © 2015 Eyrolles.

À PROPOS DES AUTEURS

Michael J. Head, CIA, CPA, CMA, CBA, CISA
Managing Director of Corporate Audit
TD Ameritrade

Mike est responsable de la coordination et de la prestation des services de revue, d'assurance et de conseil fondés sur les risques et axés sur les processus au sein de TD Ameritrade. Au cours de ses 33 ans de carrière, il a occupé diverses fonctions, parmi lesquelles celles de directeur de l'audit interne, de manager de l'audit et de contrôleur de gestion, auprès d'entreprises telles que PricewaterhouseCoopers, KPMG, The Guarantee Life Companies Inc., Bank of America (anciennement NationsBank), FirsTier Financial, Inc., et Standard Havens, Inc. Il possède une expérience dans le développement et la mise en place de fonctions d'audit interne, fondées sur les risques, et d'activités de conseil liées aux contrôles stratégiques, financiers, opérationnels et de conformité, destinées au secteur des services financiers.

Outre ses nombreux titres professionnels – *Certified Internal Auditor, Certified Public Accountant, Certified Management Accountant, Chartered Bank Auditor, et Certified Information Systems Auditor* – Mike est *General Securities Representative* (séries 7), *General Securities Principal* (séries 24), et *Financial and Operations Principal* (séries 27) de la FINRA. Il est membre actif de l'IIA et occupe actuellement la fonction de Président du *North American Advocacy Committee*. Il a également été nommé membre de *l'Investor Advisory Group* (IAG) du *Public Accounting Oversight Board* (PCAOB). Par le passé, Mike a occupé la fonction de Vice-président, en charge de la finance, du Comité exécutif du Conseil international de l'IIA. Il a par ailleurs été membre et Président du Comité d'audit du Conseil international de l'IIA. Il a également été membre du Conseil d'administration de l'IIARF, membre du *North American Board* et *District Advisor* pour la région centre-ouest. Mike est coauteur de l'article *Blended Engagements*, publié dans la revue *Internal Auditor*, qui a valu aux auteurs le prix de contributeur exceptionnel (*Outstanding Contributor Award*) en 2010. Mike, titulaire du BSBA de l'Université du Missouri-Columbia, est également membre de l'American Institute of Certified Public Accountants, de la *Society of CPAs du Nebraska*, de la *Society of CPAs du Missouri*, de *l'Information Systems Audit & Control Association*, et de *l'Institute of Management Accountants*.

Mike a récemment intégré le *College of Business de l'Université Creighton* en qualité d'enseignant suppléant au sein du département de la comptabilité. Il enseigne l'initiation à la comptabilité.

Copyright © 2015 Eyrolles.

À PROPOS DES AUTEURS

Sridhar Ramamoorti, PhD, ACA, CIA, CPA, CFE, CFF, CFFA, CFSA, CGAP, CGFM, CGMA, CITP, CRMA

***Associate Professor*, School of Accountancy**

***Director, Board Culture & Behavioral Dynamics, Center for Corporate Governance*, Michael J. Coles College of Business, Université de Kennesaw, Géorgie**

Sri a rejoint la *School of Accountancy* de l'Université de Kennesaw en 2010. Ses domaines de recherche et d'enseignement couvrent la gouvernance d'entreprise, la gestion des risques, l'audit interne et externe, la comptabilité internationale, la comptabilité judiciaire et l'évaluation d'entreprises.

Auparavant, Sri était responsable d'*Infogix Advisory Services*, une division d'Infogix, Inc. axée sur la gouvernance, les risques et les contrôles. Avant cela, il était associé en charge de la gouvernance d'entreprise chez Grant Thornton, au siège social à Chicago (Illinois). Il était l'un des principaux membres de l'équipe de rédaction et d'élaboration de l'ouvrage du COSO intitulé *Guidance on Monitoring Internal Control Systems*, publié en 2009. Avant de rejoindre Grant Thornton, Sri était consultant, expert de la loi Sarbanes-Oxley (*Sarbanes-Oxley Advisor*), dans le cadre des activités de conseil d'Ernst & Young en Amérique du Nord (*National Advisory Practices*). En tant que membre du département *Fraud Investigation & Dispute Services* d'Ernst & Young, il a organisé des sessions de sensibilisation au problème de la fraude pour plus de 1 000 associés et responsables d'audit aux États-Unis. Au début de sa carrière, Sri occupait une fonction de responsable au sein du *Professional Standards Group* chez Arthur Andersen. Il coordonnait les réponses de l'entreprise aux propositions de normes d'audit en matière de reporting financier frauduleux. Par ailleurs, il auditait les instruments dérivés et agissait en qualité d'intermédiaire clé dans le cadre des recherches menées en collaboration par Andersen et le MIT (à hauteur de 10 millions de dollars).

Sri est titulaire du BCom (*Bachelor of Commerce*) de l'Université de Bombay (Inde), ainsi que du MAcc et du PhD de l'Université de l'Ohio. Après avoir obtenu son PhD, Sri a rejoint le département de la comptabilité de l'Université de l'Illinois à Urbana-Champaign. Auteur de plus de 25 articles professionnels et de recherche, il a largement contribué aux travaux dans les domaines de la gouvernance, des risques et des contrôles. Il travaille actuellement sur son dixième ouvrage, intitulé *Behavioral Forensics : Bringing Freud to Fraud*. Parmi ses monographies, financées par l'IIA, figurent : *Research Opportunities in Internal Auditing*, *Using Neural Networks for Risk Assessment in Internal Auditing*, *Behavioral Dimensions of Internal Auditing*, et *CAE Strategic Relationships: Building Rapport with the Executive Suite*.

Sri a agi en qualité de Président bénévole de l'*Academy for Government Accountability*, membre du Conseil d'administration de l'IIARF et co-président dans le cadre de l'enquête 2010 du *Global Common Body of Knowledge* (CBOK) de l'IIARF. Il est aujourd'hui membre du *Global Ethics Committee* de l'IIA. Au cours des dix dernières années, il a effectué des présentations professionnelles aux États-Unis, au Brésil, au Canada, en France, en Inde, au Japon, en Malaisie, au Qatar, en Afrique du Sud, en Espagne, aux Pays-Bas, en Turquie et aux Émirats arabes unis.

Copyright © 2015 Eyrolles.

À PROPOS DES AUTEURS

Mark Salamasick, CIA, CISA, CRMA, CSP
Director of the *Center for Internal Auditing Excellence*
Université du Texas, Dallas

Mark est actuellement Directeur du *Center for Internal Auditing Excellence* de l'Université du Texas (Dallas), l'un des six programmes d'audit interne les plus importants au monde. Ce programme particulièrement complet a débuté à l'automne 2003 et couvre les domaines suivants : audit interne, technologie, logiciels d'audit, sécurité de l'information, gouvernance d'entreprise et comptabilité judiciaire. Il dispense des cours sur l'audit interne, l'audit des systèmes d'information, la gestion des risques et l'audit avancé.

Son dernier ouvrage, intitulé *Auditing Outsourced Functions : Risk Management in an Outsourced World*, a été publié par l'IIA en octobre 2012. Il a été directeur de recherche dans le cadre d'un projet mené conjointement avec l'IIARF et Intel, qui a donné lieu à un rapport intitulé *PC Management Best Practices*, et dans le cadre d'une autre publication, intitulée *Auditing Vendor Relationships*. Ces deux écrits ont été publiés en 2003. Auparavant, il a travaillé au sein de Bank of America pendant plus de 20 ans. Il est resté membre de la direction d'audit interne Groupe pendant 18 ans, en qualité de *Senior Vice President* et de *Director of Information Technology Audit*. Il était alors responsable de plusieurs audits des systèmes d'information, financiers et opérationnels. Il était chargé des partenariats et de l'audit dans les domaines de la technologie, de la sécurité de l'information et de la continuité d'activité. Avant de rejoindre Bank of America, Mark était *Senior consultant* chez Accenture (Andersen Consulting).

Il est aujourd'hui membre du Conseil d'administration de l'IIARF, et membre du *Board of Research and Education Advisors* de l'IIA (anciennement *Board of Research Advisors*) depuis 1997. En 1994, l'IIA lui a décerné le prix international de l'audit et des systèmes d'information (*International Audit and Technology Award*). En 2005, il a reçu le prix Leon R. Radde de l'IIA, qui récompense le meilleur formateur de l'année (*Leon R. Radde Educator of the Year*).

Il intervient régulièrement lors de conférences portant sur les problématiques technologiques émergentes, les pratiques d'audit interne et l'orientation future de l'audit interne. Il est membre du *Board of Governors* du Chapitre de Dallas de l'IIA. Mark est titulaire d'un BS en gestion des affaires et d'un MBA de l'Université de Central Michigan, où il a dispensé des cours sur les systèmes d'information et la comptabilité en tant qu'étudiant de cycle supérieur et membre à temps complet du corps enseignant.

Copyright © 2015 Eyrolles.

À PROPOS DES AUTEURS

Cris Riddle, MA, CIA, CRMA
Solutions & Strategy Audit Manager
TD Ameritrade

Cris est *Solutions & Strategy Audit Manager* pour le compte de TD Ameritrade. Elle est responsable de la gestion des processus, des systèmes et des bases de données pour la gestion d'un service d'audit interne. Par ailleurs, elle élabore et dispense des formations internes, et révise et corrige des supports d'audit, y compris des rapports d'audit, des présentations pour les réunions et des guides de procédure. Cris enseigne également l'art de « la composition anglaise », « le raisonnement critique et la rhétorique », et « la littérature dans le monde » à l'Université Creighton et à l'université méthodiste (*Methodist College*) du Nebraska.

Cris était rédactrice en chef de la 6e édition de l'ouvrage intitulé *Sawyer's Internal Auditing*. Par ailleurs, elle s'est vue décerner le prix de contributeur exceptionnel (*Outstanding Contributor Award*) pour l'article *Blended Engagements* qu'elle a coécrit avec Kurt Reding et Michael Head.

Elle est membre de l'IIA et *General Securities Representative* de la FINRA (séries 7). Elle a obtenu son BA et son MA en création littéraire anglaise à l'Université Creighton d'Omaha (Nebraska), où elle a également reçu une bourse d'études (*Presidential Fellowship*) en tant qu'étudiante de cycle supérieur. Cris rédige des écrits et fait des présentations sur de nombreux thèmes.

Copyright © 2015 Eyrolles.



Copyright © 2015 Eyrolles.



CHAPITRE 1
INTRODUCTION À L'AUDIT INTERNE

Objectifs pédagogiques

- Comprendre les attentes des parties prenantes vis-à-vis de la fonction d'audit interne.
- Connaître les fondamentaux de l'audit interne et de son processus.
- Comprendre la relation entre l'audit et la comptabilité.
- Différencier, dans le cadre des audits financiers, les activités d'assurance des auditeurs internes de celles qui sont menées par les auditeurs externes.
- Se familiariser avec la profession d'audit interne et avec les Instituts.
- Connaître les compétences nécessaires pour réussir dans la profession d'audit interne.
- Identifier les différentes opportunités de carrière dans l'audit interne.

Qu'est-ce que le terme « audit interne » vous évoque spontanément ? Que signifie-t-il pour vous ? Pour de nombreuses personnes, ce terme n'a pas de sens particulier tandis que, pour d'autres, il peut avoir des connotations négatives. Pendant longtemps en effet, nombreux ont été ceux qui pensaient que l'audit en général n'était qu'une branche inintéressante de la comptabilité. Pour d'autres, l'audit interne a une connotation encore plus négative : ils estiment qu'au fond, la seule chose que font les auditeurs, c'est de vérifier le travail d'autres personnes et de rendre compte des erreurs qu'elles ont commises. Il s'agit donc d'une sorte de fonction de police. Nous avons rédigé ce manuel dans le but de faire tomber ces préjugés.

En effet, l'audit interne est considéré comme une fonction qui jouit d'une reconnaissance de plus en plus affirmée. La demande de talents, à tous les niveaux de cette fonction, excède nettement l'offre, et les responsables de l'audit interne appartiennent à la catégorie des cadres dirigeants de l'organisation. Dans un certain nombre de pays, notamment anglo-saxons, ces responsables sont directement rattachés au comité d'audit.

Copyright © 2015 Eyrolles.

Commentaire du traducteur

En France, il y a un consensus en place pour que les responsables d'audit interne rapportent hiérarchiquement à la direction générale tout en ayant des relations étroites avec le comité d'audit.

Début 2013, l'*Institute of Internal Auditors* (IIA) comptait plus de 175 000 adhérents à travers le monde.

Afin d'assurer sa pérennité et sa réussite, l'audit interne doit, comme toute autre fonction d'une organisation, justifier sa raison d'être auprès des parties prenantes clés. En d'autres termes, les parties prenantes doivent mesurer la valeur des services que la fonction d'audit interne peut leur offrir. Ainsi, en 2008, l'IIA a mis en place un groupe de travail « dont la mission consistait à imaginer et à élaborer une description claire et concise de la proposition de valeur de l'audit interne… ». En 2010, le Conseil d'administration de l'IIA – son organe de gouvernance – a approuvé les conclusions de ce groupe de travail. L'encadré 1-1 présente une illustration de la proposition de valeur de l'audit interne, telle qu'établie par l'IIA. Les trois composantes de cette proposition de valeur sont définies ci-après.

Audit interne

Activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée.

- **Assurance = Gouvernance*, gestion des risques** et contrôle*****.** L'audit interne donne une assurance sur les processus de gouvernance, de gestion des risques et de contrôle de l'organisation, afin d'aider cette dernière à atteindre ses objectifs liés à la stratégie, aux opérations, au reporting et à la conformité.
- **Point de vue**** = Catalyseur, analyses et évaluations.** L'audit interne agit comme un catalyseur permettant d'améliorer l'efficacité et l'efficience d'une organisation, grâce à un point de vue et des recommandations fondés sur des analyses et des évaluations des informations et des processus opérationnels.
- **Objectivité = Intégrité, devoir de rendre compte et indépendance.** En faisant preuve d'intégrité et en assumant son devoir de rendre compte, l'audit interne crée de la valeur ajoutée pour les organes de gouvernance et la direction générale, car il constitue une source de conseils objective et indépendante.[1]

* NdT : Les termes « gouvernance » et « gouvernement d'entreprise » sont indifféremment utilisés dans la suite du texte pour traduire le terme *governance*.

** NdT : Les termes « management des risques » et « gestion des risques » sont indifféremment utilisés dans la suite du texte pour traduire le terme *risk management*.

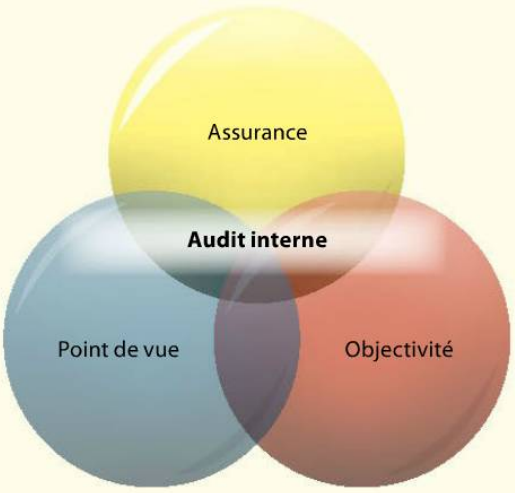
*** NdT : Les processus de contrôle s'entendent au sens large et ne se limitent pas aux activités de contrôle mais à toutes les composantes d'un dispositif de contrôle interne.

**** NdT : Le terme *insight* a été traduit par « point de vue ». En effet, l'audit interne peut être amené à donner des avis, des conseils ou un éclairage qui contribuent à la performance de l'organisation.

Copyright © 2015 Eyrolles.

ENCADRÉ 1-1

PROPOSITION DE VALEUR



Audit interne = Assurance, point de vue et objectivité

Les organes de gouvernance et la direction générale comptent sur l'audit interne pour donner une assurance et un point de vue objectifs sur l'efficacité et l'efficience des processus de gouvernance, de gestion des risques et de contrôle interne.

Miller Patty et Tara Smith, *Insight : Delivering Value to Stakeholders* (Altamonte Springs, Floride : The Institute of Internal Auditors, 2011), p. 14.

Cette proposition de valeur démontre clairement en quoi l'audit interne est important. Nous poursuivrons ce chapitre introductif en explorant la définition de l'audit interne et en présentant aux lecteurs le processus d'audit interne. Nous clarifierons ensuite la relation entre l'audit et la comptabilité, et nous établirons une distinction, dans le cadre des audits financiers, entre les activités d'assurance des auditeurs internes et celles menées par les auditeurs externes, puis nous décrirons la profession d'audit interne et le réseau des Instituts d'audit interne. Nous terminerons ce chapitre en analysant les compétences nécessaires pour réussir dans la profession d'audit interne, ainsi que les différentes opportunités de carrière interne qui s'offrent aux auditeurs passionnés et talentueux.

Valeur ajoutée

Les activités d'assurance comme les activités de conseil apportent de la valeur ajoutée en contribuant à améliorer les opportunités de réaliser les objectifs de l'organisation, en identifiant les améliorations possibles sur le plan opérationnel, et/ou en réduisant l'exposition aux risques.

DÉFINITION DE L'AUDIT INTERNE

Les Instituts ont adopté en 1999 la définition suivante de l'audit interne :

> *« L'audit interne est une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée. Il aide cette organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle, et de gouvernement d'entreprise, et en faisant des propositions pour renforcer leur efficacité. »*[2]

Copyright © 2015 Eyrolles.

Les éléments clés de cette définition sont répertoriés et analysés successivement ci-après :

- aide apportée à l'organisation afin qu'elle atteigne ses objectifs ;
- évaluation et amélioration de l'efficacité des processus de gestion des risques, de contrôle et de gouvernance ;
- activités d'assurance et de conseil destinées à créer de la valeur ajoutée et à améliorer les opérations de l'organisation ;
- indépendance et objectivité ;
- approche systématique et méthodique (le processus d'audit).

Aide apportée à l'organisation afin qu'elle atteigne ses objectifs

Les objectifs d'une organisation définissent ce qu'elle souhaite réaliser, et sa réussite dépend de la réalisation de ces objectifs. Au niveau le plus élevé, ceux-ci sont reflétés dans l'énoncé de la mission et de la vision de l'organisation. L'énoncé de la mission exprime, dans des termes généraux, ce que l'organisation souhaite réaliser aujourd'hui, et l'énoncé de la vision ce qu'elle souhaite réaliser dans l'avenir.

Il n'existe pas de méthode unique pour catégoriser les objectifs d'une organisation. Ce manuel se fonde sur la typologie proposée en 2004 par le *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) :

- **les objectifs stratégiques** ont trait aux choix opérés par le management en vue de créer de la valeur ajoutée pour les parties prenantes de l'organisation. Les « objectifs » désignent ci-après ce qu'une organisation souhaite réaliser, et la « stratégie » la manière dont le management entend atteindre les objectifs de l'organisation. Par exemple, une organisation peut avoir pour objectif d'« accroître sa part de marché » et adopter comme stratégie le « rachat d'autres organisations » en vue de réaliser cet objectif ;
- **les objectifs opérationnels** concernent l'efficacité et l'efficience des activités d'une organisation, notamment les objectifs de rentabilité et de performance et la protection des actifs contre des pertes ;
- **les objectifs de reporting** concernent la fiabilité du reporting interne comme externe et se rapportent à des informations financières et non financières ;
- **les objectifs de conformité** concernent le respect des lois et des réglementations.[3]

Copyright © 2015 Eyrolles.

Les objectifs de l'organisation, énoncés de manière compréhensible et mesurables, constituent les cibles à atteindre et établissent les paramètres qui permettront d'évaluer les réalisations effectives de l'entité sur la durée. Pour l'auditeur interne, ils constituent un fondement pour la définition des objectifs de la mission d'audit (en d'autres termes, ce que l'auditeur interne souhaite réaliser). La relation directe entre d'une part les objectifs de l'organisation et d'autre part les objectifs de la mission d'audit fixe le cadre dans lequel les auditeurs internes pourront aider l'organisation à atteindre ses objectifs. Il s'agit d'un concept important, qui sera mis en lumière dans cet ouvrage. L'encadré 1-2 illustre des exemples d'objectifs de l'organisation et d'objectifs d'audit interne correspondants.

ENCADRÉ 1-2

EXEMPLES D'OBJECTIFS DE L'ORGANISATION ET D'OBJECTIFS D'AUDIT CORRESPONDANTS

	Objectifs de l'organisation	Objectifs de la mission d'audit
Stratégie	Accroître la part de marché de l'organisation en rachetant des organisations complémentaires.	S'assurer que les informations sur lesquelles se fonde le management pour décider s'il faut racheter l'organisation X sont exactes, complètes et valides.
Opérations	Expédier toutes les commandes au maximum 48 heures après leur enregistrement.	Vérifier que les commandes sont bien expédiées dans les 48 heures après leur enregistrement.
Reporting	Comptabiliser uniquement les opérations de vente valides.	Vérifier l'adéquation de la conception et le fonctionnement effectif des activités de contrôle mises en place, afin de s'assurer que les ventes comptabilisées ont bien eu lieu (en d'autres termes, qu'elles reflètent le transfert de propriété des marchandises expédiées aux clients).
Conformité	Respecter la réglementation relative à la sécurité et à l'hygiène au travail.	Vérifier que les règles et procédures établies pour assurer la conformité à la réglementation relative à la sécurité et à l'hygiène au travail existent et sont bien comprises, documentées, diffusées et appliquées.

Objectifs

Ce qu'une organisation souhaite réaliser.

Copyright © 2015 Eyrolles.

Évaluation et amélioration de l'efficacité des processus de gestion des risques, de contrôle et de gouvernance

Une organisation ne peut atteindre ses objectifs et réussir durablement que si ses processus de gestion des risques, de contrôle et de gouvernance sont efficaces. Il s'agit de processus complexes et imbriqués, et une analyse poussée serait à ce stade prématurée. Ils seront détaillés dans les autres chapitres.

Nous proposons ici des définitions simples pour faciliter la réflexion sur le rôle que les auditeurs internes peuvent jouer dans l'évaluation et l'amélioration de ces processus. Nous commencerons par la gouvernance, car elle est généralement considérée comme le plus large de ces trois concepts :

La *gouvernance* (ou *gouvernement d'entreprise*) est le *processus piloté par le Conseil qui consiste à autoriser, diriger et surveiller les activités de la direction générale en vue de réaliser les objectifs de l'organisation.*

Commentaire du traducteur

D'autres définitions proposent une vision plus large des différents acteurs et parties prenantes de la gouvernance (direction générale, Conseil, actionnaires, régulateurs, associations, etc.). Ainsi, selon les principes de l'OCDE, la gouvernance :

- *concerne l'ensemble des relations entre la direction d'une organisation, son conseil d'administration, ses actionnaires et autres parties prenantes ;*
- *fournit le cadre au sein duquel les objectifs de l'organisation sont fixés ;*
- *définit les moyens de les atteindre et de surveiller les performances.*

Par ailleurs, le rôle conféré au Conseil n'est pas universel. Par exemple, en France, le Conseil n'a pas la responsabilité directe de mettre en place les processus et les structures ; il a un rôle de surveillance des dispositifs dont la mise en œuvre est du ressort de la direction générale. La *gestion des risques*, qui est étroitement liée à la gouvernance, est le *processus piloté par le management qui consiste à appréhender et à traiter les incertitudes (risques et opportunités) susceptibles d'affecter la capacité de l'organisation à atteindre ses objectifs, et à agir en conséquence.* Ci-après, le terme « risque » désigne la possibilité de survenance d'un événement qui entraverait la réalisation des objectifs (tel qu'une fraude commise par un collaborateur), et le terme « opportunité » la possibilité de survenance d'un événement qui favoriserait la réalisation des objectifs (par exemple, le lancement d'un nouveau produit).

Le dispositif de contrôle interne, qui est intégré à la gestion des risques, est le processus piloté par le management qui consiste à ramener les risques à un niveau acceptable.

Copyright © 2015 Eyrolles.

Ces trois processus sont axés sur la réalisation des objectifs de l'organisation. Le Conseil, dans le cadre de la gouvernance, a un rôle de surveillance des risques pesant sur la réalisation des objectifs de l'organisation. La direction générale, quant à elle, doit conduire les processus de gestion des risques et de contrôle. « Conduire » signifie ici orienter ou diriger un processus, opération qui se différencie de la réalisation opérationnelle des étapes du processus. Le Conseil et la direction générale doivent coopérer pour que les processus de gouvernance, de gestion des risques et de contrôle soient efficacement mis en œuvre. Ils ont également besoin de la fonction d'audit interne, qui joue un rôle de premier plan dans l'évaluation et l'amélioration de ces processus. Toutefois, la responsabilité de l'audit interne ne consiste pas à orienter ou à diriger les processus de gouvernance, de gestion des risques et de contrôle. Le chapitre 3, *La gouvernance*, le chapitre 4, *La gestion des risques*, et le chapitre 6, *Le contrôle interne*, analysent en détail les responsabilités de l'audit interne dans ces domaines.

Activités d'assurance et de conseil destinées à créer de la valeur ajoutée et à améliorer les opérations de l'organisation

Ces deux types de missions diffèrent par leur finalité première, qui détermine à son tour leur nature et leur périmètre, ainsi que par les parties prenantes concernées. Les termes utilisés pour les désigner sont divers et variés. Le terme « audité » fait ci-après référence aux personnes soumises à une évaluation dans le cadre d'une mission d'assurance, et le terme « client » aux personnes qui demandent certains services dans le cadre d'une mission de conseil.

Les activités d'assurance menées en interne ont pour finalité première d'évaluer les preuves relatives à un aspect intéressant pour l'utilisateur de cette assurance et d'en tirer des conclusions. L'audit interne détermine la nature et le périmètre des missions d'assurance, qui mettent habituellement trois parties en présence : l'audité, qui est directement concerné par l'aspect étudié, l'auditeur interne, qui procède à l'évaluation et rend des conclusions, et l'utilisateur, qui se fonde sur l'évaluation des preuves et sur les conclusions de l'auditeur interne.

Les activités de conseil menées en interne ont pour finalité première de rendre un avis, et d'apporter d'autres formes d'assistance, généralement à la demande expresse des clients de la mission. Le client et l'audit interne s'entendent sur la nature et le périmètre des missions de conseil, qui ne font habituellement intervenir que deux parties : le client, qui recherche et reçoit un avis, et l'auditeur interne, qui donne cet avis.

Indépendance

Capacité de l'audit interne à n'être exposé à aucune situation susceptible d'altérer, en réalité ou en apparence, l'objectivité. Les atteintes à l'indépendance doivent être appréhendées à différents niveaux : - au niveau de l'auditeur interne ; - au niveau de la conduite de la mission ; - au niveau de l'audit interne et de son positionnement dans l'organisation.

Copyright © 2015 Eyrolles.

Objectivité

Attitude impartiale qui permet aux auditeurs internes d'accomplir leurs missions de telle sorte qu'ils soient certains de la qualité de leurs travaux, menés sans compromis. L'objectivité implique que les auditeurs internes ne subordonnent pas leur propre jugement à celui d'autres personnes.

Indépendance et objectivité

Le Code de déontologie et les *Normes internationales pour la pratique professionnelle de l'audit interne* (les *Normes*) adoptés par la profession mettent l'accent sur l'importance critique de l'indépendance et de l'objectivité de l'audit interne. L'indépendance a trait au statut de l'audit interne au sein de l'organisation, et l'objectivité à l'attitude intellectuelle des différents auditeurs internes.

Pour que l'audit interne soit indépendant, le responsable de l'audit interne doit relever d'un niveau hiérarchique au sein de l'organisation investi d'un pouvoir suffisant pour veiller à ce que la mission ait une large étendue, que ses résultats soient dûment pris en compte et que des actions appropriées découlent des recommandations émises. Les Instituts recommandent que le responsable de l'audit interne soit fonctionnellement rattaché au Conseil***** et dépende administrativement ou hiérarchiquement du directeur général (Modalité Pratique d'Application 1110-1, Indépendance dans l'organisation).

L'objectivité signifie qu'un auditeur doit être à même de rendre des jugements impartiaux, sans parti pris. Pour qu'il y ait objectivité, les auditeurs internes ne doivent pas exercer de responsabilités opérationnelles permanentes dans l'organisation, prendre des décisions de gestion ou se mettre dans une situation qui pourrait induire des conflits d'intérêts. Par exemple, si une personne intègre le service d'audit interne après avoir exercé des fonctions dans un autre service de l'organisation, cet auditeur interne ne devra pas mener des activités d'assurance pour ce service pendant un an (Norme 1130.A1-1). On considère en effet que cela reviendrait pour lui à vérifier son propre travail. Le chapitre 2, *Le Cadre de référence international des pratiques professionnelles : des lignes directrices incontournables pour l'audit interne*, analyse plus en détail les concepts d'indépendance et d'objectivité.

Mission

Une mission ou un projet d'audit interne particulier qui englobe de multiples tâches ou activités menées pour atteindre un ensemble déterminé d'objectifs qui s'y rapportent. Voir également Activités d'assurance et Activités de conseil.

Une approche systématique et méthodique : le processus d'audit

Pour qu'il y ait réellement création de valeur ajoutée et amélioration des opérations, les missions internes d'assurance et de conseil doivent être menées selon une approche systématique et méthodique. Les trois étapes fondamentales du processus d'audit interne sont la planification de la mission, la réalisation de la mission et la communication

***** NdT : Le terme « Conseil » est utilisé dans les *Normes* pour désigner le niveau le plus élevé des organes de gouvernance. En règle générale, le Conseil se fait assister par différents comités, dont le comité d'audit avec lequel l'audit interne entretient des relations étroites, la 8e directive européenne confiant à ce comité le soin d'assurer le suivi de l'efficacité des systèmes de contrôle interne, d'audit interne et de gestion des risques.

Copyright © 2015 Eyrolles.

des résultats de la mission. Ces trois étapes sont abordées dans le chapitre 12, *Introduction au processus d'audit*, et traitées en détail dans le chapitre 13, *Le déroulement de la mission d'assurance*, dans le chapitre 14, *La communication des résultats d'une mission d'assurance et les procédures de suivi*, et dans le chapitre 15, *La mission de conseil*. Cependant, nous en présentons ici un bref aperçu.

La planification de la mission consiste notamment à :

- comprendre l'audité ou le client. Un auditeur interne ne peut pas mener des activités d'assurance ou de conseil, sources de valeur ajoutée, s'il ne cerne pas bien le profil de l'audité ou du client. Il doit donc déterminer les objectifs de l'audité ou du client et les risques qui menacent leur réalisation, mais aussi, entre autres, quelles sont les ressources humaines, les ressources matérielles et les opérations de l'audité ou du client ;
- fixer les objectifs de la mission. Les activités d'assurance et de conseil internes ont pour finalité générale d'aider l'organisation à atteindre ses objectifs. Les objectifs de l'audité ou du client serviront à l'auditeur interne de fondement pour définir les résultats souhaités de la mission ;
- déterminer les preuves à recueillir. L'auditeur interne doit concevoir la mission de façon à obtenir des preuves suffisantes et adéquates pour lui permettre d'atteindre les objectifs de sa mission ;
- décider de la nature, du calendrier et de l'étendue des tests d'audit. Ces décisions influeront sur le type de tests que l'auditeur interne devra mettre en œuvre pour rassembler les preuves nécessaires.

La réalisation de la mission requiert des procédures d'audit spécifiques : demandes de renseignements, observations des opérations, études de documents et analyses de la vraisemblance des informations. Pour rassembler des preuves, il importe également de formaliser les travaux réalisés et les résultats obtenus.

L'évaluation des preuves rassemblées au cours d'une mission d'assurance nécessite de tirer des conclusions logiques sur la base de ces preuves. Un auditeur interne peut, par exemple à l'issue d'analyses menées sur le processus de vente, conclure à l'efficacité (ou inefficacité) du contrôle interne. L'évaluation des preuves rassemblées au cours d'une mission de conseil nécessite de formuler des conseils pratiques sur la base de ces preuves. Un auditeur interne peut par exemple conseiller à son client d'intégrer des contrôles applicatifs spécifiques dans un nouveau système d'information informatisé.

La communication des résultats de la mission est un élément clé de toutes les missions d'assurance et de conseil. Indépendamment de sa teneur et de sa forme, qui peuvent varier, elle « doit être exacte, objective, claire, concise, constructive, complète et émise en temps utile » (Norme 2420, Qualité de la communication).

Copyright © 2015 Eyrolles.

RELATION ENTRE L'AUDIT ET LA COMPTABILITÉ

Certaines personnes pensent parfois que l'audit interne constitue une branche de la comptabilité. Cet *a priori* ne correspond pas à la réalité. L'encadré 1-3 présente une citation extraite d'un ouvrage intitulé *The Philosophy of Auditing* qui explique la différence entre audit et comptabilité.

Même si cette citation a pour contexte l'audit des états financiers mené par un auditeur externe, les idées qui y sont exprimées sont tout aussi pertinentes pour les activités d'assurance et de conseil réalisées en interne. Ces activités internes sont fondées sur des analyses et des recherches, et elles reposent sur la logique, donc sur un raisonnement et des déductions. Les auditeurs internes font appel à la logique lorsqu'ils rendent des conclusions ou un avis d'après les preuves qu'ils ont rassemblées et évaluées. La qualité de ces conclusions ou de cet avis dépend elle-même de leur capacité à réunir et à évaluer des preuves suffisantes et adéquates.

ENCADRÉ 1-3

RELATION ENTRE L'AUDIT ET LA COMPTABILITÉ

« L'audit et la comptabilité […] diffèrent largement par leur nature […]. La comptabilité consiste à rassembler, classifier, synthétiser et communiquer des données financières. Elle suppose de mesurer et de notifier les événements et les contextes qui affectent une organisation en particulier ou une autre entité. La comptabilité a pour finalité de ramener une masse considérable d'informations détaillées à des proportions gérables et compréhensibles. L'audit ne fait rien de tel. Il doit lui aussi examiner des événements et des contextes, mais il n'a pas pour finalité de les mesurer ou de les notifier. Il vise à vérifier l'adéquation des mesures et des notifications émanant de la comptabilité. L'audit est un processus analytique, et non constructif. Il consiste à porter un jugement critique, à faire des recherches et à s'intéresser aux fondements des mesures et des assertions de la comptabilité. L'audit met l'accent sur le caractère probant des éléments qui étayent les états financiers et les données financières. Il s'appuie donc essentiellement, non pas sur la comptabilité, qu'il analyse, mais sur la logique, dans laquelle il puise largement des concepts et des méthodes. »

Mautz, R. K. et Hussein A. Sharaf, *The Philosophy of Auditing* (Sarasota, Floride : American Accounting Association, 1961, p. 14).

COSO

Committee of Sponsoring Organizations of the Treadway Commission

ACTIVITÉS D'ASSURANCE MENÉES DANS LE CADRE DES AUDITS FINANCIERS

Missions externes et internes

Dans de nombreux pays, les sociétés cotées sont tenues, en vertu de la loi ou de la réglementation locale, de faire vérifier leurs états financiers annuels par un auditeur externe, tel qu'un cabinet d'experts-comptables. Un audit des états financiers (ou vérification des

Copyright © 2015 Eyrolles.

comptes) constitue une forme d'activité d'assurance, par laquelle le cabinet présente un rapport qui exprime une opinion quant à la sincérité des comptes par rapport à la réalité, conformément aux principes comptables généralement admis. Nombre d'entreprises privées, d'organismes publics et d'organisations à but non lucratif font également auditer leurs états financiers chaque année.

Aux États-Unis, la loi Sarbanes-Oxley requiert que les sociétés cotées fassent appel à un auditeur externe (que l'on appelle souvent « auditeur légal ») pour attester de l'efficacité, à la date du bilan, du contrôle interne relatif au reporting financier mis en œuvre au sein de l'organisation. L'opinion de l'auditeur légal sur le contrôle interne doit s'appuyer sur un cadre de référence reconnu, tel que celui du COSO. Le référentiel COSO est détaillé, avec d'autres référentiels de contrôle interne, dans le chapitre 6, *Le contrôle interne*. Le rapport d'audit des états financiers présenté par l'auditeur externe, de même que son rapport sur l'efficacité du contrôle interne relatif au reporting financier, sont des documents publics : ils sont inclus dans le rapport annuel de l'organisation et déposés auprès des autorités de régulation des marchés financiers (SEC aux États-Unis). Les États-Unis ne sont pas les seuls à imposer cette obligation. De nombreux autres pays ont adopté des lois prévoyant des obligations similaires en matière de reporting financier.

Commentaire du traducteur

La directive 2006/46/CE relative aux comptes annuels et aux comptes consolidés modifiant les 4e et 7e directives européennes exige des sociétés dont les titres sont admis à la négociation sur un marché réglementé une information sur les principales caractéristiques de leurs systèmes de contrôle interne et de gestion des risques dans le cadre du processus d'établissement de l'information financière. En France, la loi du 3 juillet 2008 a transposé cette directive et complété la Loi de Sécurité Financière (LSF) de 2003. Les commissaires aux comptes présentent, dans un rapport joint au rapport du Président, leurs observations sur celles des procédures de contrôle interne et de gestion des risques qui sont relatives à l'élaboration et au traitement de l'information comptable et financière. Ils attestent l'établissement des autres informations requises.

Pour la rédaction du rapport du Président, les sociétés peuvent s'appuyer sur le cadre de référence de gestion des risques et du contrôle interne élaboré par l'AMF.

C'est principalement pour les tiers que les auditeurs externes mènent leurs activités d'assurance dans le cadre des audits financiers. En effet, pour prendre des décisions financières relatives à une organisation, les tiers se fient aux attestations indépendantes la concernant qui émanent de cabinets d'audit. Ces attestations confèrent de la crédibilité à l'information exploitée par ces tiers pour prendre leurs décisions, ce qui renforce la confiance de ces utilisateurs dans l'exactitude, l'exhaustivité et la validité de cette information.

Copyright © 2015 Eyrolles.

Les auditeurs internes peuvent mener, eux aussi, des activités d'assurance dans le cadre des audits financiers. La principale différence par rapport aux activités des auditeurs externes tient au destinataire : les auditeurs internes travaillent essentiellement pour la direction générale et pour le Conseil. Aux États-Unis, la loi Sarbanes-Oxley impose notamment au directeur général et au directeur financier des sociétés cotées à la bourse de New York de certifier les états financiers de celles-ci dans le cadre des dépôts trimestriels et annuels des états financiers. Pour évaluer et se prononcer sur l'efficacité du contrôle interne relatif au reporting financier, le management de l'organisation se fonde sur les activités d'assurance menées dans le cadre des audits financiers par l'audit interne, qui doit procurer l'assurance de la véracité des assertions constituant le reporting financier.

LA PROFESSION D'AUDIT INTERNE

L'audit interne moderne : une profession dynamique et recherchée

> *« La profession d'auditeur, et plus particulièrement celle d'auditeur interne, remonte à la nuit des temps. »*[4]

Les historiens font remonter l'audit interne à plusieurs siècles avant J.-C., mais on associe souvent la genèse de l'audit interne moderne à la création de l'Institut de l'Audit interne (IIA) aux États-Unis, en 1941. À sa naissance, l'IIA était une organisation nationale qui comptait 24 membres.[5]

Les Instituts comme la profession d'audit interne ont considérablement évolué depuis cette époque. L'encadré 1-4 présente quelques dates jalons dans l'histoire de l'IIA. Il en ressort deux faits saillants : la croissance phénoménale de la profession, surtout depuis 30 ans, et sa mondialisation. Aujourd'hui, les Instituts comptent des membres dans près de 170 pays et territoires, dont 60 % ne résident pas en Amérique du Nord.[6] L'audit interne est devenu un secteur véritablement mondial, et la demande de missions d'audit interne ne cesse de croître.

Plusieurs circonstances et événements imbriqués ont alimenté cette expansion spectaculaire de la demande de services d'audit interne sur les 30 dernières années. Durant cette période, le monde de l'entreprise s'est transformé, notamment sous l'effet de la mondialisation, de la complexification des structures des organisations, du développement du commerce électronique et d'autres avancées technologiques, ainsi que d'une récession économique mondiale. Parallèlement, le monde de l'entreprise a vu éclater une succession de scandales aux conséquences dévastatrices, qui ont rapidement

Copyright © 2015 Eyrolles.

déclenché une vague de lois, de règlements et de lignes directrices nouvelles destinés aux professionnels. La conjonction de ces facteurs continue d'élargir l'éventail des risques que les cadres des organisations doivent appréhender et traiter. En conséquence, les auditeurs internes sont de plus en plus sollicités pour aider les organisations à renforcer leurs processus de gouvernance, de gestion des risques et de contrôle.

Nature et périmètre des services d'audit interne modernes

La fonction d'audit interne a un objectif majeur : « aider une organisation à atteindre les siens ». C'est pourquoi l'attention de l'audit interne doit se concentrer sur :

- le fonctionnement effectif et l'efficience des processus opérationnels ;
- la fiabilité des systèmes d'information et la qualité des informations utiles à la prise de décision produites par ces systèmes ;
- la protection des actifs contre les pertes, notamment celles résultant de fraudes du management et de collaborateurs ;
- le respect des règles de l'organisation, des contrats, des lois et règlements.

> *« Les organes de gouvernance et la direction générale comptent sur l'audit interne pour donner une assurance et un point de vue objectif sur l'efficacité et l'efficience des processus de gouvernance, de gestion des risques et de contrôle interne. »*[7]

Conformité

Respect des lois et règlements applicables, et adhésion aux règles, plans, procédures, contrats ou autres exigences.

La fonction d'audit interne aide l'organisation à atteindre ses objectifs en évaluant et en améliorant l'efficacité de ses processus de gouvernance, de gestion des risques et de contrôle, et en apportant un point de vue dans le cadre d'activités de conseil. Ces évaluations et améliorations amènent l'audit interne à se pencher sur quasiment tous les pans de l'organisation : production de biens et services, gestion financière, ressources humaines, recherche et développement, logistique, et systèmes d'information, notamment. L'audit interne répond ainsi aux besoins de différentes parties prenantes : le Conseil, la direction générale, les collaborateurs et les tiers intéressés.

L'audit interne donne son point de vue en utilisant tout un ensemble d'outils pour tester l'adéquation de la conception et le fonctionnement effectif des processus de gouvernance, de gestion des risques et de contrôle au sein de l'organisation. Il peut notamment :

- enquêter auprès des managers et des collaborateurs ;
- observer les activités ;
- inspecter les ressources et les documents ;

Copyright © 2015 Eyrolles.

ENCADRÉ 1-4

DATES MARQUANTES DE LA PROFESSION

1941	Création de l'Institut de l'Audit interne (IIA) aux États-Unis. Il compte alors 24 membres.
1947	Publication du ***Statement of Responsibilities of the Internal Auditor***.
1948	Les premiers chapitres hors d'Amérique du Nord ouvrent à Londres et Manille.
1953	L'IIA adopte sa devise officielle : « Le progrès par le partage » (*Progress Through Sharing*).
1957	Le ***Statement of Responsibilities of the Internal Auditor*** est révisé de manière à inclure davantage de responsabilités dans les domaines opérationnels.
1965	Création de l'Institut français de l'audit et du contrôle internes (IFACI).
1968	Approbation du Code de déontologie de l'IIA.
1973	Nomination du premier *Board of Regents*. Mise en place du programme d'auditeur interne certifié (CIA).
1976	Fondation de la *Foundation of Auditability, Research, and Education* (FARE), qui deviendra par la suite *The IIA Research Foundation* (Fondation pour la recherche de l'IIA).
1978	Approbation des ***Normes pour la pratique professionnelle de l'audit interne***.
1979	Approbation du *National Institute Agreement* (accord sur les Instituts nationaux) ; ouverture de cinq Instituts nationaux.
1980	L'IIA compte alors 21 549 membres.
1982	Création de l'ECIIA (Confédération européenne des instituts d'audit interne).
1984	Publication de l'ouvrage ***Quality Assurance Review Manual***. Création d'une école pilote au sein de l'Université d'État de la Louisiane. Publication du premier ouvrage ***Statement on Internal Auditing Standards*** (SIAS).
1986	Lancement du programme d'éducation cible.
1988	Création de l'Institut de l'Audit interne en République populaire de Chine.
1989	Les Nations unies accordent à l'IIA un statut consultatif.
1990	A.J. Hans Spoel est le premier président élu par l'IIA qui ne soit pas originaire d'Amérique du Nord.
1995	L'IIA devient officiellement membre de l'*American National Standards Institute* (ANSI) et le seul représentant américain auprès de l'Organisation internationale de normalisation (ISO).
1996	***Accounting Today*** nomme le président de l'IIA, William G. Bishop III, CIA, comme l'une des « 100 personnalités les plus influentes dans le domaine de la comptabilité ». L'IIA commence à promouvoir activement le programme CIA en Europe, en Asie, au Moyen-Orient et en Amérique du Sud.
1998	Le premier examen du CIA, portant sur l'ensemble des objectifs, est organisé, et un nombre record de 5 165 candidats se présentent pour une ou plusieurs parties.
1999	Introduction de la nouvelle définition de l'audit interne. 25e anniversaire de la certification CIA.
2000	Les nouvelles ***Normes*** sont publiées. L'IIA compte 68 985 membres.
2002	Les ***Normes*** deviennent obligatoires pour tous les membres de l'IIA et pour les CIA.
2003	Publication par l'IIA du nouveau Cadre de référence international des pratiques professionnelles.
2006	L'IIA compte plus de 120 000 adhérents. L'IFACI lance IFACI Certification.

Copyright © 2015 Eyrolles.

2007	Pour continuer d'employer l'expression « mené conformément aux ***Normes internationales pour la pratique professionnelle de l'audit interne*** », les fonctions d'audit interne qui existaient préalablement au 1er janvier 2002 doivent faire procéder à une évaluation externe de leur qualité avant le 1er janvier 2007.
2008	Introduction de tests informatisés pour l'ensemble des examens professionnels organisés par l'IIA.
2009	Publication du Cadre de référence international des pratiques professionnelles qui contient les dispositions obligatoires (définition de l'audit interne, Code de déontologie et *Normes internationales pour la pratique professionnelle de l'audit interne*) et les dispositions fortement recommandées (Modalités Pratiques d'Application, prises de position et guides pratiques).
2010	L'IIA accroît sa présence sur les médias sociaux Twitter, Facebook et LinkedIn. En outre, l'*Audit Executive Center* de l'IIA est mis en place. Il constitue un ensemble facilement accessible d'informations, de ressources et de services qui contribuent à la réussite des responsables de l'audit interne.
2011	L'IIA lance son propre réseau social, un nouveau site de partage de vidéos : www.auditchannel.tv. Ce réseau social propre à l'audit permet aux professionnels de l'audit interne de voir, poster et commenter de courtes vidéos sur des sujets qui les intéressent. À l'heure actuelle, le site propose des vidéos dans les langues suivantes : anglais, espagnol, français, japonais et chinois.

Source : www.theiia.org

- exécuter à nouveau les activités de contrôle ;
- analyser les tendances et les ratios ;
- analyser les données au moyen de techniques d'audit informatisées ;
- rassembler des éléments de corroboration émanant de tiers indépendants ;
- effectuer des tests directs d'événements et de transactions.

L'audit interne peut également mettre à profit diverses activités de conseil pour :

- suggérer des orientations concernant l'efficacité des processus de gouvernance, de gestion des risques et de contrôle ;
- faciliter la mise en œuvre d'actions visant à encourager la maîtrise des processus de gouvernance, de gestion des risques et de contrôle ;
- aider à la mise en place d'une formation sur les concepts existants et émergents de processus de gouvernance, de gestion des risques et de contrôle.

Professionnels procurant des services d'audit interne

Tous types d'organisations peuvent faire appel à des prestataires de services d'audit interne : des sociétés cotées et non cotées, des

Copyright © 2015 Eyrolles.

organismes publics au niveau local, national ou fédéral, ainsi que des entités à but non lucratif. Jusqu'à récemment, ces services étaient exclusivement fournis en interne, c'est-à-dire par les collaborateurs de l'organisation qui réalisent ces prestations. Tel n'est plus le cas aujourd'hui. Certaines organisations choisissent de transférer leur fonction d'audit interne, intégralement ou en partie, à des prestataires extérieurs, par exemple, à des cabinets externes. La forme la plus répandue d'externalisation est le « co-sourcing » : une organisation fait appel aux services de prestataires extérieurs pour compléter, dans une certaine mesure, sa fonction d'audit interne « maison ». En règle générale, une organisation choisira le co-sourcing de l'audit interne par exemple dans des cas où le prestataire dispose d'un savoir ou savoir-faire dans une spécialité de l'audit interne qu'elle-même n'a pas, ou lorsque ses propres ressources sont insuffisantes pour réaliser intégralement les missions planifiées. Le chapitre 9, *La gestion de l'audit interne*, détaille le co-sourcing.

La devise de l'IIA

Le progrès par le partage (*Progress Through Sharing*)

L'INSTITUT DES AUDITEURS INTERNES

L'IIA, dont le siège se trouve à Altamonte Springs en Floride, aux États-Unis, est reconnu comme « le représentant, l'organisme de normalisation et le centre de ressources pour le développement professionnel et la certification dans le secteur de l'audit interne, dans le monde entier »[8]. L'encadré 1-5 présente sa mission.

L'organisation de l'IIA

Commentaire du traducteur

L'IIA est organisé en chapitres et affiliés locaux, notamment dans le monde francophone. Par exemple, des instituts européens tels que l'IFACI, l'IIA Bel, l'ASAI, l'IIA Luxembourg, l'Institut des vérificateurs internes au Québec et à Montréal et les instituts africains.

En France, l'IFACI (Institut français de l'audit et du contrôle internes) fédère près de 6 000 auditeurs issus de quelque 900 organismes des secteurs public et privé. Chaque Institut local est gouverné par des instances spécifiques. Vous pourrez trouver plus de détails sur la gouvernance des Instituts sur leur site Internet (www.ifaci.com pour l'IFACI, www.theiia.org pour l'IIA).

La direction opérationnelle du siège de l'IIA est formée du président et directeur général, du vice-président directeur, du directeur financier et des vice-présidents. La direction de l'IIA bénéficie également de l'appui de centaines de bénévoles, parmi lesquels les membres du Conseil d'administration.

Le Conseil d'administration, qui compte 38 membres, supervise les activités de l'IIA. Le comité exécutif du Conseil se compose

Copyright © 2015 Eyrolles.

du président du Conseil, du premier vice-président, de quatre vice-présidents, du trésorier, du secrétaire et des deux plus récents anciens présidents du Conseil. Le Conseil inclut également le *North American Council*, qui dispose d'une autorité spécifique et d'un pouvoir de supervision sur les activités nord-américaines, certains administrateurs des organismes affiliés, les *directors-at-large*, ainsi que le président et directeur général de l'IIA qui est administrateur de droit.[9]

ENCADRÉ 1-5

LA MISSION DE L'IIA

Mission :
L'*Institute of Internal Auditors* a pour mission de fournir des orientations dynamiques à la profession d'audit interne à l'échelle mondiale. Les activités qui lui permettent de mener à bien cette mission consistent notamment, mais pas exclusivement, à :

- promouvoir la valeur que les professionnels de l'audit interne apportent à leur organisation ;
- proposer des offres complètes de formation et de développement professionnels ; établir des normes et d'autres lignes directrices pour la pratique professionnelle ; proposer des programmes de certification ;
- étudier l'audit interne et son rôle tout particulier en matière de contrôle, de gestion des risques et de gouvernance ;
- en diffuser et en promouvoir la connaissance auprès des professionnels et des parties prenantes ;
- former les professionnels et autres personnes concernées aux meilleures pratiques de l'audit interne ;
- favoriser le partage d'informations et d'expériences entre les auditeurs internes du monde entier.

Source : www.theiia.org

Lignes directrices à l'intention des professionnels

CRIPP

Cadre de référence international des pratiques professionnelles qui comporte les lignes directrices édictées par l'IIA, qui sont :
- soit obligatoires ;
- soit approuvées et fortement recommandées.

Les Instituts proposent des lignes directrices à l'intention des professionnels de l'audit *via*, entre autres, le Cadre de référence international des pratiques professionnelles de l'audit interne (CRIPP). Voici une introduction succincte à ce cadre de référence, qui est détaillé dans le chapitre 2, *Le Cadre de référence international des pratiques professionnelles : des lignes directrices incontournables pour l'audit interne*.

Le CRIPP comporte deux catégories de dispositions.

Catégorie 1 : dispositions obligatoires. Le respect de ces dispositions est exigé et indispensable pour la pratique professionnelle de l'audit interne. Les dispositions obligatoires sont élaborées selon un processus de *due diligence* bien établi, qui inclut une consultation publique afin de permettre aux parties prenantes d'apporter une contribution. Les trois éléments obligatoires du Cadre de référence

Copyright © 2015 Eyrolles.

international des pratiques professionnelles de l'audit interne sont la définition de l'audit interne, le Code de déontologie et les *Normes*.[10]

Catégorie 2 : dispositions fortement recommandées. Ces dispositions sont soumises à un processus d'approbation formel. Elles proposent des pratiques pour la mise en œuvre effective de la définition de l'audit interne, du Code de déontologie et des *Normes* de l'IIA. Les trois éléments du CRIPP, dont la mise en œuvre est fortement recommandée, sont les Modalités Pratiques d'Application, les prises de position et les guides pratiques.[11] Vous trouverez sur le site Internet de l'IIA (www.theiia.org) de plus amples détails sur le Cadre de référence international des pratiques professionnelles et sur les autres sources de lignes directrices.

Certifications professionnelles

***Certified Internal Auditor* (CIA, auditeur interne certifié)**

Certification professionnelle internationale proposée par l'IIA ; elle est reconnue partout dans le monde.

Le CIA est une certification professionnelle internationale proposée par l'IIA et reconnue partout dans le monde. Les examens du CIA testent les connaissances des candidats dans trois domaines : les fondamentaux de l'audit interne, la pratique de l'audit interne et les éléments de connaissance de l'audit interne. Outre la réussite aux examens du CIA, les candidats doivent justifier d'au moins deux ans d'expérience dans l'audit interne, ou d'une expérience équivalente, pour devenir CIA.

Par ailleurs, l'IIA délivre quatre autres certifications professionnelles : une certification en auto-évaluation des contrôles (CCSA®), une certification en audit des organisations publiques (CGAP®), une certification en audit des services financiers (CFSA®) et une certification en évaluation de la gestion des risques (CRMA™). Vous trouverez des informations détaillées concernant les programmes de certification sur le site Internet de l'Institut.

D'autres organisations professionnelles délivrent également des certifications dans le domaine de l'audit interne. Ainsi, l'ISACA (anciennement connu sous le nom d'*Information Systems Audit and Control Association*) décerne la certification *Certified Information Systems Auditor* (certification en audit des systèmes d'information) et l'*Association of Certified Fraud Examiners* décerne la certification *Certified Fraud Examiner*.

Produits et services de recherche et de formation

Les Instituts sont largement reconnus comme les principaux formateurs et leaders mondiaux du développement professionnel pour les auditeurs internes. La diversité des produits et services de recherche et de formation proposés est brièvement décrite ci-dessous. Vous trouverez de plus amples informations sur les sites Internet des Instituts.

Copyright © 2015 Eyrolles.

Commentaire du traducteur

Par exemple, l'IFACI anime des groupes de travail regroupant près de 200 professionnels de l'audit et du contrôle interne. Des publications sont régulièrement mises à disposition des adhérents sur le site Internet.

En outre, les événements et les formations sont autant d'opportunités de développement professionnel.

Fondée en 1976, la Fondation pour la recherche de l'IIA (*IIA Research Foundation*, IIARF) a pour mission « d'enrichir, de faire progresser et d'élargir la connaissance de l'audit interne en mettant à disposition des travaux de recherche et des produits pédagogiques pertinents pour la profession dans le monde entier ». Son principal objectif est « de soutenir la recherche et la formation en audit interne et d'encourager le développement de la profession »[12]. La fondation parraine des projets de recherche et publie des rapports. Sa librairie rassemble des centaines de produits pédagogiques, notamment des livres et des vidéos, sur tous les sujets qui intéressent les professionnels de l'audit interne.

La Fondation pour la recherche de l'IIA (*IIA Research Foundation*, IIARF)

Fondée en 1976, elle a pour mission d'enrichir, de faire progresser et d'élargir la connaissance de l'audit interne en mettant à disposition des travaux de recherche et des produits pédagogiques pertinents pour la profession dans le monde entier.

Les services d'étude comparative et les enquêtes flash du *Global Audit Information Network* (GAIN) de l'IIA permettent aux fonctions d'audit interne de partager leurs informations et leurs connaissances. Dans sa revue bimestrielle, *Internal Auditor*, l'IIA publie des articles de grand intérêt pour les auditeurs internes à travers le monde. L'Institut publie également de nombreuses lettres d'information qui couvrent des sujets intéressants pour l'audit interne, et notamment des sujets présentant un intérêt particulier pour les responsables de l'audit interne et pour divers secteurs et groupes spécifiques de l'audit interne tels que l'audit des services financiers, des jeux et des SI.

Conférence de premier plan, la conférence internationale annuelle de l'IIA attire des milliers d'auditeurs internes venus du monde entier. Par ailleurs, l'IIA propose d'autres opportunités : des conférences sur des secteurs spécifiques telles que la conférence sur les services financiers et la conférence sur l'audit des administrations publiques ; des conférences spécialisées telles que la conférence destinée aux responsables de l'audit interne (GAM – *General Audit Management Conference*) ; des conférences locales et régionales.

Grâce à l'*Academic Relations Committee*, l'IIA promeut et soutient la formation en audit interne à l'échelle mondiale. Le programme *Internal Auditing Education Partnership* (IAEP) a été conçu pour soutenir les universités et les écoles qui se sont formellement engagées à proposer un cursus d'audit interne. En fonction du niveau de développement du cursus d'audit interne qu'elles proposent, celles-ci reçoivent un soutien plus ou moins important de la part de l'IIA.

Copyright © 2015 Eyrolles.

Commentaire du traducteur

Les Instituts locaux entretiennent et développent des relations avec les universités et les grandes écoles qui délivrent des diplômes en audit interne. À ce titre, l'IFACI :

- *participe à des comités pédagogiques ;*
- *procure des intervenants en audit interne ;*
- *participe à des jurys de 3e cycle relatif à l'audit interne (sélections, soutenances de mémoires) ;*
- *favorise les échanges d'expérience avec les entreprises ;*
- *facilite la préparation des étudiants aux certifications professionnelles.*

L'IFACI a des partenariats avec, en particulier, le CNAM, SKEMA Lille, Toulouse Business School, IAE Aix-en-Provence, IAE Bordeaux, IAE Lille, IAE Lyon, IAE Tours. En outre, l'IFACI et l'ESCP Europe ont développé une coopération tout à fait particulière dans les domaines du contrôle interne et de la gestion des risques.

COMPÉTENCES NÉCESSAIRES POUR EXCELLER DANS L'AUDIT INTERNE

« J'ai à mon service six honnêtes domestiques.
Ils m'ont appris tout ce que je sais ;
ils s'appellent Quoi et Pourquoi, Quand
et Comment, et Où et Qui. »[13]

Cette citation est le début d'un poème de Rudyard Kipling, « *L'Enfant d'Éléphant* ». Il s'en dégage deux points essentiels pour les auditeurs internes : la nécessité d'apprendre en permanence et de toujours poser des questions.

Plusieurs questions apparaissent à la lecture de la définition et de la description de l'audit présentées plus haut dans ce chapitre : que faut-il savoir d'autre pour réussir en tant qu'auditeur interne ? Que doit-on savoir faire ? Certaines caractéristiques personnelles prédisposent-elles à la réussite dans ce domaine ? La bonne nouvelle, c'est que ces questions n'appellent pas une réponse unique : différentes personnes aux profils de compétences variés peuvent être de très bons auditeurs internes. De surcroît, les compétences requises pour réussir dans ce domaine ne sont pas spécifiques à l'audit interne.

Il existe, cependant, un certain nombre de compétences observées chez la plupart des auditeurs internes qui semble être un gage de réussite dans la fonction. Certaines de ces compétences sont en fait des qualités personnelles naturelles. D'autres sont des connaissances et un savoir-faire qui peuvent s'acquérir et être développés. La compréhension de ces éléments permet à quiconque de savoir, en toute connaissance de cause, si l'audit interne constitue une voie professionnelle envisageable.

Copyright © 2015 Eyrolles.

Qualités personnelles

Chacun a ses propres qualités ou caractéristiques personnelles. Ainsi, certains sont d'une nature plutôt introvertie (timides ou réservés) tandis que d'autres sont plus extravertis (ils se lient facilement et sont sociables). Voici quelques-unes des qualités personnelles communes à tous les excellents auditeurs internes.

- **Intégrité.** L'intégrité n'a rien de facultatif chez les auditeurs internes : c'est au contraire un impératif. En effet, c'est sur l'intégrité des personnes que se bâtit la confiance, sans laquelle il est impossible d'être sûr que les propos et les actions sont fiables. Ceux qui s'appuient sur les travaux d'audit interne se fient au jugement professionnel des auditeurs internes pour prendre des décisions importantes. Ils doivent avoir la certitude que les auditeurs internes sont dignes de foi.
- « **Passion** ». Il est quasiment impossible de réussir dans une activité que l'on n'aime pas véritablement. Les bons auditeurs internes ressentent un intérêt profond et un enthousiasme sincère pour leur travail. Si certains expriment davantage cette passion, celle-ci est de toute façon indispensable à une réussite durable.
- **Capacité de travail.** Pour réussir dans la profession, il faut être à même de répondre en permanence aux attentes des « clients » en termes de qualité, de coût et de délai. Il faut pour cela travailler dur. Les auditeurs internes doivent non seulement travailler dur, mais également faire intelligemment ce qu'il faut de la façon qu'il faut et au moment où il le faut.
- **Curiosité.** L'information nécessaire pour formuler un jugement au cours d'une mission d'audit interne ne saute pas toujours aux yeux. Un auditeur interne qui réussit doit donc être naturellement curieux et ne pas se contenter de poser des questions sous la forme d'une checklist. Il lui faut parfois poser des questions plus approfondies pour comprendre comment les choses fonctionnent.
- **Créativité.** La plupart des auditeurs internes aiment résoudre des problèmes. Cependant, beaucoup de problèmes n'ont pas de solution évidente. C'est pourquoi, pour réussir, les auditeurs internes doivent se montrer créatifs et faire en sorte que leur pensée sorte des sentiers battus, afin d'avoir des idées appréciées par le management et par d'autres parties prenantes.
- **Initiative.** Un auditeur interne qui réussit a l'esprit d'initiative. Il recherche de lui-même, exploite les possibilités de création de valeurs, et souhaite être un agent du changement au sein de son organisation.
- **Flexibilité.** Le changement est la seule constante dans le monde de l'entreprise d'aujourd'hui. Les organisations performantes s'y adaptent en permanence, et comme le changement s'accompagne de nouveaux risques, ceux-ci doivent être gérés.

***Internal Auditing Education Partnership* (IAEP)**

Sponsorisé par l'IIA, le programme IAEP est un cursus en audit interne dans des écoles et universités sélectionnées.

Copyright © 2015 Eyrolles.

Un auditeur interne qui réussit prend en compte le changement et s'adapte rapidement aux situations et difficultés nouvelles.

Les caractéristiques décrites ci-dessus sont les qualités personnelles que doit posséder un auditeur interne pour réussir. Doit-on en déduire que quelqu'un à qui il manque une ou plusieurs de ces caractéristiques est voué à l'échec dans cette profession ? Pas nécessairement. Certes, l'intégrité est impérative et il serait inutile de vouloir continuer dans une profession dans laquelle on ne croit pas vraiment ou pour laquelle on n'est pas prêt à s'engager pleinement. Les autres qualités énumérées peuvent s'acquérir et être développées si l'on s'en donne la peine. Il importe néanmoins de comprendre comment chacune de ces qualités permet aux auditeurs internes de réussir. Pour ceux qui visent une réussite durable, la plupart de ces qualités seront nécessaires.

Connaissances, savoir-faire et références

Compétence

Les auditeurs internes doivent posséder les connaissances, le savoir-faire et les autres compétences nécessaires à l'exercice de leurs responsabilités individuelles. L'équipe d'audit interne doit collectivement posséder ou acquérir les connaissances, le savoir-faire et les autres compétences nécessaires à l'exercice de ses responsabilités. (Norme 1210)

Les *Normes* de la profession imposent aux auditeurs internes d'accomplir leurs missions d'assurance et de conseil avec compétence, ce qui signifie qu'ils doivent posséder ou acquérir les connaissances, le savoir-faire et les autres compétences nécessaires à l'exercice de leurs responsabilités (Norme 1210). Quelles connaissances et quel savoir-faire sont nécessaires pour réussir en tant qu'auditeur interne ? La réponse à cette question varie, dans une certaine mesure, en fonction du degré d'avancement dans la carrière et des responsabilités à exercer. Ceux qui envisagent de mener une longue carrière dans l'audit interne devront sans cesse perfectionner leurs connaissances et leur savoir-faire. Ainsi, on attendra d'un chef de mission ayant quatre ans d'expérience un niveau d'exigence qui ne sera pas le même que pour un jeune diplômé. En conséquence, s'il est un savoir-faire essentiel qu'il faut commencer à développer dès l'école, c'est d'apprendre à apprendre, car les auditeurs internes ne cessent d'apprendre tout au long de leur carrière.

Nul ne saurait être un expert de l'audit interne à sa sortie d'une école. Comme toute profession, l'audit interne s'apprend en premier lieu par l'expérience, ou, comme on dit, « sur le tas ». C'est comme pour apprendre à conduire : personne ne saurait y parvenir simplement en lisant des manuels, en écoutant quelqu'un en parler ou en regardant les autres conduire. Il faut en faire l'expérience soi-même : il est nécessaire de se mettre au volant et de pratiquer, de préférence sous la supervision d'un instructeur qualifié. Il en va de même pour l'audit interne : on apprend par la pratique, sous le regard perspicace de superviseurs et mentors chevronnés.

Étant donné que les auditeurs internes doivent disposer d'un large éventail de compétences, les Instituts ont élaboré un Référentiel de compétences de l'audit interne. Ce référentiel peut aider les auditeurs internes et les fonctions d'audit interne à évaluer leurs

Copyright © 2015 Eyrolles.

niveaux de compétence actuels et à repérer les domaines dans lesquels ils doivent progresser. Il énonce le niveau minimum de connaissances et de compétences qui sont nécessaires dans quatre domaines pour que le travail soit efficace et que la fonction d'audit interne reste performante. L'encadré 1-6 présente ces quatre domaines et les qualités spécifiques recommandées pour chacun.

RÉFÉRENTIEL DE COMPÉTENCES DE L'AUDIT INTERNE

ENCADRÉ 1-6

1. Sens des relations humaines

a. Influence : déployer une tactique efficace pour convaincre.
b. Communication : envoyer des messages clairs et convaincants, savoir écouter.
c. Gestion :
   i. règles et procédures ;
   ii. effectif et compétence des auditeurs internes ;
   iii. définition des priorités, planification, gestion des performances et orientation sur les besoins des clients ;
   iv. gestion du temps, réalisation des objectifs et des tâches, talents d'organisation.
d. Leadership : inspirer et guider des groupes et des individus, susciter de la motivation au sein de l'organisation, esprit d'entreprise.
e. Catalyseur du changement : engager, gérer le changement et y faire face.
f. Gestion des conflits : négocier et régler les différends.
g. Collaboration et coopération : travailler avec d'autres personnes en vue de réaliser des objectifs communs.
h. Capacité à animer une équipe : créer une synergie de groupe pour la réalisation d'objectifs collectifs.

2. Outils et techniques

a. Requêtes pour les opérations et le management.
b. Prévisions.
c. Gestion de projets.
d. Analyse des processus opérationnels.
e. Tableaux de bord.
f. Techniques d'évaluation des risques et des contrôles (dont auto-évaluation).
g. Outils et techniques relatifs à la gouvernance, à la gestion des risques et au contrôle.
h. Outils et techniques de collecte et d'analyse de données.
i. Outils et techniques de résolution des problèmes.
j. Techniques d'audit informatisées (CAAT).

3. Normes d'audit interne, théorie et méthodologie

a. Définition de l'audit interne.
b. Code de déontologie.
c. *Normes internationales pour la pratique professionnelle de l'audit interne :*
   i. normes de qualification ;
   ii. normes de fonctionnement.

4. Domaines de compétence

a. Comptabilité financière et finance.
b. Comptabilité de gestion.
c. Réglementation, droit et économie.
d. Qualité : compréhension du cadre de référence qualitatif dans votre organisation.
e. Déontologie et fraude.
f. Systèmes d'information.
g. Gouvernance, gestion des risques et contrôle.
h. Théorie et comportement de l'organisation.
i. Connaissance du secteur.

Source : www.theiia.org

Copyright © 2015 Eyrolles.

À première vue, ce référentiel peut paraître lourd et fastidieux. Cependant, ces compétences ne sont pas obligatoires pour débuter à un poste d'audit interne, et elles peuvent être acquises au fil du temps. Il y a beaucoup de choses qu'un étudiant peut faire pour se préparer à son premier poste d'auditeur interne. Il peut acquérir certains niveaux de connaissance et de compétence par les moyens suivants :

- une formation en audit, comptabilité, systèmes d'information, risques opérationnels et contrôles, gestion, économie et finance, droit commercial ou méthodes quantitatives. Il est particulièrement intéressant d'avoir des connaissances dans plusieurs domaines plutôt que dans un seul. Les connaissances en audit et en systèmes d'information, par exemple, sont très demandées ;
- une expérience pratique des logiciels utiles à l'audit, comme ceux permettant l'établissement de diagrammes de flux, les tableurs, les bases de données et les logiciels d'audit généralisés ;
- un entraînement destiné à développer ses qualités de communication et son sens des relations humaines ;
- des projets permettant aux étudiants d'adopter une pensée analytique, d'assimiler rapidement de nouvelles informations, de réagir à une ambiguïté, de traiter des tâches pluridimensionnelles non structurées et de gérer efficacement plusieurs projets de front ;
- un apprentissage d'une ou plusieurs langues étrangères afin d'évoluer dans un contexte international.

Les références qu'un étudiant fait apparaître sur son curriculum vitae refléteront les connaissances et savoir-faire qu'il a acquis : un diplôme obtenu avec une bonne moyenne démontre la maîtrise d'une discipline ; un emploi occupé pendant ses études ou la participation à des activités extrascolaires souligne la capacité à gérer correctement plusieurs tâches à la fois. Les bourses et autres distinctions témoignent des réalisations d'un étudiant. Un stage est l'occasion de démontrer son aptitude à mettre en application ce que l'on a appris ; un poste à responsabilité dans une association d'étudiants indique une motivation et une aptitude à diriger ; l'obtention du CIA avant même celle du diplôme de l'école témoigne non seulement d'une compétence particulière pour l'audit interne et des sujets connexes, mais également d'une volonté de réussir.

Le passage du statut de simple membre de l'équipe d'audit interne à celui de chef de mission chevronné signale que la personne est prête à encadrer des subordonnés et à les faire profiter de son expérience, à faire des présentations et à animer des réunions, à faire preuve de persuasion dans la communication avec tous les échelons de la hiérarchie, à établir des relations durables avec les audités et les clients, et à encourager activement le changement. Les références qu'il faut présenter à ce stade d'une carrière d'auditeur

Copyright © 2015 Eyrolles.

interne peuvent inclure, par exemple, un historique de missions réussies, des témoignages d'audités et de clients (qui reconnaissent que cette personne « a de l'avenir »), un master en audit interne, diverses certifications professionnelles, et un poste d'encadrement parmi les bénévoles d'une organisation professionnelle, telle qu'un chapitre d'une ville américaine ou un Institut national.

Les professionnels de l'audit interne qui continuent de développer leurs compétences de gestion et de leadership peuvent poursuivre leur carrière dans la direction d'un service d'audit interne. Ils doivent être à même d'accompagner et d'encadrer des collaborateurs, d'aborder habilement les problèmes de gestion stratégique et d'inspirer du respect aux cadres supérieurs et à leurs collègues. À mesure qu'une personne est de plus en plus considérée comme un possible leader à venir de l'audit interne, elle sera vraisemblablement invitée à faire profiter de ses compétences, par exemple en agissant comme bénévole à un niveau international, en faisant des communications lors de réunions d'associations professionnelles ou de conférences, ou en rédigeant des articles pour des revues spécialisées.

LES CARRIÈRES DANS L'AUDIT INTERNE

Accès à l'audit interne

Jusqu'à une date très récente, dans les pays anglo-saxons essentiellement, la plupart des auditeurs internes commençaient leur carrière dans l'audit comptable. En général, dans ces pays, un diplômé en comptabilité commence en tant qu'auditeur des états financiers dans un cabinet, puis, quand il a acquis de l'expérience, il passe à un poste d'auditeur interne, le plus souvent auprès d'anciens clients. Si cette trajectoire reste reconnue, elle n'est certainement pas unique.

Depuis quelques années, on embauche de plus en plus souvent directement des auditeurs internes parmi les jeunes diplômés. Les sociétés cotées et non cotées, les entités publiques, les organisations à but non lucratif et les organisations qui délivrent des services d'audit interne recrutent régulièrement des auditeurs internes à leur sortie d'école ou d'université. Toujours plus nombreuses, les grandes écoles et universités qui proposent un cursus d'audit interne établi en partenariat avec les Instituts gagnent en popularité parmi les recruteurs. Les meilleurs de leurs étudiants, munis d'un diplôme en comptabilité, systèmes d'information ou dans une autre discipline liée ou non à l'entreprise, sont très demandés. Pour ceux qui ont effectué un ou plusieurs stages liés à l'audit interne, l'expérience du monde réel constitue un véritable atout.

Copyright © 2015 Eyrolles.

Responsable de l'audit interne

Désigne une personne, occupant un poste hiérarchique de haut niveau, qui a la responsabilité de gérer l'activité d'audit interne.

De nombreuses organisations estiment que l'audit interne est une composante importante de leur programme de formation en gestion parce qu'il offre aux hauts potentiels une occasion unique d'acquérir une expérience en gouvernance, gestion des risques et contrôle portant sur de nombreux domaines de l'organisation. Dans ces organisations, les éventuels futurs managers de différents services doivent passer un certain temps dans la fonction d'audit interne avant de pouvoir progresser dans la hiérarchie.

Après l'audit interne

Une grande majorité de ceux qui choisissent l'audit interne n'y passent pas l'ensemble de leur carrière. Comme indiqué ci-dessus, l'audit interne constitue un excellent terrain de formation pour les personnes aspirant à des postes d'encadrement supérieur. Beaucoup d'auditeurs internes utilisent l'expertise qu'ils ont acquise dans l'audit interne comme un tremplin vers des positions de responsabilité dans les domaines financiers ou opérationnels, que ce soit dans l'organisation dans laquelle ils ont travaillé jusque-là ou ailleurs.

Il y a quelques années, aucun auditeur interne n'imaginait pouvoir trouver un nouveau poste dans une société de prestation de services d'assurance et de conseil. C'est aujourd'hui une voie possible, surtout pour les personnes disposant d'une spécialisation très appréciée dans une branche particulière (comme l'énergie ou la banque) ou un domaine (par exemple les systèmes d'information, ou la prévention, la dissuasion et la détection de la fraude).

Carrières dans l'audit interne

Cependant, certaines personnes, peu nombreuses au demeurant, choisissent de faire toute leur carrière dans l'audit interne. Plusieurs options s'offrent à elles. La première consiste à gravir les échelons de la fonction d'audit interne d'une seule et même organisation jusqu'à la direction de l'audit interne. Une autre option consiste à rester dans l'audit interne, mais à progresser dans la hiérarchie en passant d'une organisation à l'autre. La troisième solution est de progresser entre les différents niveaux d'une société de prestation de services d'assurance et de conseil aux professionnels.

L'objectif ultime d'une carrière d'auditeur interne est d'être responsable de l'audit interne. Très respecté au sein de l'organisation, il est le plus souvent cadre supérieur. Il interagit avec les personnes au sommet de la direction générale et avec le Conseil. Il est souvent rattaché hiérarchiquement au directeur général et fonctionnellement au comité d'audit. Le chapitre 9, *La gestion de l'audit*

Copyright © 2015 Eyrolles.

interne, détaille les rôles et responsabilités du responsable de l'audit interne.

Dans un cabinet qui propose des services d'audit interne à de nombreuses autres organisations, un auditeur interne peut s'élever au rang d'associé ou atteindre une position tout aussi prestigieuse. Contrairement aux responsables de l'audit interne d'une organisation, il interagit avec l'encadrement supérieur et le Conseil de plusieurs organisations et leur est subordonné.

Quelle que soit la carrière choisie, les auditeurs internes voient aujourd'hui s'offrir à eux beaucoup plus d'opportunités qu'il y a encore quelques années. Ceux qui développent un large éventail de compétences et acquièrent de l'expérience dans différents domaines seront bien placés pour envisager des voies très diverses.

RÉSUMÉ

Ce premier chapitre a présenté l'audit interne comme une profession de premier plan, avec une proposition de valeur claire pour les principales parties prenantes. Il a défini l'audit interne et ébauché le processus d'audit interne. Il a souligné la différence entre les activités d'assurance menées, dans le cadre des audits financiers, par un auditeur interne et par un commissaire aux comptes. Il a également décrit la profession d'audit interne et le réseau des Instituts d'audit interne. Enfin, il a mis en exergue les compétences nécessaires pour réussir en tant qu'auditeur interne, ainsi que les différentes voies envisageables.

Ce manuel traite à la fois des concepts nécessaires à la compréhension de l'audit interne, ainsi que des étapes de la réalisation des missions d'audit interne. Les 11 premiers chapitres forment la section consacrée aux concepts fondamentaux de l'audit interne. Ces chapitres traitent exclusivement de ces concepts, que les auditeurs internes doivent connaître et comprendre. Cependant, une bonne maîtrise de ces concepts est nécessaire, mais pas suffisante pour comprendre l'audit interne. Les quatre derniers chapitres constituent la section du manuel qui décrit la réalisation des missions d'audit interne. Ces chapitres sont centrés sur les étapes requises pour planifier les missions d'assurance et de conseil, pour les mener à bien et pour en communiquer les résultats. Enfin, les études de cas qui accompagnent le manuel développent les concepts et les étapes présentés tout au long de cet ouvrage. On peut les utiliser à titre d'exercice.

Copyright © 2015 Eyrolles.

Questions de révision

1. Quelles sont les trois composantes de la proposition de valeur de l'audit interne établie par l'IIA ?

2. Comment les Instituts définissent-ils l'audit interne ?

3. D'après le COSO, quelles sont les quatre catégories d'objectifs d'une organisation ?

4. Comment la gouvernance, la gestion des risques et le contrôle sont-ils définis dans ce chapitre ?

5. Quelle est la différence entre les activités d'assurance internes et les activités de conseil internes ?

6. Quelle est la différence entre les concepts d'indépendance et d'objectivité qui s'appliquent aux auditeurs internes ?

7. Quelles sont les trois phases fondamentales du processus d'audit interne ?

8. Quelle est la relation entre l'audit et la comptabilité ?

9. Quelle est la principale différence entre les activités d'assurance internes et externes menées dans le cadre des audits financiers ?

10. Énumérez quelques-uns des facteurs qui ont alimenté l'expansion spectaculaire de la demande de services d'audit interne ces 30 dernières années.

11. Quels types de procédures un auditeur interne pourrait-il utiliser pour tester l'adéquation de la conception et le fonctionnement effectif des processus de gouvernance, de gestion des risques et de contrôle ?

12. Qu'est-ce que le co-sourcing ? Pourquoi une organisation choisit-elle le co-sourcing pour sa fonction d'audit interne ?

13. Comment l'IIA est-il organisé ?

14. Quelles sont les deux catégories de dispositions figurant dans le CRIPP ?

15. Quelles sont les trois parties de l'examen du CIA ?

16. Quel est le principal objectif de la Fondation au sein de l'IIA pour la recherche ?

17. Quelles sont les sept qualités personnelles communes aux auditeurs internes qui réussissent et qui sont énumérées dans ce chapitre ?

Copyright © 2015 Eyrolles.

Questions de révision

18. Pourquoi est-il impératif que les auditeurs internes soient intègres ?

19. Quels sont les quatre domaines présentés dans le Référentiel de compétences de l'audit interne ?

20. Quelles sont les trois principales voies permettant d'entrer dans la profession d'audit interne ?

21. Est-ce que la plupart des personnes qui travaillent dans l'audit interne y passent la totalité de leur carrière ? Expliquez pourquoi.

22. Quelles options s'offrent à une personne qui souhaite faire carrière dans l'audit interne ?

Copyright © 2015 Eyrolles.

Questions à choix multiples

Sélectionnez la meilleure réponse pour chacune des questions suivantes.

1. Le nouveau directeur financier de l'organisation AVF demande à rencontrer le responsable de l'audit interne pour discuter du rôle de la fonction d'audit interne. Le responsable de l'audit interne doit l'informer de la responsabilité globale de l'audit interne, à savoir :
   a. agir en tant que prestataire de conseil et d'assurance indépendant, source de valeur ajoutée et d'amélioration pour le fonctionnement de l'organisation ;
   b. évaluer les méthodes qu'utilise l'organisation pour préserver ses actifs et, le cas échéant, vérifier l'existence des actifs ;
   c. vérifier l'intégrité de l'information financière et opérationnelle, et examiner les méthodes employées pour recueillir des informations et établir des rapports ;
   d. déterminer si le système de contrôle interne de l'organisation permet de donner une assurance raisonnable que les informations sont communiquées au management avec efficacité et efficience.

2. Laquelle des affirmations suivantes concernant les objectifs de l'organisation est fausse ?
   a. Les objectifs de l'organisation représentent des cibles de performance.
   b. La définition d'objectifs significatifs de l'organisation est un prérequis pour que le contrôle interne soit efficace.
   c. La définition d'objectifs significatifs de l'organisation est une composante clé du processus de gestion.
   d. Les objectifs de l'organisation sont les moyens dont dispose le management pour employer les ressources et assigner les responsabilités.

3. Dans le contexte de l'audit interne, la meilleure définition des activités d'assurance est la suivante :
   a. Examens objectifs de preuves dans l'optique d'une évaluation indépendante.
   b. Activités de conseil visant à créer de la valeur ajoutée et à améliorer le fonctionnement d'une organisation.
   c. Activités professionnelles qui mesurent et communiquent des données financières et professionnelles.
   d. Évaluations objectives de la conformité aux règles, plans, procédures, lois et règlements.

4. Les auditeurs internes doivent avoir le sens des relations humaines. Laquelle des compétences suivantes ne témoigne pas du sens des relations humaines ?
   a. La communication.
   b. Le leadership.
   c. La gestion de projets.
   d. La capacité à travailler en équipe.

Copyright © 2015 Eyrolles.

Questions à choix multiples

5. Lorsqu'ils planifient un audit interne, les auditeurs internes acquièrent des connaissances sur l'audité afin, notamment, de :
   a. Faire preuve de scepticisme vis-à-vis des critères de qualité retenus par le management.
   b. Comprendre les objectifs de l'audité et les risques associés.
   c. Formuler des suggestions constructives à l'intention du management concernant des améliorations à apporter au contrôle interne.
   d. Déterminer si des erreurs dans les rapports d'évaluation de l'audité doivent être notifiées à la direction générale et au comité d'audit.

Copyright © 2015 Eyrolles.

Thèmes de discussion

1. Définissez la « proposition de valeur ». Expliquez pourquoi il est important que l'audit interne en ait une. Décrivez les trois composantes de la proposition de valeur de l'audit interne établie par l'IIA.

2. Décrivez la relation qui existe entre objectifs et stratégies. Quel est votre principal objectif ? Expliquez votre stratégie pour atteindre cet objectif.

3. Ina Icandoit a un cours tous les jours à 8 h. Le professeur a fait comprendre à ses élèves qu'il était important d'arriver à l'heure en cours. Ina en a fait l'un de ses objectifs pour le semestre. Quels risques menacent la réalisation de l'objectif d'Ina ? Quels contrôles Ina peut-elle mettre en œuvre pour maîtriser ces risques ?

4. Prim Rose possède cinq magasins de fleurs dans la banlieue d'une grande ville. Chaque magasin est géré par une personne différente. L'un des tests effectués par Prim pour suivre les performances de ses magasins consiste en une simple analyse de l'évolution du chiffre d'affaires en glissement mensuel pour chaque magasin. Supposons que l'analyse des performances communiquée pour l'une de ses boutiques fasse apparaître que le chiffre d'affaires mensuel est resté à peu près constant de janvier à juin. Est-ce que ces performances sur six mois doivent être source de satisfaction ou d'inquiétude pour Prim ? Expliquez.

5. Développez :
   a. les qualités personnelles nécessaires pour réussir dans l'audit interne ;
   b. les connaissances, compétences et références attendues d'un auditeur interne débutant ;
   c. les connaissances, compétences et références supplémentaires attendues d'un chef de mission ;
   d. les connaissances, compétences et références supplémentaires attendues d'un responsable de l'audit interne.

Copyright © 2015 Eyrolles.

ÉTUDES DE CAS



Rendez-vous sur le site Internet de l'IIA ou de tout autre Institut francophone. Localisez, imprimez, lisez et préparez des arguments pour traiter des sujets suivants :

1. Les questions les plus fréquemment posées à propos de l'audit interne.
2. Quelles sont les différences entre les auditeurs internes et externes, et comment ces deux catégories entrent-elles en relation ?
3. Comment l'audit interne préserve-t-il son indépendance et son objectivité ?
4. Est-il obligatoire d'avoir une activité d'audit interne ?
5. Quelles sont les compétences et les qualités essentielles du responsable de l'audit interne ?
6. Quels sont les compétences et l'effectif prévisionnel de l'audit interne ?
7. Quel est le rôle de l'audit interne dans la prévention, la détection et l'investigation des fraudes ?
8. Quels services l'audit interne peut-il proposer au comité d'audit ?
9. À qui le responsable de l'audit interne doit-il rendre compte ?
10. Quelles normes guident le travail des professionnels de l'audit interne ?
11. Pourquoi une organisation doit-elle avoir un comité d'audit ?
12. Le descriptif du contenu des trois parties de l'examen du CIA.

Copyright © 2015 Eyrolles.



Copyright © 2015 Eyrolles.



Copyright © 2015 Eyrolles.

CHAPITRE 2
LE CADRE DE RÉFÉRENCE INTERNATIONAL DES PRATIQUES PROFESSIONNELLES : DES LIGNES DIRECTRICES INCONTOURNABLES POUR L'AUDIT INTERNE

Objectifs pédagogiques

- Connaître l'histoire qui a conduit à l'adoption de lignes directrices professionnelles pour la pratique de l'audit interne.
- Décrire la structure du Cadre de référence international des pratiques professionnelles (CRIPP) de l'audit interne et les différents types de lignes directrices qu'il établit.
- Comprendre la relation entre le CRIPP et la proposition de valeur de l'audit interne pour les parties prenantes.
- Comprendre les dispositions obligatoires du CRIPP : la définition de l'audit interne, le Code de déontologie et les *Normes internationales pour la pratique professionnelle de l'audit interne*.
- Comprendre les dispositions fortement recommandées du CRIPP : les Modalités Pratiques d'Application, les prises de position et les guides pratiques.
- Décrire le processus d'actualisation du CRIPP.
- Comprendre en quoi les lignes directrices publiées par d'autres organisations professionnelles influencent la pratique de l'audit interne.

La stature et la réputation d'une profession peuvent s'évaluer, dans une large mesure, à l'aune de la rigueur de sa déontologie et de ses pratiques. Il en va ainsi, notamment, du corps médical, des ingénieurs, des professionnels du droit ou des experts-comptables. Et cela vaut aussi pour les professionnels de l'audit interne.

Ce chapitre explique en quoi les lignes directrices émises par l'*Institute of Internal Auditors* (IIA), traduites en français par l'IFACI, répondent à des questions telles que :

- Que peuvent attendre les parties prenantes des activités d'audit interne ?
- Quelles sont les conditions nécessaires à la réussite de l'audit interne ?

- Quelles sont les qualités requises pour être un bon auditeur interne ?
- Quelles responsabilités le responsable de l'audit interne endosse-t-il ?
- Comment le Conseil et la direction générale évaluent-ils les activités d'audit interne ?
- En bref, comment l'audit interne crée-t-il de la valeur ajoutée ?

Selon la définition de l'audit interne donnée au chapitre 1, *Introduction à l'audit interne*, l'audit interne est « … une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée ». Les auditeurs internes délivrent ces services à un ensemble varié d'organisations, qui va des sociétés cotées et non cotées au secteur public ou aux entités à but non lucratif. Au sein de ces organisations, l'audit interne interagit avec diverses parties prenantes, qui ont chacune leurs besoins et leurs exigences propres. Ces parties prenantes sont des instances internes, comme le conseil d'administration ou de surveillance* (*via* le comité d'audit) d'une organisation, la direction générale, le management, ainsi que des acteurs externes, comme les investisseurs, les créanciers, les autorités de régulation et de supervision, les fournisseurs et les clients. Ce chapitre explique comment les lignes directrices à l'intention de la profession permettent aux auditeurs internes de fournir des services à valeur ajoutée en répondant aux besoins de ce large éventail de parties prenantes.

IIA (*Institute of Internal Auditors*)

Organisme dont le siège se situe à Altamonte Springs (Floride) et qui est reconnu dans le monde entier comme le leader de la certification, de l'enseignement, de la recherche et des orientations technologiques pour la profession d'audit interne.

Ce chapitre commence par un historique des lignes directrices destinées à la pratique professionnelle de l'audit interne, depuis la création de l'IIA, en 1941. Il présente ensuite le CRIPP (Cadre de référence international des pratiques professionnelles), qui reflète la nature mondiale de la profession d'audit interne, et détaille les dispositions obligatoires et les dispositions fortement recommandées du cadre. Puis, ce chapitre décrit comment ces lignes directrices sont élaborées et publiées. Enfin, il explique comment les lignes directrices publiées par d'autres organisations professionnelles influencent la pratique de l'audit interne.

HISTORIQUE DES LIGNES DIRECTRICES À L'INTENTION DES PROFESSIONNELS DE L'AUDIT INTERNE

La pratique de l'audit interne s'est développée sur une longue période. Lorsque les organisations ont commencé à s'étendre et à

* NdT : Dans la suite du texte, le terme « Conseil » sera utilisé pour désigner le conseil d'administration ou de surveillance.

Copyright © 2015 Eyrolles.

devenir plus complexes, et aussi géographiquement plus dispersées, leurs dirigeants n'ont pas pu continuer à surveiller personnellement les opérations dont ils étaient responsables ni entretenir suffisamment de contacts directs avec tous leurs subordonnés. Cette distanciation de la direction générale par rapport aux opérations dont elle était responsable a rendu nécessaire l'émergence d'autres acteurs de l'organisation qui l'aident à examiner les opérations et à établir des rapports sur la base de ces examens. Pour apporter cette aide, ces personnes ont commencé à mener des activités d'audit interne. Au fil du temps, ces activités ont été davantage formalisées et, avec la création de l'IIA aux États-Unis, la pratique de l'audit interne a commencé à se constituer en profession. Les praticiens se sont progressivement entendus sur le rôle, ainsi que sur les concepts et pratiques génériques de l'audit interne.

Peu après la formation de l'IIA, les premières lignes directrices à l'intention de la profession d'auditeur interne ont été élaborées. Le premier texte officiel encadrant les pratiques des auditeurs, le *Statement of the Responsibilities of the Internal Auditor* (Énoncé des responsabilités de l'auditeur interne), a été publié en 1947. Ce bref document définissait les objectifs et le périmètre de l'audit interne. À mesure que la profession a évolué, ses révisions successives ont tenu compte de l'élargissement du périmètre d'intervention de la profession. Ainsi, si la version initiale de 1947 s'attachait essentiellement aux audits financiers, celle de 1957 a été élargie à d'autres domaines.[1] Au fil des ans, le périmètre des activités de l'audit interne a continué de s'étendre à mesure que la profession évoluait, et ce *Statement of Responsibilities* a été révisé en conséquence, en 1971, 1976, 1981 et en 1990.

En 1968, l'IIA a établi des lignes directrices d'ordre éthique à l'intention de ses membres en publiant un Code de déontologie. Ce code se composait de huit articles dont les principes fondamentaux se retrouvent encore dans sa version actuelle. L'IIA a également précisé les compétences (c'est-à-dire les connaissances et le savoir-faire) que devaient posséder les professionnels de l'audit interne avec la publication du *Common Body of Knowledge* (CBOK, socle commun de connaissances), en 1972, et la mise en œuvre du programme de certification de *Certified Internal Auditor* (CIA) en 1973. Enfin, en 1978, l'IIA a publié *Les Normes pour la pratique professionnelle de l'audit interne* (les Normes de 1978). Celles-ci se composaient de cinq règles générales et de 25 directives spécifiques sur la manière de gérer l'audit interne et d'exécuter les missions d'audit. Ces normes ont été largement adoptées et traduites dans plusieurs langues par les Instituts nationaux dont l'IFACI. Elles ont, de plus, été souvent incorporées aux lois et règlements de différentes entités publiques.

Les *Normes* de 1978 se sont révélées suffisamment solides pour accompagner l'évolution de la profession, et sont restées pratiquement inchangées pendant les 20 années qui ont suivi leur

Copyright © 2015 Eyrolles.

publication. Cependant, pour faciliter l'interprétation de ces normes, l'IIA a publié des documents supplémentaires :

- des règles accompagnant les *Normes* de 1978 ;
- les *Professional Standards Practice Releases* – communiquant la réponse de l'IIA à des questions fréquemment posées ;
- des prises de position de l'IIA ;
- des études.

À la fin des années 1990, parmi les diverses formes de lignes directrices, on ne savait plus quelles règles primaient sur les autres et on a relevé des contradictions entre certaines d'entre elles.

De plus, la profession d'audit interne avait commencé à changer dans les années 1980. Le recours à l'évaluation des risques comme méthode d'affectation des ressources (approche par les risques) a rapidement gagné en popularité. Dans les années 1990, des organisations se sont mises à sous-traiter les activités d'audit interne auprès de prestataires externes. Le temps consacré aux activités traditionnelles d'audit a été spectaculairement révisé à la baisse, tandis que l'on se consacrait de plus en plus à l'efficacité et à l'efficience des opérations. Aux États-Unis en particulier, des prestations d'audit interne non traditionnelles, comme les programmes d'auto-évaluation du contrôle interne, les formations sur le contrôle interne, les conseils concernant les projets de mise en œuvre de systèmes, ainsi que les autres activités de conseil, se sont mises à absorber une part croissante des ressources d'audit interne. Les *Normes* de 1978 n'étaient pas adaptées à ce nouvel environnement.

Reconnaissant le rôle important du *Statement of Responsibilities*, du Code de déontologie et surtout des *Normes* de 1978 dans l'évolution de cette profession internationale qu'était devenu l'audit interne, l'Institut a mis en place, en 1997, un groupe de travail (*Guidance Task Force*) chargé d'étudier les besoins et les mécanismes de communication des orientations pour l'avenir. Après plus d'un an de travaux, ce groupe a présenté son rapport, intitulé *A Vision for the Future: Professional Practices Framework for Internal Auditing* (« Une vision pour l'avenir : le Cadre de Référence des Pratiques Professionnelles de l'audit interne »). Ce rapport proposait une nouvelle définition de l'audit interne, destinée à remplacer celle contenue dans le *Statement of Responsibilities*, ainsi qu'une nouvelle structure permettant de communiquer rapidement des orientations pertinentes pour la profession. Cette nouvelle définition et cette structure ont été adoptées en 1999. Leur application a commencé avec la révision du Code de déontologie en 2000 et l'achèvement de la rédaction des nouvelles *Normes internationales pour la pratique professionnelle de l'audit interne* (les *Normes*) en 2002.

En 2006, les *Normes* étaient adoptées au plan mondial, avec des traductions autorisées dans 32 langues. En outre, de plus en plus de

Copyright © 2015 Eyrolles.

pays et de juridictions sur la planète ont intégré les *Normes* dans des textes de loi et des règlements. Étant donné le statut et la reconnaissance grandissants de ces lignes directrices, les Instituts ont ressenti le besoin de s'assurer qu'elles étaient claires, d'actualité, pertinentes et cohérentes à l'échelle internationale. Le processus de leur élaboration devait également être suffisamment réactif aux besoins de la profession et d'une transparence qui convienne aux parties prenantes. Un groupe de travail et un comité de pilotage ont été mis en place dans l'optique de réviser la structure des lignes directrices existantes, ainsi que leur processus d'élaboration, de révision et de publication. Cette révision a donné lieu à un nouveau Cadre de référence international des pratiques professionnelles (CRIPP) et à la réorganisation du processus d'élaboration des lignes directrices. Un nouveau groupe, le conseil de surveillance du CRIPP (*IPPF Oversight Council*), composé essentiellement de parties prenantes extérieures, a également été créé, avec pour mission de superviser la définition des lignes directrices incontournables.

LE CADRE DE RÉFÉRENCE INTERNATIONAL DES PRATIQUES PROFESSIONNELLES

Les composantes du CRIPP sont présentées dans l'encadré 2-1. Seul cadre de référence reconnu partout dans le monde pour la profession d'audit interne, le CRIPP renferme des éléments jugés essentiels dès lors que l'on veut exécuter des activités d'audit interne. Il décrit les compétences dont doivent disposer les auditeurs internes, les caractéristiques du service qui effectue ces activités, la nature des missions d'audit interne et les critères de qualité permettant de mesurer la performance de ces activités. Le CRIPP offre donc des lignes directrices à la profession et définit les attentes des parties prenantes vis-à-vis de la réalisation des activités d'audit interne.

Le CRIPP comporte à la fois des dispositions obligatoires (définition de l'audit interne, Code de déontologie et *Normes*) et des dispositions fortement recommandées (Modalités Pratiques d'Application, prises de position et guides pratiques). Le respect des dispositions obligatoires est jugé fondamental. L'élaboration de ces dispositions suit un processus rigoureux, qui compte notamment une période de consultation publique. Les dispositions fortement recommandées décrivent les pratiques qui sous-tendent une mise en œuvre efficace des principes énoncés dans la définition, le Code de déontologie et les *Normes*. L'ensemble des Instituts d'audit interne approuve ces dispositions et incite vivement les parties prenantes à les respecter, tout en reconnaissant qu'il peut exister d'autres pratiques efficaces. Le processus d'élaboration des dispositions fortement recommandées est, lui, moins long, moins contraignant et plus rapide, car, dans la mesure où il ne s'agit pas de dispositions obligatoires, elles peuvent faire l'objet d'une période de consultation moins longue par les parties prenantes.

Cadre de référence international des pratiques professionnelles (CRIPP)

Seules lignes directrices reconnues partout dans le monde pour la profession d'audit interne. Le CRIPP est téléchargeable sur le site de l'IIA (www.theiia.org) et sur le site des Instituts nationaux tels que l'IFACI (www.ifaci.com).

Copyright © 2015 Eyrolles.

Le CRIPP englobe la totalité des lignes directrices de l'audit interne publiées par l'IIA et en facilite l'accès pour les professionnels de l'audit interne du monde entier. Il constitue le fondement qui permet à l'audit interne d'exercer ses fonctions et d'assumer efficacement ses responsabilités. Reflet de la nature mondiale de la profession d'audit interne, le CRIPP est accepté dans la plupart des pays, grâce aux traductions officielles de la définition de l'audit interne, du Code de déontologie et des *Normes* réalisées par les Instituts nationaux dans plus de 25 langues.

ENCADRÉ 2-1

LE CADRE DE RÉFÉRENCE INTERNATIONAL DES PRATIQUES PROFESSIONNELLES



Source : www.global.theiia.org

Copyright © 2015 Eyrolles.

DISPOSITIONS OBLIGATOIRES

La définition

Le CRIPP donne la définition suivante de l'audit interne :

> *L'audit interne est une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée. Il aide cette organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle, et de gouvernement d'entreprise, et en faisant des propositions pour renforcer leur efficacité.*

Cette définition souligne que l'objectif ultime de l'audit interne en général, et de chaque auditeur interne en particulier, est de créer de la valeur ajoutée pour l'organisation au moyen d'activités d'assurance et de conseil. Plus particulièrement, ces activités permettent de créer de la valeur ajoutée grâce à l'évaluation et l'amélioration de l'efficacité des processus de gestion des risques, de contrôle et de gouvernance de l'organisation. Pour la plupart des organisations, la création de valeur ajoutée n'est évidemment pas une option. Le management exige de toutes les fonctions de l'organisation qu'elles créent de la valeur ajoutée avec transparence. En énonçant expressément que l'audit interne contribue à créer de la valeur ajoutée et apporte ses conseils pour améliorer ces processus, la définition ci-dessus met l'accent sur l'engagement de la profession à répondre aux besoins de l'organisation.

Toutefois, étant donné que, par leur nature, les activités de l'audit interne n'ont pas un impact aussi direct que celles des autres fonctions de l'organisation sur les résultats, l'audit interne doit être capable d'expliquer clairement au management et aux autres parties prenantes comment il crée de la valeur ajoutée. Pour ce faire, l'IIA a élaboré une illustration représentant la proposition de valeur de l'audit interne (encadré 2-2 en page suivante). Cette illustration décrit de manière succincte comment les concepts contenus dans la définition de l'audit interne s'associent pour créer de la valeur ajoutée.

La référence faite à l'indépendance et à l'objectivité, ainsi qu'à l'approche systématique et méthodique adoptée par la profession, forme la base des activités d'audit interne. Ces éléments sont détaillés dans les composantes du CRIPP.

Le Code de déontologie

Le Code de déontologie a pour objectif déclaré de promouvoir une culture de l'éthique dans la profession d'audit interne. Il comporte

Copyright © 2015 Eyrolles.

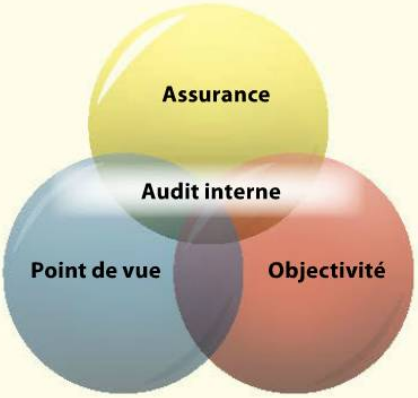
ENCADRÉ 2-2

LA VALEUR DE L'AUDIT INTERNE POUR LES PARTIES PRENANTES

En tant qu'organisation, vous savez qu'il est essentiel de mettre en place une gouvernance, un système de gestion des risques et des dispositifs de contrôle interne efficaces pour assurer la réussite et la pérennité de l'organisation. L'audit interne aide la direction générale et l'organe de gouvernance (par exemple le Conseil, le comité d'audit, les entités publiques) à s'acquitter de leurs responsabilités, en évaluant, par une approche systématique et méthodique, l'efficacité du système de contrôle interne et des processus de gestion des risques en termes de conception et d'exécution.

Qu'êtes-vous en droit d'attendre de votre service d'audit interne ?

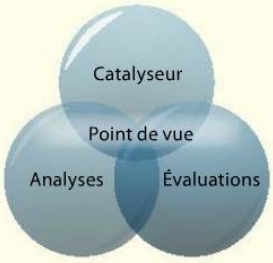
Quelles sont les caractéristiques d'un service d'audit interne mature ? Quelle valeur unique l'audit interne apporte-t-il spécifiquement aux parties prenantes ? Votre service d'audit interne est-il à la hauteur de vos attentes ?



Audit interne = Assurance, point de vue et objectivité

Les organes de gouvernance et la direction générale comptent sur l'audit interne pour donner une assurance et un point de vue objectifs sur l'efficacité et l'efficience des processus de gouvernance, de gestion des risques et de contrôle interne.







Assurance = Gouvernance, gestion des risques et contrôle

L'audit interne donne une assurance sur les processus de gouvernance, de gestion des risques et de contrôle de l'organisation, afin d'aider cette dernière à atteindre ses objectifs liés à la stratégie, aux opérations, au reporting et à la conformité.

Point de vue = Catalyseur, analyses et évaluations

L'audit interne agit comme un catalyseur permettant d'améliorer l'efficacité et l'efficience d'une organisation, grâce à un point de vue et des recommandations fondés sur des analyses et des évaluations des informations et des processus opérationnels.

Objectivité = Intégrité, devoir de rendre compte et indépendance

En faisant preuve d'intégrité et en assumant son devoir de rendre compte, l'audit interne crée de la valeur ajoutée pour les organes de gouvernance et la direction générale, car il constitue une source de conseils objective et indépendante.

Mautz, R. K. et Hussein A. Sharaf, *The Philosophy of Auditing* (Sarasota, Floride : *American Accounting Association*, 1961, p. 14).

Copyright © 2015 Eyrolles.

deux volets : des principes fondamentaux et des règles de conduite. Il va au-delà de la définition de l'audit interne, en précisant les compétences et les comportements indispensables chez toute personne exerçant des activités d'audit interne.

Les principes fondamentaux expriment quatre idéaux que les professionnels de l'audit interne doivent chercher à préserver lorsqu'ils mènent leurs travaux et qui représentent des valeurs clés auxquelles les auditeurs internes doivent se tenir s'ils veulent gagner la confiance de ceux qui se fient à leurs services. Les règles de conduite décrivent douze normes comportementales auxquelles les auditeurs internes doivent se conformer pour mettre en œuvre ces principes. Les points de vue peuvent certes diverger sur le fait que telle ou telle mission d'audit interne sera plus avantageusement exécutée par des prestataires internes ou externes, mais il est difficile d'imaginer que les professionnels de l'audit interne puissent s'écarter des quatre principes et douze règles de conduite décrits ci-après.

Intégrité — D'après le Code de déontologie, « l'intégrité des auditeurs internes est à la base de la confiance et de la crédibilité accordées à leur jugement ».

Intégrité

Qualité à la base de la confiance et de la crédibilité accordées au jugement des auditeurs internes.

Les règles de conduite associées au principe d'intégrité énoncent que « les auditeurs internes :

- doivent accomplir leur mission avec honnêteté, diligence et responsabilité ;
- doivent respecter la loi et faire les révélations requises par les lois et les règles de la profession ;
- ne doivent pas sciemment prendre part à des activités illégales ou s'engager dans des actes déshonorants pour la profession d'audit interne ou leur organisation ;
- doivent respecter et contribuer aux objectifs éthiques et légitimes de leur organisation ».

L'intégrité correspond au « droit d'entrée » des auditeurs internes. Elle est si fondamentale que, sans elle, il est impossible d'exercer la profession d'audit interne. En effet, quelle confiance une partie prenante pourrait-elle accorder à un rapport d'audit interne qui contiendrait des affirmations intentionnellement erronées ou trompeuses ? Ou encore, une partie prenante serait-elle rassurée si un auditeur interne avait été licencié de son précédent emploi pour avoir fraudé ? Les auditeurs internes doivent se conformer aux valeurs éthiques de l'organisation afin de gagner la confiance et le respect nécessaires pour s'acquitter de leurs responsabilités professionnelles.

Objectivité

Les auditeurs internes ne se laissent pas influencer dans leur jugement par leurs propres intérêts ou par autrui.

Objectivité – Le Code de déontologie requiert que « les auditeurs internes montrent le plus haut degré d'objectivité professionnelle

Copyright © 2015 Eyrolles.

en collectant, évaluant et communiquant les informations relatives à l'activité ou au processus examiné. Les auditeurs internes évaluent de manière équitable tous les éléments pertinents et ne se laissent pas influencer dans leur jugement par leurs propres intérêts ou par autrui. »

Les règles de conduite associées au principe d'objectivité énoncent que « les auditeurs internes :

- ne doivent pas prendre part à des activités ou établir des relations qui pourraient compromettre ou risquer de compromettre le caractère impartial de leur jugement. Ce principe vaut également pour les activités ou relations d'affaires qui pourraient entrer en conflit avec les intérêts de leur organisation ;
- ne doivent rien accepter qui pourrait compromettre ou risquer de compromettre leur jugement professionnel ;
- doivent révéler tous les faits matériels dont ils ont connaissance et qui, s'ils n'étaient pas révélés, auraient pour conséquence de fausser le rapport sur les activités examinées ».

L'objectivité est une qualité fondamentale de l'audit interne. Lorsqu'ils réalisent leurs travaux, il est impératif que les auditeurs internes soient conscients des menaces potentielles qui pèsent sur leur objectivité, comme leurs relations personnelles ou les conflits d'intérêts. Ainsi, accepter des cadeaux de la part des audités, auditer une entité dans laquelle travaille son conjoint ou s'entendre avec le manager de la division pour être muté dans la division examinée à la fin de l'audit, serait perçu comme une atteinte à l'objectivité de l'auditeur interne. De surcroît, les auditeurs internes doivent être objectifs dans leurs communications et éviter les formulations trompeuses. Par exemple, il est inadéquat d'affirmer que les contrôles sur les stocks présentent le même niveau d'efficacité que lors du dernier audit, en omettant de préciser que lors du dernier audit, on avait jugé que les activités de contrôle n'étaient pas satisfaisantes.

Confidentialité – Le Code de déontologie exige en outre que « les auditeurs internes respectent la valeur et la propriété des informations qu'ils reçoivent ; ils ne divulguent ces informations qu'avec les autorisations requises, à moins qu'une obligation légale ou professionnelle ne les oblige à le faire ».

Confidentialité

Les auditeurs internes ne divulguent les informations qu'ils reçoivent qu'avec les autorisations requises, à moins qu'une obligation légale ou professionnelle ne les oblige à le faire.

Les règles de conduite associées au principe de confidentialité énoncent que « les auditeurs internes :

- doivent utiliser avec prudence et protéger les informations recueillies dans le cadre de leurs activités ;
- ne doivent pas utiliser ces informations pour en retirer un bénéfice personnel, ou d'une manière qui contreviendrait aux dispositions légales ou porterait préjudice aux objectifs éthiques et légitimes de leur organisation ».

Copyright © 2015 Eyrolles.

Pour réaliser ses travaux, l'auditeur interne a besoin d'un accès illimité à toutes les données pertinentes. Pour lui accorder cet accès, le management doit pouvoir être certain que l'auditeur interne ne communiquera pas ou n'utilisera pas ces données d'une façon qui nuise à l'organisation, viole la législation ou la réglementation ou qui se traduise par des gains personnels. De même, l'auditeur interne doit protéger les données en sa possession et veiller à ce que les informations confidentielles ne soient pas divulguées par inadvertance à des parties qui ne doivent pas en avoir connaissance. Ainsi, l'auditeur doit utiliser des mots de passe, codages et autres mesures de sécurité s'il a enregistré dans son ordinateur portable des informations personnelles identifiables. Dans le même ordre d'idées, un auditeur interne qui détient des informations confidentielles importantes ne peut les communiquer à des tiers ou les utiliser à des fins personnelles (délit d'initié).

Compétence – Enfin, le Code de déontologie exige que « les auditeurs internes utilisent et appliquent les connaissances, les savoir-faire et expériences requis pour la réalisation de leurs travaux ».

Compétence

Les auditeurs internes utilisent et appliquent les connaissances, les savoir-faire et expériences requis pour la réalisation de leurs travaux.

Les règles de conduite associées au principe de compétence énoncent que « les auditeurs internes :

- ne doivent s'engager que dans des travaux pour lesquels ils ont les connaissances, le savoir-faire et l'expérience nécessaires ;
- doivent réaliser leurs travaux d'audit interne dans le respect des *Normes internationales pour la pratique professionnelle de l'audit interne* ;
- doivent toujours s'efforcer d'améliorer leur compétence, l'efficacité et la qualité de leurs travaux ».

Les activités d'audit interne peuvent être effectuées par des personnes qui font preuve d'intégrité, d'objectivité et de confidentialité, mais ces activités n'auront guère de valeur si ces personnes n'ont pas les connaissances et les qualifications requises pour accomplir ce travail et en tirer des conclusions valides. C'est pourquoi il existe des normes spécifiques qui imposent aux auditeurs internes d'enrichir en permanence leurs compétences et leurs connaissances.

Le Code de déontologie s'applique à toutes les personnes et à toutes les entités qui fournissent des services d'audit interne, et pas uniquement aux membres des Instituts d'audit interne ou aux titulaires d'une certification professionnelle telle que le CIA. Cependant, les Instituts n'ont de pouvoir, en cas d'infraction, que sur leurs membres et les titulaires de ces certifications professionnelles. Toute personne relevant de l'autorité de l'Institut et qui violerait le Code de déontologie est passible de blâme, de suspension de son adhésion ainsi que de radiation et/ou de révocation de la certification, selon la décision du comité de déontologie des Instituts. Il convient également de noter que le fait qu'un comportement

Copyright © 2015 Eyrolles.

donné ne figure pas explicitement dans les règles de conduite ne l'empêche pas d'être inacceptable ou déshonorant, et peut donc entraîner une action disciplinaire à l'encontre de la personne qui s'en est rendue coupable.

Les *Normes internationales pour la pratique professionnelle de l'audit interne*

Les principes fondamentaux de l'audit interne sont mis en exergue dans les *Normes* de l'IIA. L'introduction aux *Normes* reconnaît que « l'audit interne est exercé dans différents environnements juridiques et culturels ainsi que dans des organisations dont l'objet, la taille, la complexité et la structure sont divers. Il peut être en outre exercé par des professionnels de l'audit, internes ou externes à l'organisation ». Si les différences entre les organisations peuvent influencer la pratique de l'audit interne, « il est essentiel de se conformer aux [*Normes*] pour que les auditeurs internes et l'audit interne s'acquittent de leurs responsabilités ».

L'introduction aux *Normes* souligne en outre que « les *Normes* s'appliquent aux auditeurs internes et à l'activité d'audit interne ». Tous les auditeurs internes ont la responsabilité de se conformer aux *Normes* relatives à l'objectivité, aux compétences et à la conscience professionnelle individuelles. De plus, ils doivent se conformer aux *Normes* relatives aux responsabilités associées à leur poste. Les responsables de l'audit interne « ont la responsabilité d'assurer la conformité globale de l'activité d'audit interne avec les *Normes* et d'en rendre compte ».

Les Normes

Principes obligatoires constitués de déclarations et d'interprétations.

« Les *Normes* ont pour objet :

- de définir les principes fondamentaux de la pratique de l'audit interne ;
- de fournir un cadre de référence pour la réalisation et la promotion d'un large champ d'intervention d'audit interne à valeur ajoutée ;
- d'établir les critères d'appréciation du fonctionnement de l'audit interne ;
- de favoriser l'amélioration des processus organisationnels et des opérations » (Introduction aux *Normes*).

« Les *Normes* sont des principes obligatoires constitués :

- de *déclarations* sur les conditions fondamentales pour la pratique professionnelle de l'audit interne et pour l'évaluation de sa performance. Elles sont internationales et applicables tant au niveau du service qu'au niveau individuel ;
- d'*interprétations* clarifiant les termes et les concepts utilisés dans les déclarations. »

Copyright © 2015 Eyrolles.

Ainsi, dans la Norme 2040, Règles et procédures, la *déclaration* est : « Le responsable de l'audit interne doit établir des règles et procédures fournissant un cadre à l'activité d'audit interne ». L'*interprétation* est : « La forme et le contenu des règles et procédures dépendent de la taille, de la manière dont est structuré l'audit interne et de la complexité de ses travaux ». Dans ce cas, l'interprétation explique que la forme et le contenu adéquats des règles et procédures varient d'une fonction d'audit interne à l'autre en raison de la taille, de la structure de l'organisation et du type d'activité.

Les *Normes* incluent un glossaire des termes utilisés dans un sens spécifique. Les déclarations, leurs interprétations et les termes définis dans le glossaire doivent être considérés ensemble si l'on veut comprendre et appliquer les *Normes* correctement. Les *Normes* sont reproduites dans leur intégralité à l'annexe A de ce manuel.

Il existe trois types de *Normes* :

- les **Normes de qualification**, qui « énoncent les caractéristiques que doivent présenter les organisations et les personnes accomplissant des missions d'audit interne » ;
- les **Normes de fonctionnement**, qui « décrivent la nature des missions d'audit interne et définissent des critères de qualité permettant de mesurer la performance des services fournis » ;
- les **Normes de mise en œuvre**, qui « précisent les Normes de qualification et les Normes de fonctionnement en indiquant les exigences applicables dans les activités d'assurance (A) ou de conseil (C) » (Introduction aux *Normes*).

Trois types de *Normes*

– Normes de qualification.
– Normes de fonctionnement.
– Normes de mise en œuvre.

Les *Normes* sont organisées à l'aide d'un système de nombres et de lettres. Les Normes de qualification forment la série des 1000 et les Normes de fonctionnement la série des 2000. Les Normes de qualification comme les Normes de fonctionnement s'appliquent à la fois aux activités d'assurance et de conseil. Les Normes de mise en œuvre sont présentées directement sous la Norme de qualification ou de fonctionnement à laquelle elles renvoient, et leur code comporte un « A » si elles ont trait à des activités d'assurance, et un « C » s'il s'agit d'activités de conseil. Ce système de numérotation est synthétisé à l'encadré 2.3.

Les activités d'assurance et de conseil

Les deux catégories d'activités d'audit interne, les activités de conseil et d'assurance, ont été présentées dans le chapitre 1, *Introduction à l'audit interne*. Le glossaire contenu dans les *Normes* les définit comme suit :

- **activités d'assurance** – Il s'agit d'un examen objectif d'éléments probants, effectué en vue de fournir à l'organisation une évaluation indépendante des processus de gouvernement

Copyright © 2015 Eyrolles.

d'entreprise, de management des risques et de contrôle. Par exemple entrent dans cette catégorie les audits financiers, de performance, de conformité, de sécurité des systèmes et de *due diligence* ;

- **activités de conseil** – Il s'agit des conseils et services y afférents rendus au client donneur d'ordre, dont la nature et le champ sont convenus au préalable avec lui. Ces activités ont pour objectifs de créer de la valeur ajoutée et d'améliorer les processus de gouvernement d'entreprise, de management des risques et de contrôle d'une organisation sans que l'auditeur interne n'assume aucune responsabilité de management. Quelques exemples : avis, conseil, assistance et formation.

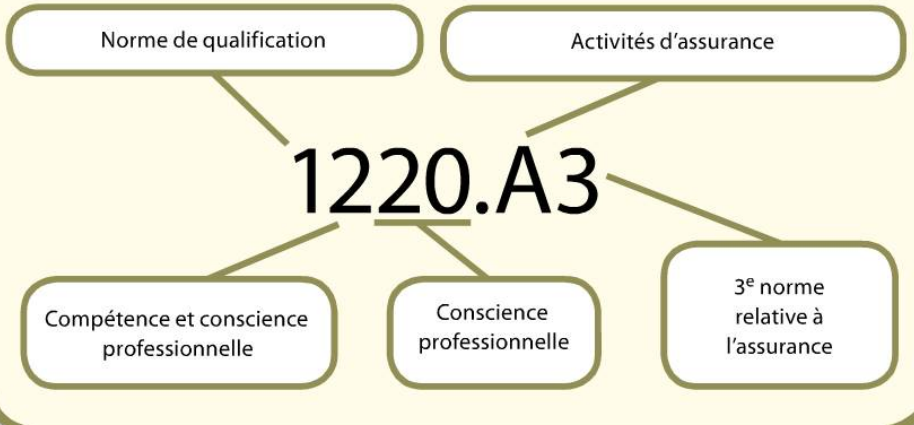
ENCADRÉ 2-3

ILLUSTRATION DU SYSTÈME DE NUMÉROTATION UTILISÉ DANS LES NORMES

1220 – Conscience professionnelle

Les auditeurs internes doivent apporter à leur travail la diligence et le savoir-faire que l'on peut attendre d'un auditeur interne raisonnablement averti et compétent. La conscience professionnelle n'implique pas l'infaillibilité.

1220.A3 – Les auditeurs internes doivent exercer une vigilance particulière à l'égard des risques significatifs susceptibles d'affecter les objectifs, les opérations ou les ressources. Toutefois, les procédures d'audit seules, même lorsqu'elles sont menées avec la conscience professionnelle requise, ne garantissent pas que tous les risques significatifs seront détectés.

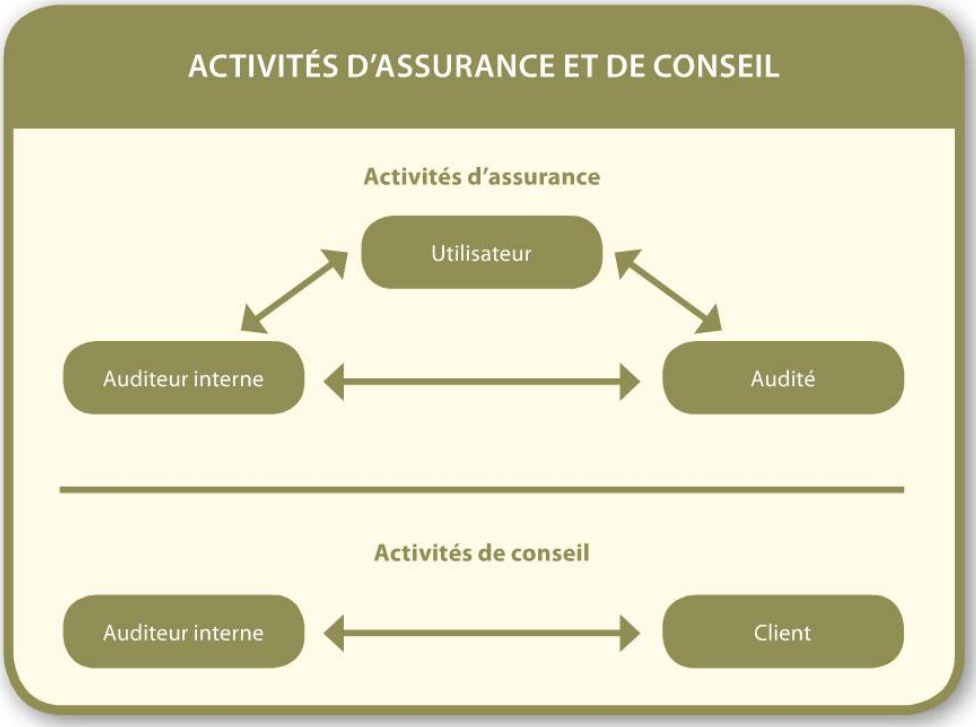


La différence d'objectif entre ces deux types d'activités est claire. Les activités d'assurance permettent de procurer des évaluations indépendantes. Les missions de conseil ont pour but d'apporter des services de conseil, de formation et d'assistance.

En revanche, la différence de structure entre ces deux types d'activités n'est pas aussi évidente ; elle est illustrée dans l'encadré 2-4.

Copyright © 2015 Eyrolles.

ACTIVITÉS D'ASSURANCE ET DE CONSEIL



La structure des missions de conseil est relativement simple. Ces missions font en général intervenir deux parties :

- la partie sollicitant et recevant le conseil, à savoir le client ;
- la partie qui fournit le conseil, à savoir l'audit interne.

L'audit interne travaille directement avec le client afin d'ajuster la mission, de sorte qu'elle réponde aux besoins du client. La structure des missions d'assurance est plus complexe. Elles font généralement intervenir trois parties :

- la partie directement responsable du processus, du système ou autre faisant l'objet de l'évaluation, à savoir l'audité ;
- la partie qui procède à l'évaluation, à savoir la fonction d'audit interne ;
- la partie/les parties qui utilise(nt) l'évaluation, à savoir l'utilisateur ou les utilisateurs.

Ces derniers ne participent pas directement à la mission et, dans certains cas, ne sont pas identifiés explicitement.

La relative complexité des missions d'assurance se reflète dans les *Normes*. L'audit interne doit planifier et accomplir une mission d'assurance et en rapporter les résultats d'une façon qui satisfasse les besoins des tiers utilisateurs qui ne participent pas directement à la mission. En outre, l'audit interne doit prendre soin d'éviter tout conflit d'intérêts éventuel avec ces utilisateurs. Les *Normes* et le Code de déontologie mettent en exergue la nécessité de faire correspondre les intérêts des prestataires d'activités d'assurance et

Copyright © 2015 Eyrolles.

ceux des utilisateurs tiers. En conséquence, les Normes de mise en œuvre pour les activités d'assurance sont plus exigeantes et plus nombreuses que celles relatives aux activités de conseil.

Si les *Normes* distinguent les activités d'assurance et les activités de conseil, les missions ont généralement trait, dans la pratique, à des activités d'assurance et d'amélioration opérationnelle. La proposition de valeur (encadré 2-2) peut s'appliquer tant au niveau de la fonction qu'au niveau de la mission. Au niveau de la mission, la valeur ajoutée résulte d'une assurance et d'un point de vue objectifs. Bien que certaines missions visent essentiellement à donner une assurance, elles peuvent également offrir un point de vue à travers des recommandations et des conseils destinés au management. De même, si les missions de conseil visent essentiellement à offrir un point de vue sur une opération ou un processus, elles peuvent également donner au minimum une assurance limitée concernant l'efficacité de la gestion des risques dans le domaine considéré. S'agissant des Normes de mise en œuvre applicables, si l'objectif principal de la mission consiste à donner une assurance, ce sont les Normes de mise en œuvre relatives à l'assurance qui s'appliqueront. En revanche, si l'objectif principal de la mission consiste à offrir un point de vue (c'est-à-dire améliorer l'efficacité et l'efficience de l'organisation), ce sont les Normes de mise en œuvre relatives au conseil qui s'appliqueront, étant précisé que, dans pareil cas, le niveau d'assurance obtenu sera moindre si les Normes de mise en œuvre relatives à l'assurance ne sont pas appliquées. Certaines missions sont parfois organisées de telle manière que les objectifs sont significatifs, tant en termes d'assurance que de point de vue. Ces missions sont appelées « missions mixtes ». Le chapitre 15 traite des problématiques liées à l'organisation des missions mixtes.

L'analyse qui suit sur les Normes de qualification et les Normes de fonctionnement portera aussi sur les Normes de mise en œuvre.

Les Normes de qualification

Les Normes de qualification, qui traitent des caractéristiques que les fonctions d'audit interne et chaque auditeur interne doivent posséder pour mener à bien des activités d'audit interne efficaces, se répartissent en quatre grandes catégories :

- 1000 – Mission, pouvoirs et responsabilités ;
- 1100 – Indépendance et objectivité ;
- 1200 – Compétence et conscience professionnelle ;
- 1300 – Programme d'assurance et d'amélioration qualité.

Mission, pouvoirs et responsabilités. L'audit interne doit être doté d'une charte qui énonce clairement la mission, les pouvoirs

Copyright © 2015 Eyrolles.

et les responsabilités de l'audit interne, et qui précise la nature des activités d'assurance et de conseil réalisées par l'audit interne. Cette charte doit également prendre acte de la responsabilité qu'a l'audit interne de respecter la définition de l'audit interne, le Code de déontologie ainsi que les *Normes*. Ces informations peuvent prendre la forme d'un contrat de service lorsque les activités d'audit interne sont externalisées. Le responsable de l'audit interne « doit revoir périodiquement la charte d'audit interne et la soumettre à l'approbation de la direction générale et du Conseil » (Norme 1000, Mission, pouvoirs et responsabilités). L'approbation finale de la charte relève du Conseil. La charte d'audit interne est présentée en détail dans le chapitre 9, *La gestion de l'audit interne*.

Indépendance et objectivité. « L'audit interne doit être indépendant et les auditeurs internes doivent effectuer leurs travaux avec objectivité » (Norme 1100, Indépendance et objectivité). Le glossaire des *Normes* définit l'indépendance et l'objectivité comme suit :

> **Indépendance.** Capacité de l'audit interne à assumer, de manière impartiale, ses responsabilités.
>
> **Objectivité.** Attitude impartiale qui permet aux auditeurs internes d'accomplir leurs missions de telle sorte qu'ils soient certains de la qualité de leurs travaux menés sans le moindre compromis. L'objectivité implique que les auditeurs internes ne subordonnent pas leur propre jugement à celui d'autres personnes.

Indépendance

Capacité de l'audit interne à n'être exposé à aucune situation susceptible d'altérer, en réalité ou en apparence, l'objectivité.

Objectivité

Attitude impartiale.

Il importe de noter qu'indépendance et objectivité sont deux notions distinctes, mais interdépendantes, essentielles à la prestation de services d'audit interne qui créent de la valeur ajoutée : la fonction d'audit interne doit être indépendante et chaque auditeur interne doit être objectif. Si l'indépendance est une caractéristique de la fonction d'audit interne, l'objectivité est une caractéristique de l'auditeur interne. Cette distinction est subtile, mais néanmoins extrêmement importante.

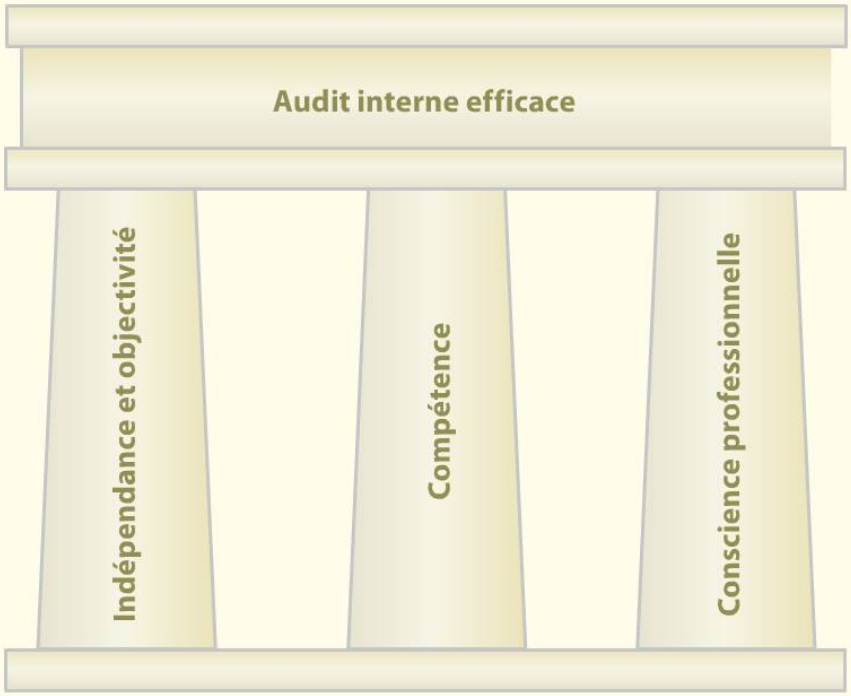
Le degré d'indépendance de l'audit interne dépend du statut relatif de ce service dans l'organisation. La Norme 1110, Indépendance dans l'organisation, indique que « le responsable de l'audit interne doit relever d'un niveau hiérarchique suffisant au sein de l'organisation pour permettre au service d'audit interne d'exercer ses responsabilités [et] doit confirmer au Conseil, au moins annuellement, l'indépendance de l'audit interne au sein de l'organisation ». La Norme 1111, Relation directe avec le Conseil, précise que le responsable de l'audit interne doit « pouvoir communiquer et dialoguer directement avec le Conseil ». Positionner la fonction d'audit interne à un niveau élevé dans l'organisation permet d'élargir le champ de l'audit et favorise une prise en compte adéquate des résultats de la mission. À l'inverse, positionner la fonction d'audit interne plus bas dans l'organisation augmente sensiblement le

Copyright © 2015 Eyrolles.

risque que des conflits d'intérêts n'entravent la capacité de l'audit interne à fournir des évaluations et des conseils objectifs. Ainsi, une fonction d'audit interne qui serait rattachée au contrôleur de gestion ayant la responsabilité de l'adéquation de la conception des contrôles relatifs au reporting financier et de leur fonctionnement effectif aurait du mal à évaluer avec objectivité ces contrôles.

ENCADRÉ 2-5

LES TROIS PILIERS D'UN AUDIT INTERNE EFFICACE



Comme le montre l'encadré 2-5, l'indépendance/l'objectivité est l'un des trois piliers sur lesquels repose l'efficacité de l'audit interne. L'indépendance de l'audit interne vis-à-vis de l'organisation favorise l'objectivité des auditeurs internes. L'objectivité est un état d'esprit et elle est définie comme l'absence de préjugés. Elle suppose le recours à des faits, sans déformation induite par les sentiments ou les préjugés personnels.[2] Dans la pratique, cela revient à affirmer que, face à des faits et des circonstances identiques, deux personnes disposant du même niveau de savoir-faire doivent tirer des conclusions identiques.

Des conflits d'intérêts peuvent entraver l'indépendance et l'objectivité. Un conflit d'intérêts est une « situation dans laquelle un auditeur interne, qui jouit d'une position de confiance, a un intérêt personnel ou professionnel venant en concurrence avec ses devoirs et responsabilités » (Interprétation de la Norme 1120, Objectivité

Copyright © 2015 Eyrolles.

individuelle). Les conflits d'intérêts potentiels résultent souvent d'un concours de circonstances. Des exemples sont cités ci-après.

- On demande au manager d'un service de l'organisation de devenir responsable de l'audit interne.
- Un collaborateur intègre le service d'audit interne après avoir travaillé dans un autre service de l'organisation, ou bien il doit passer par le service d'audit interne dans le cadre de sa formation.
- On demande à un auditeur interne spécialisé en comptabilité d'accepter temporairement un poste dans un service comptable.
- On demande à un auditeur interne ayant une expérience de gestion d'occuper un poste opérationnel vacant le temps que l'organisation trouve un remplaçant convenable.
- On demande à un auditeur interne de concevoir des règles et des procédures de contrôle dans un service de l'organisation qui ne dispose pas de l'expertise requise pour combler les déficiences de contrôle existantes.
- Le responsable de l'audit interne gère, outre l'audit interne, des fonctions telles que la gestion des risques, la sécurité ou la conformité.

Les menaces planant sur l'indépendance et l'objectivité découlant de l'activité peuvent s'expliquer par la nature même du travail. Ainsi, une personne qui est récemment entrée dans le service d'audit interne peut se voir demander d'auditer le service dont elle était précédemment responsable. Dans les faits, elle devrait alors auditer son propre travail.

Dans une telle situation, l'objectivité est compromise, car on a parfois du mal à voir ou à admettre les déficiences ou les erreurs de son propre travail. Les êtres humains se caractérisent par un biais inconscient à servir leurs propres intérêts, qui représente une faiblesse cognitive. Ainsi, des études ont montré qu'il est beaucoup plus difficile de détecter les faiblesses des systèmes que l'on a soi-même conçus, que les failles dans les systèmes conçus par d'autres.[3]

L'indépendance et l'objectivité peuvent également être mises à mal par des incitations ou des relations personnelles. Les *incitations* font référence à des situations dans lesquelles l'auditeur interne a un intérêt économique aux résultats de son travail, susceptible d'altérer son jugement. Quelques exemples de telles situations sont présentés ci-après.

- Le management de l'audité promet à l'auditeur interne de lui offrir un poste ou d'appuyer sa promotion si la mission se passe bien et si aucun problème n'est décelé.
- Un manager ou un collaborateur offre un cadeau ou rend un service à un auditeur interne, faisant ainsi pression sur ce dernier pour qu'il lui rende la pareille.

Copyright © 2015 Eyrolles.

- La structure de rémunération au sein de l'audit interne accorde des primes en fonction du nombre d'observations que les auditeurs internes intègrent dans leurs rapports.

Les *relations personnelles* peuvent être source de conflits d'intérêts lorsque les auditeurs internes effectuent des missions dans des services de l'organisation au sein desquels des parents ou des amis proches travaillent. À cause de ces relations, les auditeurs internes peuvent être tentés de fermer les yeux sur certains problèmes ou d'atténuer des conclusions négatives.

Conflit d'intérêts

Toute relation qui n'est pas ou ne semble pas être dans l'intérêt de l'organisation.

Le responsable de l'audit interne est chargé de protéger la fonction d'audit interne d'éventuels conflits d'intérêts. La Norme 1130.A1 reconnaît que « les auditeurs internes doivent s'abstenir d'auditer des opérations particulières dont ils étaient auparavant responsables. L'objectivité d'un auditeur interne est présumée altérée lorsqu'il réalise une mission d'assurance pour une activité dont il a eu la responsabilité au cours de l'année précédente ». La Norme 1130.A2 indique que « les missions d'assurance concernant des fonctions dont le responsable de l'audit a la charge doivent être supervisées par une personne ne relevant pas de l'audit interne ».

Les normes ayant trait aux activités de conseil ne sont pas aussi strictes. La Norme 1130.C1 énonce que « les auditeurs internes peuvent être amenés à réaliser des missions de conseil liées à des opérations dont ils ont été auparavant responsables ». D'après la Norme 1130.C2, si leur indépendance ou leur objectivité est susceptible d'être compromise, ils doivent toutefois en informer le client donneur d'ordre avant d'accepter la mission.

Les atteintes à l'indépendance ou à l'objectivité, dans les faits ou en apparence, sont inévitables dans certaines circonstances. La Norme 1130, Atteinte à l'indépendance ou à l'objectivité, souligne que, dans ces cas-là, les parties concernées doivent en être informées de manière précise. Suivant la nature de l'atteinte et des responsabilités du responsable de l'audit interne vis-à-vis de la direction générale et du Conseil, telles que spécifiées dans la charte d'audit interne, le responsable de l'audit interne ne rendra pas compte à la même personne. Les utilisateurs des services d'audit interne n'ont ainsi pas à placer indûment une confiance aveugle dans les résultats des travaux de l'audit interne et peuvent déterminer par eux-mêmes dans quelle mesure ils souhaitent se fier à ces travaux.

Compétence et conscience professionnelle. Comme l'illustre l'encadré 2-5, la compétence et la conscience professionnelle sont les deuxième et troisième piliers étayant l'efficacité des services d'audit interne. Les activités d'assurance et de conseil exécutées par des auditeurs internes ne disposant pas des connaissances, du savoir-faire et autres compétences requis, ou n'y apportant pas la diligence et le savoir-faire nécessaires ne seront, pour le moins, pas d'une grande

Copyright © 2015 Eyrolles.

utilité. Ainsi, les *Normes* imposent à la fonction d'audit interne et aux auditeurs internes de posséder les connaissances, le savoir-faire et les autres compétences nécessaires à l'exercice de leurs responsabilités, et de faire preuve de conscience professionnelle.

Les *Normes* ne définissent pas un ensemble précis de connaissances, de savoir-faire ou autres compétences obligatoires. Des dispositions fortement recommandées concernant la compétence figurent à la Modalité Pratique d'Application 1210-1, Compétence. On trouvera d'autres lignes directrices dans le *Competency Framework* de l'IIA (voir chapitre 1, *Introduction à l'audit interne*), ainsi que dans les programmes de préparation aux examens du CIA.[4]

Commentaire du traducteur

Les programmes de préparation aux examens du CIA sont disponibles en langue française.
Le Référentiel de compétences (Competency Framework) *est régulièrement mis à jour.*

Les *Normes* imposent notamment, comme compétence spécifique, une connaissance des risques de fraude. La Norme 1210.A2 stipule que « les auditeurs internes doivent posséder des connaissances suffisantes pour évaluer le risque de fraude et la façon dont ce risque est géré par l'organisation. Toutefois, ils ne sont pas censés posséder l'expertise d'une personne dont la responsabilité première est la détection et l'investigation des fraudes ». Le chapitre 8, *Les risques de fraude et d'actes illégaux*, examine en détail la nature des risques de fraude et des contrôles qu'une organisation peut mettre en place pour maîtriser ces risques.

De même, la Norme 1210.A3 indique que « les auditeurs internes doivent posséder une connaissance suffisante des principaux risques et contrôles relatifs aux technologies de l'information, et des techniques d'audit informatisées susceptibles d'être mises en œuvre dans le cadre des travaux qui leur sont confiés. Toutefois, tous les auditeurs internes ne sont pas censés posséder l'expertise d'un auditeur dont la responsabilité première est l'audit informatique ». Le chapitre 7, *Les risques et les contrôles des systèmes d'information*, étudie en détail la nature des risques SI et les contrôles que les organisations peuvent mettre en place pour maîtriser ces risques. Le chapitre 10, *Les preuves d'audit et les papiers de travail*, propose un aperçu des techniques d'audit informatisées.

L'impératif de compétence s'applique à l'ensemble de la fonction d'audit interne aussi bien qu'à chaque auditeur interne. Il incombe au responsable de l'audit interne de veiller à ce que son service possède les connaissances, le savoir-faire et les autres compétences nécessaires à l'exercice de ses responsabilités conformément à la charte. Si le service ne dispose pas des compétences nécessaires

Compétence

Les connaissances, le savoir-faire et les autres compétences nécessaires à l'exercice des responsabilités professionnelles de l'audit interne.

Copyright © 2015 Eyrolles.

pour exécuter tout ou partie d'une mission d'assurance, le responsable de l'audit interne doit « obtenir l'avis et l'assistance de personnes qualifiées » extérieures (Norme 1210.A1). Le chapitre 9, *La gestion de l'audit interne* examine la possibilité d'obtenir avis et assistance de la part de prestataires extérieurs. Lorsque l'audit interne doit réaliser une mission de conseil pour laquelle il ne possède pas les compétences nécessaires, le responsable de l'audit interne doit décliner la mission ou obtenir l'avis et l'assistance de personnes qualifiées (Norme 1210.C1).

Conscience professionnelle

La diligence et le savoir-faire que l'on peut attendre d'un auditeur interne raisonnablement averti et compétent.

La Norme 1220, Conscience professionnelle, impose aux auditeurs internes d'« apporter à leur travail la diligence et le savoir-faire que l'on peut attendre d'un auditeur interne raisonnablement averti et compétent ». Cela ne signifie pas que les auditeurs internes ne feront jamais d'erreurs factuelles ou de jugement, mais qu'ils feront preuve du degré d'attention et de compétence attendu d'un professionnel. Faire preuve de conscience professionnelle ne signifie pas non plus que les auditeurs internes examineront chaque transaction, visiteront chaque site ou s'entretiendront avec chaque personne travaillant pour l'audité ou le client de la mission. En revanche, cela signifie qu'ils devront déployer le même degré d'effort que d'autres professionnels de l'audit interne dans des situations analogues.

Les *Normes* définissent les aspects à prendre en considération lorsque l'on détermine le niveau de soin approprié à apporter aux missions d'assurance et de conseil. La Norme 1220.A1 indique que, dans ses missions d'assurance, l'auditeur interne doit « [prendre] en considération les éléments suivants :

- l'étendue du travail nécessaire pour atteindre les objectifs de la mission ;
- la complexité relative, la matérialité ou le caractère significatif des domaines auxquels sont appliquées les procédures propres aux missions d'assurance ;
- l'adéquation et l'efficacité des processus de gouvernement d'entreprise, de management des risques et de contrôle ;
- la probabilité d'erreurs significatives, de fraudes ou de non-conformité ;
- le coût de la mise en place de contrôles par rapport aux avantages escomptés ».

Commentaire du traducteur

L'analyse coûts/bénéfices des contrôles revient à s'assurer qu'ils sont proportionnés aux risques encourus et aux seuils de tolérance définis par l'organisation.

L'auditeur interne doit également « envisager l'utilisation de techniques informatiques d'audit et d'analyse des données » (Norme 1220.A2) et « exercer une vigilance particulière à l'égard

Copyright © 2015 Eyrolles.

des risques significatifs susceptibles d'affecter les objectifs, les opérations ou les ressources » (Norme 1220.A3).

La Norme 1220.C1 indique que, dans ses missions de conseil, l'auditeur interne doit « [prendre] en considération les éléments suivants :

- les besoins et attentes des clients, y compris sur la nature, le calendrier et la communication des résultats de la mission ;
- la complexité de celle-ci et l'étendue du travail nécessaire pour atteindre les objectifs fixés ;
- son coût par rapport aux avantages escomptés. »

La Norme 1230, Formation professionnelle continue, stipule que « les auditeurs internes doivent améliorer leurs connaissances, savoir-faire et autres compétences par une formation professionnelle continue ». Les personnes désireuses de devenir auditeur interne et les auditeurs internes qui n'ont pas encore obtenu de certification professionnelle doivent suivre des cours, une formation, un programme d'apprentissage qui les mettent en position d'obtenir une ou plusieurs certifications pertinentes compte tenu de leurs responsabilités professionnelles. Les Instituts d'audit interne organisent plusieurs certifications : le CIA (*Certified Internal Auditor*, auditeur interne certifié), le CGAP (*Certified Governmental Audit Professional*, certification en audit des organisations publiques), le CFSA (*Certified Financial Services Auditor*, certification en audit des services financiers), le CCSA (*Certified in Control Self-Assessment*, certification en auto-évaluation des contrôles) et le CRMA (*Certification in Risk Management Assurance*, certification en évaluation de la gestion des risques). D'autres organisations professionnelles proposent des certifications qui peuvent être utiles aux professionnels de l'audit interne. Ainsi, le CISA (*Certified Information Systems Auditor*, certification en audit des systèmes d'information) est décerné par l'ISACA (anciennement connu sous le nom d'*Information Systems Audit and Control Association*), et la certification CFE (*Certified Fraud Examiner*) a été mise en place par l'*Association of Certified Fraud Examiners* (ACFE). Les auditeurs internes qui ont obtenu des certifications professionnelles doivent remplir certains critères de formation professionnelle continue pour conserver leur certification. Cette norme complète la règle 4.3 du Code de déontologie, qui précise que les auditeurs internes doivent toujours s'efforcer d'améliorer leur compétence, l'efficacité et la qualité de leurs travaux.

Programmes d'assurance et d'amélioration qualité. Le concept d'assurance qualité est le même, qu'on l'applique aux services d'audit interne, à la fabrication d'un produit ou à la prestation de quelque service que ce soit. L'assurance qualité permet de donner l'assurance que le produit ou service possède bien les caractéristiques ou traits essentiels qu'il est censé posséder. Ainsi, s'agissant de la production d'un type particulier de boulons en acier, l'assurance qualité cherchera à s'assurer que les boulons fabriqués

Certifications proposées par les Instituts d'audit

– *Certified Internal Auditor* (CIA, auditeur interne certifié).
– *Certified Governmental Audit Professional* (CGAP, certification en audit des organisations publiques).
– *Certified Financial Services Auditor* (CFSA, certification en audit des services financiers).
– *Certification in Control Self-Assessment* (CCSA, certification en auto-évaluation des contrôles).
– *Certification in Risk Management Assurance* (CRMA, certification en évaluation de la gestion des risques).
– Certification professionnelle de l'auditeur interne (CPAI).

Copyright © 2015 Eyrolles.

répondent bien au cahier des charges. Dans le même ordre d'idées, un programme d'assurance et d'amélioration qualité d'une fonction d'audit interne « est conçu de façon à évaluer la conformité de l'audit interne avec la définition de l'audit interne et les *Normes* [ainsi que] le respect du Code de déontologie par les auditeurs internes. Ce programme permet également de s'assurer de l'efficacité et de l'efficience de l'activité d'audit interne et d'identifier toutes opportunités d'amélioration » (Interprétation de la Norme 1300, Programme d'assurance et d'amélioration qualité).

Assurance qualité

Activité qui permet de donner l'assurance que le produit ou service possède bien les caractéristiques ou traits essentiels qu'il est censé posséder.

« Le responsable de l'audit interne doit élaborer et tenir à jour un programme d'assurance et d'amélioration qualité portant sur tous les aspects de l'audit interne » (Norme 1300, Programme d'assurance et d'amélioration qualité). Le responsable de l'audit interne doit également « communiquer les résultats du programme d'assurance et d'amélioration qualité à la direction générale ainsi qu'au Conseil » (Norme 1320, Rapports relatifs au programme d'assurance et d'amélioration qualité) et il peut « indiquer que l'activité d'audit interne est conduite conformément aux *Normes internationales pour la pratique professionnelle de l'audit interne* seulement si les résultats du programme d'assurance et d'amélioration qualité l'ont démontré » (Norme 1321, Utilisation de la mention « conforme aux *Normes internationales pour la pratique professionnelle de l'audit interne* »). « Quand la non-conformité de l'activité d'audit interne avec la définition de l'audit interne, le Code de déontologie ou encore les *Normes* a une incidence sur le champ d'intervention ou sur le fonctionnement de l'audit interne, le responsable de l'audit interne doit informer la direction générale et le Conseil de cette non-conformité et de ses conséquences » (Norme 1322, Indication de non-conformité).

La Norme 1310, Exigences du programme d'assurance et d'amélioration qualité, précise que « le programme d'assurance et d'amélioration qualité doit comporter des évaluations tant internes qu'externes ». « Les évaluations internes doivent comporter :

- une surveillance continue de la performance de l'audit interne ;
- des évaluations périodiques, effectuées par auto-évaluation ou par d'autres personnes de l'organisation possédant une connaissance suffisante des pratiques d'audit interne » (Norme 1311, Évaluations internes).

« Des évaluations externes doivent être réalisées au moins tous les cinq ans par un évaluateur ou une équipe d'évaluateurs qualifiés, indépendants et extérieurs à l'organisation. Le responsable de l'audit interne doit s'entretenir avec le Conseil au sujet :

- des modalités et de la fréquence de l'évaluation externe ;
- et des qualifications de l'évaluateur ou de l'équipe d'évaluation externes ainsi que de leur indépendance y compris au regard de tout conflit d'intérêts potentiel » (Norme 1312, Évaluations externes).

Copyright © 2015 Eyrolles.

ENCADRÉ 2-6

CADRE DE RÉFÉRENCE POUR LA CONCEPTION D'UN PROGRAMME D'ASSURANCE QUALITÉ

Hiérarchie des composantes de l'assurance qualité

Composante du contrôle	Objectif du contrôle	Source	Niveau d'assurance
Professionnalisme (conscience professionnelle)	Travaux de l'auditeur interne	Personne	Auditeur interne
Surveillance continue/Contrôle par le superviseur	Mission	Superviseur à l'intérieur de la ligne hiérarchique	Management de la fonction d'audit
Évaluation interne	Ensemble des missions ou des audits de divisions ou des unités d'audit autonomes	Superviseur/Pair en dehors de la ligne hiérarchique	Responsable de l'audit interne
Évaluation externe	Fonction d'audit dans son ensemble	Personnes qualifiées n'appartenant pas à l'organisation	Comité d'audit et direction générale

L'encadré 2-6 propose un cadre de référence pour la conception d'un programme d'assurance qualité, reposant sur le principe de substituabilité, puisque les composantes de l'assurance qualité peuvent y remplacer une composante de rang supérieur, à condition que des critères d'indépendance précis soient respectés. Ainsi, une évaluation externe peut être remplacée par une évaluation interne tant que les évaluateurs internes sont indépendants (en d'autres termes, qu'ils n'appartiennent pas à la ligne hiérarchique et n'ont pas de responsabilité directe vis-à-vis de l'aspect du travail qu'ils ont à évaluer). En conséquence, de grandes fonctions d'audit qui comptent plusieurs unités d'audit décentralisées (par exemple en Asie, en Amérique du Nord, en Amérique du Sud et en Europe) peuvent procéder à une évaluation interne des travaux effectués par des auditeurs internes lors de missions d'assurance ou de conseil qui leur ont été confiées. Dans de telles situations, l'évaluation externe pourrait se concentrer sur le processus d'assurance qualité de l'audit interne, sur l'indépendance de la fonction d'audit interne au sein de l'organisation, sur le processus d'évaluation des risques et sur les relations avec le comité d'audit et la direction générale. En revanche, l'évaluation des missions d'assurance et de conseil réalisées par une petite fonction d'audit interne centralisée devra être effectuée par des évaluateurs externes qualifiés.

Le chapitre 9, *La gestion de l'audit interne,* donnera plus de détail sur la mise en œuvre des programmes d'assurance et d'amélioration qualité.

Copyright © 2015 Eyrolles.

On trouvera d'autres lignes directrices permettant de mener à bien des revues internes et externes dans le *Quality Assessment Manual* de l'IIA.

Commentaire du traducteur

Plusieurs Instituts proposent des prestations pour l'évaluation indépendante externe des services d'audit interne. Ainsi, IFACI Certification *a développé un référentiel d'évaluation et le met à jour au rythme de l'évolution des* Normes *afin de proposer une certification de services d'audit interne de qualité.*

Les Normes de fonctionnement

Les Normes de fonctionnement, qui décrivent la nature des activités d'audit interne et les critères au regard desquels ces activités peuvent être évaluées, sont réparties en sept grandes sections :

- 2000 – Gestion de l'audit interne ;
- 2100 – Nature du travail ;
- 2200 – Planification de la mission ;
- 2300 – Accomplissement de la mission ;
- 2400 – Communication des résultats ;
- 2500 – Surveillance des actions de progrès ;
- 2600 – Communication relative à l'acceptation des risques.

Gestion de l'audit interne. La Norme 2000 indique que c'est au responsable de l'audit interne qu'il revient de gérer activement l'audit interne (également appelé « activité d'audit interne » ou « service d'audit interne » dans les *Normes*) et de veiller à ce qu'il apporte une valeur ajoutée à l'organisation. Même lorsque les activités d'audit interne sont externalisées à un tiers, il faut qu'il y ait une personne au sein de l'organisation qui soit chargée d'approuver les contrats de service, de superviser la qualité des travaux fournis par le prestataire de services, de rendre compte des résultats de la mission d'assurance et de conseil à la direction générale et au Conseil, et d'effectuer un suivi des résultats des missions et des observations. Dans de nombreux cas, cette personne agit en qualité de responsable de l'audit interne. Toutefois, si cette personne a des responsabilités qui la mettent dans une situation de conflit d'intérêts ou si le Conseil gère l'activité externalisée, le prestataire de services externe doit en outre « alerter l'organisation qu'elle reste responsable du maintien d'un audit interne efficace » (Norme 2070, Responsabilité de l'organisation en cas de recours à un prestataire externe pour ses activités d'audit interne). L'interprétation de cette Norme spécifie que : « Cette responsabilité est démontrée par le programme d'assurance et d'amélioration qualité, lequel évalue la conformité avec la définition de l'audit interne, le Code de déontologie et les *Normes*. »

Copyright © 2015 Eyrolles.

La Norme 2000 énonce que « l'activité d'audit interne est gérée efficacement quand :

- les résultats des travaux de l'audit interne répondent aux objectifs et responsabilités définis dans la charte d'audit interne ;
- l'audit interne est exercé conformément à la définition de l'audit interne et aux *Normes* ;
- les membres de l'équipe d'audit agissent en respectant le Code de déontologie et les *Normes* » (Interprétation de la Norme 2000, Gestion de l'audit interne).

Les normes suivantes précisent que, pour satisfaire à ses responsabilités de gestion, le responsable de l'audit interne doit :

- « établir un plan d'audit fondé sur les risques afin de définir des priorités cohérentes avec les objectifs de l'organisation » (Norme 2010, Planification) ;
- « communiquer à la direction générale et au Conseil son plan d'audit et ses besoins, pour examen et approbation, ainsi que tout changement important susceptible d'intervenir en cours d'exercice. Le responsable de l'audit interne doit également signaler l'impact de toute limitation de ses ressources » (Norme 2020, Communication et approbation) ;
- « veiller à ce que les ressources affectées à cette activité soient adéquates, suffisantes et mises en œuvre de manière efficace pour réaliser le plan d'audit approuvé » (Norme 2030, Gestion des ressources) ;
- « établir des règles et procédures fournissant un cadre à l'activité d'audit interne » (Norme 2040, Règles et procédures) ;
- « partager des informations et coordonner les activités avec les autres prestataires internes et externes d'assurance et de conseil [afin d'assurer une couverture adéquate et d'éviter les doubles emplois] » (Norme 2050, Coordination) ;
- « rendre compte périodiquement à la direction générale et au Conseil des missions, des pouvoirs et des responsabilités de l'audit interne, ainsi que du degré de réalisation du plan d'audit ». Le responsable de l'audit interne « doit plus particulièrement rendre compte de l'exposition aux risques significatifs (y compris des risques de fraude) et des contrôles correspondants ; des sujets relatifs au gouvernement d'entreprise ; et de tout autre problème répondant à un besoin ou à une demande de la direction générale ou du Conseil » (Norme 2060, Rapports à la direction générale et au Conseil).

Ces responsabilités du responsable de l'audit interne sont approfondies au chapitre 9, *La gestion de l'audit interne.*

Nature du travail. La Norme 2100, Nature du travail, reprend des éléments de la définition de l'audit interne. Elle indique que

Copyright © 2015 Eyrolles.

« l'audit interne doit évaluer les processus de gouvernement d'entreprise, de management des risques et de contrôle, et contribuer à leur amélioration sur la base d'une approche systématique et méthodique ».

En premier lieu, « l'audit interne doit évaluer le processus de gouvernement d'entreprise et formuler des recommandations appropriées en vue de son amélioration. À cet effet, il détermine si le processus répond aux objectifs suivants :

- promouvoir des règles d'éthique et des valeurs appropriées au sein de l'organisation ;
- garantir une gestion efficace des performances de l'organisation, assortie d'une obligation de rendre compte ;
- communiquer aux services concernés de l'organisation les informations relatives aux risques et aux contrôles ;
- fournir une information adéquate au Conseil, aux auditeurs internes et externes et au management, et assurer une coordination de leurs activités » (Norme 2110, Gouvernement d'entreprise).

De même, « l'audit interne doit évaluer l'efficacité des processus de management des risques et contribuer à leur amélioration » (Norme 2120, Management des risques). « Afin de déterminer si les processus de management des risques sont efficaces, les auditeurs internes doivent s'assurer que :

- les objectifs de l'organisation sont cohérents avec sa mission et y contribuent ;
- les risques significatifs sont identifiés et évalués ;
- les modalités de traitement des risques retenues sont appropriées et en adéquation avec l'appétence pour le risque de l'organisation ;
- les informations relatives aux risques sont recensées et communiquées en temps opportun au sein de l'organisation pour permettre aux collaborateurs, à leur hiérarchie et au Conseil d'exercer leurs responsabilités » (Interprétation de la Norme 2120, Management des risques).

Enfin, « l'audit interne doit aider l'organisation à maintenir un dispositif de contrôle approprié en évaluant son efficacité et son efficience et en encourageant son amélioration continue » (Norme 2130, Contrôle).

L'audit interne évalue l'exposition aux risques, ainsi que l'adéquation de la conception et le fonctionnement effectif des contrôles. « Cette évaluation doit porter sur les aspects suivants :

- l'atteinte des objectifs stratégiques de l'organisation ;
- la fiabilité et l'intégrité des informations financières et opérationnelles ;
- l'efficacité et l'efficience des opérations et des programmes ;

Copyright © 2015 Eyrolles.

- la protection des actifs ;
- le respect des lois, règlements, règles, procédures et contrats » (Normes 2120.A1 et 2130.A1).

Le chapitre 3, *La gouvernance*, le chapitre 4, *La gestion des risques*, et le chapitre 6, *Le contrôle interne*, proposent un examen détaillé des processus de gouvernance, de gestion des risques et de contrôle, et présentent les responsabilités de l'audit interne dans l'évaluation de ces processus ainsi que sa contribution à leur amélioration.

Le processus d'audit. L'exécution de missions, qu'elles soient d'assurance ou de conseil, peut être scindée en trois étapes, illustrées à l'encadré 2-7. Les sections suivantes des Normes de fonctionnement ont directement trait au processus d'audit :

- 2200 – Planification de la mission ;
- 2300 – Accomplissement de la mission ;
- 2400 – Communication des résultats ;
- 2500 – Surveillance des actions de progrès.

Les deux dernières sections ont été combinées en une phase de « communication » dans l'encadré 2-7. Les normes qui ont plus spécifiquement trait au processus d'audit sont intentionnellement rédigées dans des termes généraux afin de couvrir tout l'éventail des missions d'audit interne.

ENCADRÉ 2-7

LES DIFFÉRENTES ÉTAPES DU PROCESSUS D'AUDIT ET LES NORMES CORRESPONDANTES

2200 Planification de la mission	2300 Accomplissement de la mission	2400 Communication des résultats
2201 Considérations relatives à la planification	2310 Identification des informations	2410 Contenu de la communication
2210 Objectifs de la mission	2320 Analyse et évaluation	2420 Qualité de la communication
2220 Champ de la mission	2330 Documentation des informations	2421 Erreurs et omissions
2230 Ressources affectées à la mission	2340 Supervision de la mission	2430 Utilisation de la mention « conduit conformément aux *Normes* »
2240 Programme de travail de la mission		2431 Indication de non-conformité
		2440 Diffusion des résultats
		2450 Les opinions globales
		2500 Surveillance des actions de progrès

Copyright © 2015 Eyrolles.

La Norme 2200, Planification de la mission, énonce que « les auditeurs internes doivent concevoir et documenter un plan pour chaque mission. Ce plan de mission précise les objectifs, le champ d'intervention, la date et la durée de la mission, ainsi que les ressources allouées ».

« Lors de la planification de la mission, les auditeurs internes doivent prendre en compte :

- les objectifs de l'activité soumise à l'audit et la manière dont elle est maîtrisée ;
- les risques significatifs liés à l'activité, ses objectifs, les ressources mises en œuvre et ses tâches opérationnelles, ainsi que les moyens par lesquels l'impact potentiel du risque est maintenu à un niveau acceptable ;
- la pertinence et l'efficacité des processus de gouvernement d'entreprise, de management des risques et de contrôle de l'activité, en référence à un cadre ou modèle de contrôle approprié ;
- les opportunités d'améliorer de manière significative les processus de gouvernement d'entreprise, de management des risques et de contrôle de l'activité » (Norme 2201, Considérations relatives à la planification).

Les normes suivantes s'appliquent à la planification d'une mission d'audit interne :

- « les objectifs doivent être précisés pour chaque mission » (Norme 2210, Objectifs de la mission) ;
- « le champ doit être suffisant pour atteindre les objectifs de la mission » (Norme 2220, Champ de la mission) ;
- « les auditeurs internes doivent déterminer les ressources appropriées et suffisantes pour atteindre les objectifs de la mission. Ils s'appuient sur une évaluation de la nature et de la complexité de chaque mission, des contraintes de temps et des ressources disponibles » (Norme 2230, Ressources affectées à la mission) ;
- « les auditeurs internes doivent élaborer et documenter un programme de travail permettant d'atteindre les objectifs de la mission » (Norme 2240, Programme de travail de la mission).

Lorsqu'ils effectuent une mission, les auditeurs internes doivent :

- « identifier les informations suffisantes, fiables, pertinentes et utiles pour atteindre les objectifs de la mission » (Norme 2310, Identification des informations) ;
- « fonder leurs conclusions et les résultats de leur mission sur des analyses et évaluations appropriées » (Norme 2320, Analyse et évaluation) ;

Copyright © 2015 Eyrolles.

- « documenter les informations perti
  conclusions et les résultats de la missi
  mentation des informations) ;
- s'assurer que la mission « [fait] l'objet
  priée afin de garantir que les objectifs
  assurée et le développement professio
  tué » (Norme 2340, Supervision de la m

Pour que les missions d'audit soient utiles
être communiqués en temps opportun au
Toutefois, il ne suffit pas que les utilisateu
la communication doit se faire sous une for
de mauvaise interprétation. La Norme 241
nication, précise que « la communication d
le champ de la mission, ainsi que les conclu
et plans d'actions ». La Norme 2420, Qual
indique que « la communication doit être
concise, constructive, complète et émise en
la Norme 2421, Erreurs et omissions, souli
nication finale contient une erreur ou une
responsable de l'audit interne doit faire p
corrigées à tous les destinataires de la ver

Les auditeurs internes peuvent « indique
leurs missions sont "conduites conformém

Copyright © 2015 Eyrolles.

Par ailleurs, « le responsable de l'audit interne doit mettre en place et tenir à jour un système permettant de surveiller la suite donnée aux résultats communiqués au management » (Norme 2500, Surveillance des actions de progrès). Pour les missions d'assurance, cela signifie que « le responsable de l'audit interne doit mettre en place un processus de suivi permettant de surveiller et de garantir que des mesures ont été effectivement mises en œuvre par le management ou que la direction générale a accepté de prendre le risque de ne rien faire » (Norme 2500.A1). S'il s'agit de missions de conseil, « l'audit interne doit surveiller la suite donnée aux résultats des missions de conseil conformément à l'accord passé avec le client donneur d'ordre » (Norme 2500.C1).

Le déroulement d'une mission est traité de manière approfondie dans les chapitres 12, *Introduction au processus d'audit*, 13, *Le déroulement de la mission d'assurance*, 14, *La communication des résultats d'une mission d'assurance et les procédures de suivi*, et 15, *La mission de conseil*.

Risque résiduel

Part du risque inhérent qui subsiste après prise en compte des modalités de traitement des risques mises en œuvre par le management (on parle parfois de risque net).

Communication relative à l'acceptation des risques (Norme 2600, Communication relative à l'acceptation des risques). Le risque résiduel est défini comme la part du risque inhérent qui subsiste après prise en compte des modalités de traitement des risques mises en œuvre par le management. « Lorsque le responsable de l'audit interne conclut que le management a accepté un niveau de risque qui pourrait s'avérer inacceptable pour l'organisation, il doit examiner la question avec la direction générale. Si le responsable de l'audit interne estime que le problème n'a pas été résolu, il doit soumettre la question au Conseil. » L'identification de ce niveau de risque résiduel peut résulter d'une mission d'assurance, d'une mission de conseil, de la surveillance des plans d'actions du management à la suite de missions d'audit interne antérieures, ou d'autres moyens. L'interprétation de la Norme 2600 précise que « la réponse au risque ne relève pas du responsable d'audit interne », mais de la direction générale et du Conseil.

Commentaire du traducteur

Le traitement des risques est fonction de l'appétence pour le risque et des seuils de tolérance de l'organisation.

DISPOSITIONS FORTEMENT RECOMMANDÉES

Les dispositions obligatoires du CRIPP (définition de l'audit interne, Code de déontologie et *Normes*) sont de nature relativement générale, car elles sont applicables à toutes les activités d'audit interne. Des missions d'assurance et de conseil sont menées dans des organisations variées, par des fonctions d'audit interne « maison » ou des prestataires extérieurs, dans des structures centralisées aussi

Copyright © 2015 Eyrolles.

bien que décentralisées, dans divers environnements culturels et juridiques.

Les dispositions fortement recommandées (Modalités Pratiques d'Application, prises de position et guides pratiques) donnent des orientations plus spécifiques et non obligatoires. Elles suggèrent en général un mode opératoire. Les dispositions fortement recommandées peuvent ne pas être applicables à certaines fonctions d'audit interne. Parfois, elles peuvent ne constituer qu'une des nombreuses solutions applicables. Quoi qu'il en soit, ces dispositions font autorité, dans le sens où l'IIA les a validées *via* un processus d'approbation formel, qui inclut un examen par l'*Ethics Committee* (Comité de déontologie) et par l'*Internal Audit Standards Board* (Conseil sur les normes d'audit interne), au cours duquel est vérifiée leur cohérence avec les dispositions obligatoires.

Les Modalités Pratiques d'Application. Les Modalités Pratiques d'Application (MPA) donnent des orientations concises quant à la manière d'appliquer les *Normes*. Elles traitent des approches, méthodologies et facteurs que l'audit interne doit prendre en compte, mais n'ont pas pour objet de détailler des processus et procédures que l'audit interne devrait suivre. Elles peuvent concerner des missions spécifiques ou préciser des pratiques propres à certaines régions géographiques ou à certains secteurs. Chaque Modalité Pratique d'Application est mise en relation, au moyen de son numéro, avec une norme, et renvoie également, le cas échéant, au Code de déontologie.

Modalités Pratiques d'Application (MPA)

Orientations concises quant à la manière d'appliquer les *Normes*.

C'est au *Professional Issues Committee* (Comité des questions professionnelles) qu'il revient de rédiger les Modalités Pratiques d'Application. En 2012, 59 Modalités Pratiques d'Application ont été publiées. Contrairement aux dispositions obligatoires du CRIPP, les Modalités Pratiques d'Application ne font pas l'objet d'une consultation publique. Elles sont néanmoins examinées, avant publication, par le *Standards Board* et l'*Ethics Committee*, qui vérifient leur cohérence avec d'autres parties du CRIPP. Les Modalités Pratiques d'Application sont disponibles dans la version publiée du CRIPP, qui est généralement actualisé tous les trois ans. Toutes les Modalités Pratiques d'Application publiées sont disponibles sur le site Internet de l'IIA et de certains Instituts locaux tels que l'IFACI.

L'encadré 2-8 propose un exemple de Modalité Pratique d'Application. La MPA 1000-1, La charte d'audit interne, donne des conseils relatifs à la Norme 1000, Mission, pouvoirs et responsabilité. Outre le texte qui expose le conseil, la MPA contient la norme à laquelle elle se réfère et, le cas échéant, son interprétation. En l'occurrence, la MPA vient étoffer la norme en y apportant des orientations supplémentaires concernant la charte d'audit interne.

Copyright © 2015 Eyrolles.

ENCADRÉ 2-8

EXEMPLE DE MODALITÉ PRATIQUE D'APPLICATION

MPA 1000-1

Charte d'audit interne

1. L'existence d'une charte d'audit interne formalisée est essentielle pour la gestion du service d'audit interne. La charte est un document officiel soumis pour avis et acceptation à la direction générale, et approuvée par le comité d'audit ou le Conseil. Il précise le rôle du responsable d'audit interne et facilite ainsi l'évaluation périodique de la pertinence de sa mission, de ses pouvoirs et de ses responsabilités. Son approbation est consignée dans les procès-verbaux du Conseil. Il facilite en outre l'évaluation périodique de la pertinence de la mission, des pouvoirs et des responsabilités de l'audit interne, précisant ainsi le rôle de l'audit interne. En cas d'interrogation, la charte est la référence écrite officielle de l'accord passé avec la direction générale et le Conseil sur le rôle et les responsabilités du service d'audit interne de l'organisation.
2. Le responsable de l'audit interne évalue périodiquement si la mission, les pouvoirs, et les responsabilités définis dans la charte permettent toujours au service d'audit interne d'atteindre ses objectifs. Il est également chargé de communiquer le résultat de cette évaluation périodique à la direction générale et au Conseil.

Publié en janvier 2009

Principale Norme de référence

1000 – Mission, pouvoirs et responsabilités

La mission, les pouvoirs et les responsabilités de l'audit interne doivent être formellement définis dans une charte d'audit interne, être cohérents avec la définition de l'audit interne, le Code de déontologie ainsi qu'avec les *Normes*. Le responsable de l'audit interne doit revoir périodiquement la charte d'audit interne et la soumettre à l'approbation de la direction générale et du Conseil.

Interprétation

La charte d'audit interne est un document officiel qui précise la mission, les pouvoirs et les responsabilités de cette activité. La charte définit la position de l'audit interne dans l'organisation y compris la nature de la relation fonctionnelle entre le responsable de l'audit interne et le Conseil ; autorise l'accès aux documents, aux personnes et aux biens, nécessaires à la réalisation des missions ; définit le champ des activités d'audit interne. L'approbation finale de la charte d'audit interne relève de la responsabilité du Conseil.

Date de publication : 1er janvier 2009

Prises de position

Orientations sur des problématiques qui dépassent la simple caractérisation du travail du responsable de l'audit interne, de la fonction d'audit interne et des auditeurs internes individuellement.

Prises de position. Les prises de position de l'IIA donnent des orientations sur des problématiques qui dépassent la simple caractérisation du travail du responsable de l'audit interne, de la fonction d'audit interne et des auditeurs internes individuellement. Elles ne sont pas écrites uniquement à l'intention des auditeurs internes, mais aussi pour d'autres parties intéressées, qui ne sont pas membres de la profession, comme par exemple, la direction générale, le Conseil et les membres du comité d'audit, ainsi que des parties prenantes extérieures, telles que les législateurs, les autorités de régulation et de supervision ou les autres experts avec qui les auditeurs internes sont amenés à travailler (notamment les auditeurs externes et autres prestataires de services participant à des programmes de conformité et de respect de la déontologie de l'organisation ou à des initiatives de gestion des risques). Les prises

Copyright © 2015 Eyrolles.

de position s'intéressent au rôle de l'audit interne dans le système de gestion des risques de l'organisation, à la manière dont l'organisation confie des missions à l'audit interne, et aux trois lignes de maîtrise pour une gestion des risques et un contrôle efficaces. Elles peuvent traiter de questions importantes comme la gouvernance, la gestion des risques et le contrôle, dans l'optique d'apporter une clarification et d'améliorer la compréhension qu'en ont les auditeurs internes et les autres parties prenantes.

C'est souvent le *Professional Issues Committee* (Comité des questions professionnelles) de l'IIA qui est à l'origine des prises de position, mais ce peut aussi être tout autre comité international ou Institut local. Les propositions de prises de position doivent être approuvées par le *Professional Guidance Advisory Council* (groupe composé des présidents du *Standards Board*, du *Professional Issues Committee*, du *Global Ethics Committee* et du *Public Sector Committee*, présenté plus loin dans ce chapitre). Le *Professional Issues Committee* est chargé de l'élaboration et de la rédaction des prises de position. Les prises de position proposées sont ensuite examinées par les comités techniques internationaux de l'IIA (*Standards Board*, *Professional Issues Committee* et *Ethics Committee*), qui vérifient leur cohérence avec le CRIPP. Les prises de position peuvent également être élaborées et publiées en partenariat avec d'autres organisations professionnelles. Contrairement à d'autres types de dispositions fortement recommandées, les prises de position doivent être soumises à la consultation des Instituts IIA locaux et d'autres comités techniques internationaux pendant une période d'un mois avant d'être publiées.

Guides pratiques. Les guides pratiques de l'IIA fournissent des lignes directrices détaillées sur des outils et techniques d'audit interne. Ils se composent de quatre séries. Deux de ces séries traitent des problématiques liées aux risques et aux contrôles en matière de systèmes d'information : la série des *Global Technology Audit Guide*s (Guides pratiques d'audit des technologies de l'information, GTAG) et celle des *Guide to the Assessment of IT Risk* (Guide de l'évaluation des contrôles informatiques généraux basée sur les risques, GAIT). La troisième et la quatrième séries traitent respectivement des problématiques générales d'audit interne et des problématiques liées au secteur public. Tous ces guides sont sur le site Internet de l'IIA ou de certains Instituts locaux tels que l'IFACI. L'encadré 2-9 dresse la liste des guides pratiques actuels par série. Les guides pratiques généraux sont traités dans les chapitres suivants. Le chapitre 7, *Les risques et les contrôles des systèmes d'information*, renseigne plus précisément sur ces lignes directrices portant sur les systèmes d'information.

Tout comité technique a la possibilité de proposer une idée de guide pratique, mais c'est le *Professional Guidance Advisory Council* susmentionné qui en supervise l'élaboration et la publication. Celui-ci approuve le projet et en confie la gestion à l'un de ses comités (le

Guides pratiques

Lignes directrices détaillées sur des outils et techniques d'audit interne.

Copyright © 2015 Eyrolles.

Professional Issues Committee en règle générale). Les comités les plus souvent sollicités pour rédiger des guides pratiques sont le *Professional Issues Committee* (Comité des questions professionnelles) et le *Public Sector Committee* (Comité du secteur public). Avant d'être publiés, les guides sont examinés par le *Standards Board* et l'*Ethics Committee* qui vérifient leur cohérence avec le CRIPP. Contrairement aux dispositions obligatoires du CRIPP et aux prises de position, les guides ne font pas l'objet d'une consultation publique.

Autres documents. L'IIA publie également des documents qui ne font pas partie du CRIPP, mais qui peuvent être utiles aux professionnels de l'audit interne et aux parties prenantes. Ces documents sont disponibles sur le site Internet de l'IIA dans la section « Leading Practices ». À l'heure actuelle, les sujets traités concernent des problématiques liées à la pratique de l'audit interne dans le secteur public, ainsi que des lignes directrices applicables à diverses problématiques liées à la participation de l'audit interne aux mesures prévues aux termes des sections 302 et 404 de la loi Sarbanes-Oxley.

ACTUALISATION DU CADRE DE RÉFÉRENCE INTERNATIONAL DES PRATIQUES PROFESSIONNELLES

Le CRIPP n'entend pas être un corpus statique de lignes directrices de référence, mais veut évoluer en même temps que la profession d'audit interne, à mesure que les professionnels s'adaptent à un environnement en constante mutation.

Le *Professional Guidance Advisory Council* est chargé de coordonner le lancement, l'élaboration, la publication et la mise à jour des lignes directrices constitutives du CRIPP et qui font autorité. Ce *Council* se compose du vice-président du *Professional Practices Committee* et des présidents des quatre comités techniques internationaux, à savoir le *Global Ethics Committee* (Comité mondial de déontologie), l'*International Internal Audit Standards Board* (IASB), le *Professional Issues Committee* (Comité des questions professionnelles) et le *Public Sector Committee* (comité du secteur public). Les trois premiers ont la responsabilité directe de tenir à jour les pans spécifiques du CRIPP.

Chaque année, le *Professional Guidance Advisory Board* conçoit un plan de travail pour l'année qui vient, ainsi qu'un projet de plan pour les deux années suivantes, traçant les grandes lignes du travail de l'*Ethics Committee*, de l'*Internal Audit Standards Board* et du *Professional Issues Committee*. En outre, le *Council* coordonne la révision de toutes les lignes directrices existantes sur un cycle de trois ans.

Le *Global Ethics Committee* (Comité mondial de déontologie). La mission du *Global Ethics Committee*, qui consiste à

Copyright © 2015 Eyrolles.

ENCADRÉ 2-9

GUIDES PRATIQUES

Général	*Global Technology Audit Guides* (Guides pratiques d'audit des technologies de l'information, GTAG)
Business Continuity Management Sélectionner, utiliser et développer des modèles de maturité : un outil pour les missions d'assurance et de conseil *Integrated Auditing* L'audit des risques d'atteinte à la vie privée, 2e édition Élaborer le plan stratégique de l'audit interne *Assessing Organizational Governance in the Private Sector* Évaluer les programmes et les activités relatifs à l'éthique Programme d'assurance et d'amélioration qualité *Coordinating Risk Management and Assurance* *Reliance by Internal Audit on Other Assurance Providers* Indépendance et objectivité *Interaction with the Board* *Assisting Small Internal Audit Activities in Implementing the International Standards for the Professional Practice of Internal Auditing* Auditer l'environnement de contrôle *Measuring Internal Audit Effectiveness and Efficiency* Évaluer l'adéquation du management des risques en utilisant la norme ISO 31000 *Chief Audit Executives — Appointment, Performance, Evaluation, and Termination* Auditer la rémunération et les avantages des dirigeants *Evaluating Corporate Social Responsibility/ Sustainable Development* Audit interne et Fraude L'audit des relations avec les partenaires externes Formuler et exprimer une opinion d'audit	GTAG 17 : Auditing IT Governance GTAG 16 : Data Analysis Technologies GTAG 15 : Information Security Governance GTAG 14 : Auditing User-developed Applications GTAG 13 : Fraud Prevention and Detection in an Automated World GTAG 12 : Audit des projets SI GTAG 11 : Élaboration d'un plan d'audit des SI GTAG 10 : Gestion de la continuité d'activité GTAG 9 : Gestion des identités et des accès GTAG 8 : Audit des contrôles applicatifs GTAG 7 : L'infogérance, 2e édition GTAG 6 : Gérer et auditer les vulnérabilités des technologies de l'information GTAG 5 : (remplacé par le guide pratique intitulé « L'audit des risques d'atteinte à la vie privée », 2e édition) GTAG 4 : Management de l'audit des systèmes d'information GTAG 3 : Audit continu : répercussions sur l'assurance, le pilotage et l'évaluation des risques GTAG 2 : Contrôles de la gestion du changement et des patchs : un facteur clé de la réussite pour toute organisation, 2e édition GTAG 1 : Les contrôles des systèmes d'information, 2e édition
Secteur public	***Guide to the Assessment of IT Risk* (Guide de l'évaluation des contrôles informatiques généraux basée sur les risques, GAIT)**
Assessing Organizational Governance in the Public Sector *How to Build a Strategic Competency Plan in the Public Sector*	*The* GAIT Methodology *GAIT for IT General Control Deficiency Assessment* *GAIT for Business and IT Risk (GAIT-R)*

Copyright © 2015 Eyrolles.

répondre aux besoins des professionnels de l'audit interne dans le monde entier, est axée sur le Code de déontologie de l'audit interne : ce comité doit le tenir à jour, en favoriser la compréhension et le respect, évaluer les plaintes relatives à la violation de ce Code, enquêter et imposer des sanctions, et promouvoir la déontologie comme partie intégrante du processus de gouvernance. Il doit effectuer une révision formelle du Code de déontologie tous les trois ans. Tout changement dans le Code de déontologie, comme l'intégration de nouvelles règles, se fait sur l'initiative de ce comité. L'adoption de nouvelles règles nécessite une période de consultation de 90 jours, durant laquelle le public peut formuler des commentaires. La validation finale revient au Conseil d'administration de l'IIA. En outre, ce comité évalue, en cas de besoin, la conduite des adhérents, des candidats à une certification professionnelle et des titulaires d'une telle certification.

L'*International Internal Auditing Standards Board* (Conseil international sur les normes d'audit interne). Ce comité a pour mission de publier, de réviser et de promouvoir les *Normes* professionnelles de l'audit interne dans le monde entier. Il doit procéder à une révision des *Normes* tous les trois ans. Il prend l'initiative de publier de nouvelles normes et de modifier les normes existantes, sur lesquelles le public peut formuler des commentaires pendant une période de consultation de 90 jours. La consultation publique implique une traduction vers l'espagnol, le français et, souvent, vers d'autres langues majeures parlées par les adhérents (par exemple, le chinois, l'italien, l'allemand, le japonais, etc.). Après prise en compte des réactions, un vote à la majorité du comité est nécessaire pour l'adoption définitive.

Le *Professional Issues Committee* (Comité des questions professionnelles). Ce comité a pour mission d'orienter la réflexion et de donner en temps voulu des lignes directrices aux membres de la profession et aux parties prenantes sur les méthodes, techniques et positions de référence incluses dans le CRIPP et de formuler des commentaires ou de soutenir des positions sur d'autres sujets qui influencent la profession d'audit interne. Il prend l'initiative des Modalités Pratiques d'Application, les rédige, les tient à jour et révise toutes les MPA existantes selon un cycle de trois ans. C'est également ce comité qui est à l'initiative des prises de position et des guides pratiques de l'IIA. Les avant-projets d'éventuelles MPA, les prises de position et les guides pratiques sont diffusés, avant publication, auprès de l'*Ethics Committee* et de l'*International Internal Audit Standards Board*, qui doivent vérifier qu'ils ne sont en rien contradictoires avec les dispositions obligatoires existantes. Les prises de position bénéficient aussi d'une période de 30 jours de consultation publique auprès des Instituts locaux de l'IIA.

Copyright © 2015 Eyrolles.

Le processus d'élaboration des dispositions obligatoires et fortement recommandées incluses dans le CRIPP est résumé à l'encadré 2-10.

Pour améliorer la transparence des lignes directrices faisant autorité pour la profession et rehausser la confiance que les législateurs, les autorités de régulation et de supervision ainsi que les autres utilisateurs des services d'audit interne y accordent, le *2006 Vision for the Future Task Force* (groupe de travail 2006 Vision pour le futur) de l'IIA a recommandé l'instauration d'un comité de surveillance indépendant. Le Conseil de surveillance du CRIPP (*IPPF Oversight Council*) représente les intérêts des parties prenantes extérieures à la profession d'audit interne et veille au respect du protocole mis en place pour l'élaboration, la publication et la mise à jour du CRIPP.[5] La majorité des membres sont des parties prenantes réputées à travers le monde, parmi lesquelles l'*International Federation of Accountants*, la Banque mondiale, l'Organisation de coopération et de développement économique (OCDE), la *National Association of Corporate Directors* (NACD) et l'*International Organisation of Supreme Audit Institutions* (INTOSAI). Les représentants du Conseil de surveillance du CRIPP observent comment les lignes directrices sont définies et certifient que les procédures prévues sont respectées avant la publication des dispositions obligatoires.

Étant donné la montée en puissance de la profession d'audit interne, le CRIPP, et plus précisément les *Normes* professionnelles de l'audit interne, sont de plus en plus largement reconnus comme la référence mondiale pour la pratique de l'audit interne.

- Le Trésor national de l'Afrique du Sud impose à toutes les entités du secteur public de pratiquer l'audit interne conformément à la définition qu'en donne l'IIA et en se référant aux *Normes*.[6]
- Le rapport King II approuve la définition de l'audit interne et les *Normes* de l'IIA pour les sociétés cotées en Afrique du Sud.[7]
- Un rapport de 2007 du Conseil de l'Europe recommande aux États membres que les fonctions d'audit interne soient établies au niveau local et régional, conformément aux normes internationales généralement acceptées, telles que celles publiées par l'IIA.[8]
- La *Finnish Financial Supervision Authority* (autorité de supervision financière finlandaise), qui régule les marchés financiers et les banques, les sociétés d'investissement et la Bourse de Finlande, impose que les entités disposent d'une fonction d'audit interne et recommande que cette fonction respecte les *Normes* de l'IIA.[9]
- Le gouvernement du Canada et ses ministères ont adopté le CRIPP pour leurs travaux de vérification interne.[10]

Copyright © 2015 Eyrolles.

ENCADRÉ 2-10

PROCESSUS D'ÉLABORATION DES DISPOSITIONS DU CRIPP

Élément du CRIPP/ responsabilité	Processus	Approbation finale
Définition		
___	Le Conseil d'administration instaure un groupe de travail spécial : 90 jours de consultation publique	Conseil d'administration de l'IIA
Code de déontologie		
Global Ethics Committee	Élaboré et actualisé par le *Global Ethics Committee* : 90 jours de consultation publique	Conseil d'administration de l'IIA
Normes internationales pour la pratique professionnelle de l'audit interne		
International Internal Audit Standards Board	Élaborées et actualisées par l'*International Internal Audit Standards Board* : 90 jours de consultation publique	*International Internal Audit Standards Board* Le Conseil de surveillance du CRIPP (IPPF *Oversight Council*) approuve le processus
Prises de position		
Professional Issues Committee	C'est essentiellement le *Professional Issues Committee* qui les élabore, mais les Instituts locaux ou d'autres comités peuvent en prendre l'initiative : – versions préliminaires examinées par l'*Ethics Committee* et le *Standards Board* pour vérifier l'absence de contradiction ; – 30 jours de consultation publique auprès des Instituts locaux.	*IIA Executive Committee*
Modalités Pratiques d'Application		
Professional Issues Committee	Élaborées et actualisées par le *Professional Issues Committee* : – versions préliminaires examinées par l'*Ethics Committee* et le *Standards Board* pour vérifier l'absence de contradiction ; – pas de soumission supplémentaire.	*Professional Guidance Advisory Council*
Guides pratiques		
Professional Guidance Advisory Council	Le *Professional Guidance Advisory Council* est chargé de leur élaboration, de leur approbation et de leur actualisation. – Le *Council* confie l'élaboration de tel ou tel guide à un comité technique international. – Versions préliminaires examinées par l'*Ethics Committee* et le *Standards Board* pour vérifier l'absence de contradiction. – Pas de soumission supplémentaire.	*Professional Guidance Advisory Council*

Copyright © 2015 Eyrolles.

Commentaire du traducteur

En France, la promulgation (2001) et l'application à toute l'administration (2006) de la Loi Organique relative aux Lois de Finance (LOLF) entraînent le développement, au sein du secteur public, d'une véritable fonction d'audit interne. Cette structuration s'est poursuivie en 2011 avec le décret du 28 juin 2011 et la circulaire du Premier ministre du 30 juin 2011 relatifs à l'audit interne dans l'administration de l'État. En juin 2013, le Comité d'harmonisation de l'audit interne a publié le Cadre de Référence de l'Audit Interne de l'État qui s'appuie très largement sur les dispositions obligatoires du CRIPP.

Au Canada, selon la politique sur la vérification interne du Conseil du Trésor du Canada (CT) en vigueur depuis le 1er avril 2012, les administrateurs généraux s'assurent « que la fonction de vérification interne du ministère est conforme à la présente politique ainsi qu'à toutes les directives ou normes qui y sont associées, y compris les Normes relatives à la vérification interne au sein du gouvernement du Canada ».

NORMES PUBLIÉES PAR D'AUTRES ORGANISATIONS

L'IIA reconnaît que d'autres organisations publient des lignes directrices qui peuvent être pertinentes pour la profession d'audit interne. De fait, certaines fonctions d'audit interne doivent respecter, en plus du CRIPP, d'autres lignes directrices pour la profession. Il s'agit, par exemple, des *Governmental Auditing Standards* (Normes d'audit public) de l'*U.S. Government Accountability Office* (GAO), des *Standards for the Professional Practice of Environmental, Health and Safety Auditing* (Normes pour la pratique professionnelle de l'audit concernant l'environnement, la santé et la sécurité) et des normes publiées par l'Organisation internationale de normalisation (ISO). Ainsi, aux États-Unis, il n'est pas rare que des organismes publics locaux et d'État incorporent dans leur charte les *Normes* de l'IIA et les *Governmental Auditing Standards* (*Yellow Book*) publiés par le *Government Accountability Office*.

U.S. GAO (*Government Accountability Office*)

Organisme qui publie des normes relatives aux audits publics (*Yellow Book*).

L'introduction aux *Normes* professionnelles de l'audit interne indique la marche à suivre lorsque plusieurs normes s'appliquent :

> *« Si les* Normes *sont conjointement utilisées avec des dispositions d'autres organes de référence, les communications de l'audit interne peuvent, le cas échéant, citer l'utilisation d'autres normes. S'il y a des contradictions entre les* Normes *et ces autres dispositions, les auditeurs internes et l'audit interne doivent se conformer aux* Normes *et peuvent respecter les autres dispositions si celles-ci sont plus exigeantes. »*

Les *Normes* professionnelles de l'audit interne sont des principes obligatoires, conçus pour être utilisés par l'audit interne dans une multitude d'organisations opérant au sein d'environnements juridiques et culturels variés. C'est pourquoi il existe peu voire pas de conflit direct entre les *Normes* professionnelles de l'audit interne et les normes publiées par d'autres organisations professionnelles.

Copyright © 2015 Eyrolles.

ISACA (*Information Systems Audit and Control Association*)

Organisme qui publie des normes, règles et procédures relatives à l'audit des systèmes d'information.

Lorsqu'il existe des différences, il s'agit généralement de règles plus exigeantes pour un principe particulier. Ainsi, la Norme S9.10 de l'ISACA (*Information Systems Audit and Control Association*) impose aux auditeurs des systèmes d'information d'obtenir, au moins tous les ans, une déclaration écrite qui reconnaisse la responsabilité du management dans la conception et la mise en œuvre du contrôle interne afin de prévenir et de détecter tout acte illégal.[11] Les *Normes* professionnelles de l'audit interne n'imposent pas spécifiquement d'obtenir une déclaration écrite de la part du management, mais l'obtention de ce document n'est nullement contradictoire avec ces *Normes*.

Normes relatives à l'audit interne des administrations publiques. Aux États-Unis, le *Government Accountability Office* (GAO) publie des normes destinées aux audits des entités publiques, généralement appelées normes du *Yellow Book* (normes du livre jaune) en raison de la couverture jaune de l'ouvrage qui les compile. Les normes du *Yellow Book* s'appliquent aux audits financiers fédéraux, aux audits de performance (ou opérationnels) et à d'autres activités liées à l'audit. La législation fédérale américaine impose aux auditeurs, travaillant au niveau fédéral ou non, de se conformer aux normes du *Yellow Book* pour les audits des organisations, programmes et fonctions fédéraux. Ces normes sont généralement pertinentes, et leur utilisation est recommandée, pour les auditeurs ou experts-comptables des entités publiques à l'échelon local ou des États, pour la plupart des audits d'administrations publiques à l'échelon local ou de l'État. Le *Yellow Book* reconnaît explicitement que les *Normes* professionnelles de l'audit interne sont pertinentes pour l'audit des entités publiques ; cependant, en cas de conflit ou lorsque les normes du *Yellow Book* sont plus strictes, il impose le respect de ces dernières. Par exemple, selon les *Normes* professionnelles de l'audit interne, des évaluations externes doivent être effectuées tous les cinq ans, mais le *Yellow Book* en fixe la fréquence à trois ans.

À l'instar des États-Unis, la plupart des pays disposent d'un ensemble de normes destinées à l'audit des entités et marchés publics. Beaucoup ont pris modèle sur les principes établis par l'*International Organization of Supreme Audit Institution* (INTOSAI). Tout comme le *Yellow Book*, ces normes tendent à se concentrer sur les audits de performance et financiers à l'intention des utilisateurs extérieurs.

Normes relatives à l'audit des systèmes d'information. L'audit des systèmes d'information informatisés fait partie intégrante du travail de l'audit interne. Bien que les *Normes* professionnelles de l'audit interne procurent un cadre de référence suffisant pour l'audit des systèmes informatisés, l'ISACA (*Information Systems Audit and Control Association*) donne des lignes directrices plus détaillées et plus spécialisées. Les Normes de l'ISACA sont tout à

Copyright © 2015 Eyrolles.

fait similaires aux *Normes* professionnelles de l'audit interne, à ceci près qu'elles s'appliquent à un domaine bien plus précis. L'ISACA publie des « normes », des « règles » et des « outils et techniques d'assurance et d'audit des systèmes d'information » relatifs à l'audit des systèmes d'information. Les « règles » de l'ISACA énoncent des informations plus spécifiques sur la manière d'appliquer ces « normes » et requièrent que l'on justifie tout écart le cas échéant. Les « outils et techniques d'assurance et d'audit des systèmes d'information » donnent des exemples de ce qu'un auditeur des systèmes d'information est amené à faire lorsqu'il réalise une mission d'audit, mais il ne s'agit pas d'impératifs. À l'heure actuelle, il n'y a pas d'incompatibilité entre les Normes de l'ISACA et les *Normes* professionnelles de l'audit interne. Les fonctions d'audit interne qui travaillent sur les systèmes d'information doivent avoir connaissance des lignes directrices de l'ISACA et envisager de les adopter pour leur travail d'audit sur les systèmes d'information.

Normes pour la pratique professionnelle de l'audit concernant l'environnement, la santé et la sécurité. Le *Board of Environmental, Health and Safety Auditor Certifications* (BEAC, Conseil de certification des auditeurs de l'environnement, de la santé et de la sécurité) a établi des *Standards for the Professional Practice of Environmental, Health and Safety Auditing* (Normes pour la pratique professionnelle de l'audit concernant l'environnement, la santé et la sécurité) visant à répondre aux besoins des professionnels de l'audit dans les domaines de l'environnement, de la santé et de la sécurité. Dans certaines organisations, ce sont des services autres que l'audit interne qui donnent l'assurance que l'organisation respecte les lois et règlements relatifs à la protection de l'environnement, à la santé et à la sécurité. D'autres organisations estiment qu'il est de la responsabilité de l'audit interne de donner cette assurance. Lorsque l'audit interne effectue une mission portant sur l'environnement, la santé ou la sécurité, il peut s'appuyer sur les Normes du BEAC pour orienter son action. Celles-ci ne sont pas contradictoires avec les *Normes* professionnelles de l'audit interne.

BEAC (*Board of Environmental, Health, and Safety Auditor Certifications*)

Conseil de certification qui publie des normes visant à répondre aux besoins des professionnels de l'audit dans les domaines de l'environnement, de la santé et de la sécurité.

Normes relatives aux audits financiers. Actuellement, ce sont le *Public Company Accounting Oversight Board* (PCAOB) et l'*American Institute of Certified Public Accountants* qui fixent les normes relatives aux audits des états financiers des organisations aux États-Unis. Dans d'autres pays, des normes pour les audits des états financiers sont également fixées séparément. Cependant, comme pour les normes comptables, certaines initiatives tentent d'harmoniser les normes d'audit financier entre plusieurs pays. Ainsi, l'*International Auditing and Assurance Standards Board* (IAASB, Conseil des normes internationales d'audit et d'assurance), qui fait partie de l'*International Federation of Accountants* (IFAC), publie des normes d'audit internationales qui sont adoptées par un certain nombre de pays. Bien que ces normes concernent directement

PCAOB (*Public Company Accounting Oversight Board*) et AICPA (*American Institute of Certified Public Accountants*)

Organismes qui publient les normes relatives aux audits des états financiers des organisations aux États-Unis.

Copyright © 2015 Eyrolles.

IFAC (*International Federation of Accountants*)

Organisme qui publie des normes d'audit internationales adoptées par un certain nombre de pays.

l'audit externe des états financiers, elles peuvent également avoir une influence sur les travaux d'audit interne, en particulier pour les normes qui portent sur la coordination entre l'audit interne et externe.

Commentaire du traducteur

En France, la Loi de Sécurité Financière (2003) a confié l'élaboration des Normes d'exercice professionnel (NEP) à la Compagnie nationale des commissaires aux comptes (CNCC), qui les transmet au Garde des Sceaux pour homologation après avis du Haut Conseil du Commissariat aux Comptes (H3C).

Autres lignes directrices pertinentes. Les lignes directrices publiées par d'autres organisations professionnelles peuvent également se révéler pertinentes pour les auditeurs internes.

- L'Organisation internationale de normalisation (ISO) définit des normes pour les audits qualité et environnementaux.
- *Standards Australia* publie des normes sur les processus de gouvernance et de gestion des risques.
- Le *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) a édité des référentiels ayant spécifiquement trait au contrôle interne et à la gestion des risques.
- La *Society of Corporate Compliance and Ethics* (SCCE) formule des lignes directrices à l'intention des spécialistes de la déontologie et de la conformité.
- La *Health Care Compliance Association* (HCCA) propose des normes de conformité à l'intention des professionnels du secteur de la santé.
- Le Comité de Bâle sur le contrôle bancaire a établi des normes spécifiques (appelées Bâle I, Bâle II et Bâle III) pour l'audit interne des systèmes de gestion des risques et d'évaluation des établissements bancaires et financiers.

Commentaire du traducteur

En France, l'AMF (Autorité des marchés financiers) a publié le cadre de référence de gestion des risques et du contrôle interne qui s'applique à toute société cotée.

Ce ne sont là que quelques-unes des organisations qui publient des lignes directrices pertinentes pour les auditeurs internes. Ces derniers doivent avoir connaissance de ces organisations et de la nature des lignes directrices qu'elles publient. Les auditeurs internes qui opèrent dans certains pays ou dans certains secteurs doivent être au courant des lignes directrices existantes autres que le CRIPP de l'IIA et qui sont pertinentes pour leurs travaux.

Copyright © 2015 Eyrolles.

RÉSUMÉ

Ce chapitre visait à présenter en détail le Cadre de référence international des pratiques professionnelles de l'audit interne (CRIPP). Ce cadre de référence contient deux types de dispositions : des dispositions obligatoires et des dispositions fortement recommandées, qui permettent à l'audit interne d'effectuer des activités d'assurance et de conseil créatrices de valeur ajoutée. Les dispositions obligatoires sont la définition de l'audit interne, le Code de déontologie et les *Normes*. Les dispositions fortement recommandées sont constituées des Modalités Pratiques d'Application, des prises de position et des guides pratiques. Ce chapitre présente en outre le processus par lequel les Instituts d'audit interne tiennent à jour et développent le CRIPP, ainsi que les lignes directrices publiées par des organisations professionnelles autres que l'IIA et susceptibles d'intéresser les auditeurs internes.

Le Code de déontologie expose les principes déontologiques et les règles de comportement pertinents pour la pratique de l'audit interne. Les Normes de qualification permettent de comprendre les caractéristiques essentielles que doivent regrouper la fonction d'audit interne et les auditeurs internes pour proposer des activités d'assurance et de conseil efficaces. Les Normes de fonctionnement donnent les lignes directrices de référence sur la manière de gérer l'audit interne et de mener des missions d'assurance et de conseil. Les Normes de mise en œuvre précisent les Normes de qualification et les Normes de fonctionnement, en donnant des orientations qui s'appliquent soit aux activités d'assurance soit aux activités de conseil. Les Modalités Pratiques d'Application, les prises de position et les guides pratiques donnent des orientations utiles aux auditeurs internes lorsqu'ils appliquent la définition de l'audit interne, le Code de déontologie et les *Normes* professionnelles de l'audit interne. Enfin, les normes publiées par d'autres organisations qui sont pertinentes pour les auditeurs internes ont été présentées.

Le CRIPP, en particulier les *Normes* professionnelles de l'audit interne et les Modalités Pratiques d'Application, seront examinés de façon plus approfondie dans la suite de cet ouvrage.

Copyright © 2015 Eyrolles.



Questions de révision

1. Comment la nécessité de parler d'activités d'audit interne est-elle apparue ?

2. Quelles sont les six composantes du Cadre de référence international des pratiques professionnelles de l'audit interne ? Quelles sont les dispositions obligatoires ? Quelles sont les dispositions fortement recommandées ?

3. En vous appuyant sur la proposition de valeur de l'audit interne, expliquez en quoi celui-ci crée de la valeur ajoutée pour l'organisation.

4. Quel est l'objectif du Code de déontologie ?

5. Énoncez les quatre principes fondamentaux du Code de déontologie. Pourquoi les auditeurs internes doivent-ils s'efforcer de respecter ces règles ?

6. Quel est l'objectif des *Normes* professionnelles de l'audit interne ? Expliquez la différence entre Normes de qualification et Normes de fonctionnement.

7. Quelle est la différence entre activités d'assurance et activités de conseil ? Pourquoi les Normes de mise en œuvre ne sont-elles pas les mêmes dans les deux cas ?

8. Quelle est la définition de l'indépendance dans son acception relative à l'audit interne ? Quelle est la définition de l'objectivité dans son acception relative à l'audit interne ?

9. Que signifie l'expression « conflits d'intérêts » ? Comment ces conflits d'intérêts surviennent-ils ?

10. Que signifie le terme « compétence » ? Que signifie l'expression « conscience professionnelle » ?

11. Quel est l'objectif du programme d'assurance et d'amélioration qualité de la fonction d'audit interne ?

12. Quelles sont les sept grandes sections des Normes de fonctionnement ?

13. Identifiez les Normes de fonctionnement qui ont spécifiquement trait aux points suivants :
    a. planification de la mission ;
    b. accomplissement de la mission ;
    c. communication des résultats.

14. Quelle est la relation entre les *Normes* et les Modalités Pratiques d'Application ?

Copyright © 2015 Eyrolles.

Questions de révision

15. Définissez les prises de position. Définissez les guides pratiques.

16. Quelles sont les responsabilités du *Professional Guidance Advisory Council* ?

17. Précisez la mission des comités suivants :
    a. *Global Ethics Committee* ;
    b. *International Internal Audit Standards Board* ;
    c. *Professional Issues Committee*.

18. Quelles organisations, autres que l'IIA, ont publié des lignes directrices pertinentes pour les auditeurs internes ?

Copyright © 2015 Eyrolles.

Questions à choix multiples

Sélectionnez la meilleure réponse pour chacune des questions suivantes.

1. L'un des principaux objectifs des *Normes* professionnelles de l'audit interne est de :
   a. Promouvoir la coordination des efforts d'audit interne et externe.
   b. Proposer une base pour l'évaluation des performances de l'audit interne.
   c. Renforcer la cohérence dans les pratiques d'audit interne.
   d. Codifier les pratiques existantes.

2. Dans le CRIPP, lesquels des éléments suivants sont des « dispositions obligatoires » ?
   I. Les Modalités Pratiques d'Application.
   II. Le Code de déontologie.
   III. La définition de l'audit interne.
   IV. Les *Normes* professionnelles de l'audit interne.
   a. I, II et IV
   b. II et IV.
   c. II, III et IV.
   d. I, II, III et IV.

3. Un auditeur interne procure des services relatifs à l'impôt sur le revenu pendant la période des déclarations fiscales. Pour laquelle des activités suivantes considérera-t-on plus vraisemblablement que l'auditeur interne viole le Code de déontologie ?
   a. Remplir, contre rémunération, la déclaration d'impôts sur le revenu personnelle de l'un des managers d'une division de l'organisation.
   b. Être invité par une station de radio locale pour débattre de questions fiscales et de planification de la retraite.
   c. Être rémunéré pour dispenser un cours du soir sur la fiscalité à l'Institut universitaire voisin.
   d. Travailler le week-end pour un ami qui possède un petit cabinet d'expert-comptable.

4. Un auditeur interne est en train d'auditer une division dont le directeur financier est un ami intime. L'auditeur apprend que son ami doit être remplacé après une série de négociations pour un contrat sensible avec le ministère de la Défense et relaie cette information à son ami. Quel est le principe du Code de déontologie qui a été violé ?
   a. L'intégrité.
   b. L'objectivité.
   c. La confidentialité.
   d. La vie privée.

Copyright © 2015 Eyrolles.

Questions à choix multiples

5. Lors de l'exécution d'une mission d'assurance, les *Normes* professionnelles de l'audit interne requièrent que l'auditeur interne fasse preuve de conscience professionnelle. Parmi les propositions suivantes, laquelle désigne un élément que l'auditeur interne peut laisser de côté lorsqu'il détermine en quoi consiste l'exercice de la conscience professionnelle dans les missions d'assurance concernant des opérations de trésorerie ?
   a. Le comité d'audit souhaite être assuré que les opérations de trésorerie sont bien conformes à une nouvelle politique appliquée aux instruments financiers.
   b. La direction de la trésorerie n'a pas mis en place de politique de gestion des risques.
   c. Les auditeurs externes demandent à voir le rapport et les papiers de travail de la mission.
   d. La fonction de trésorerie vient d'achever la mise en place d'un nouveau système de suivi des investissements en temps réel.

6. Dans laquelle des situations suivantes l'auditeur interne risque-t-il de manquer d'objectivité ?
   a. Un collaborateur de la comptabilité de la paie aide un auditeur interne à vérifier le stock physique des petits moteurs.
   b. Un auditeur interne discute d'un problème significatif avec le vice-président à qui l'audité rend compte, avant de rédiger son rapport d'audit.
   c. Un auditeur interne recommande des normes de contrôle et des mesures de performance pour un contrat avec une organisation chargée du traitement de la paie et des avantages sociaux.
   d. Un ancien membre du service Achats examine le contrôle interne relatif aux achats quatre mois après avoir été transféré au service d'audit interne.

7. Parmi les éléments suivants, lequel ou lesquels fait/font partie des *Normes* ?
   I. Les déclarations.
   II. Les interprétations.
   III. Le glossaire.
   a. I uniquement.
   b. I et II.
   c. I et III.
   d. I, II et III.

Copyright © 2015 Eyrolles.

8. D'après les *Normes*, à quoi le responsable de l'audit interne doit-il penser lorsqu'il prête attention à la conscience professionnelle, lors de la planification d'une mission d'assurance ?
   a. L'opportunité pour les collaborateurs de l'audit interne d'effectuer une formation croisée.
   b. Le coût de la mise en place de contrôles par rapport aux avantages escomptés.
   c. Les opportunités d'emploi dans des services qui peuvent être intéressants pour les auditeurs internes affectés à la mission.
   d. La possibilité de proposer des activités de conseil à l'audité.

9. Parmi les différentes catégories de dispositions suivantes du CRIPP, laquelle ou lesquelles doit/doivent être soumise(s) aux divers Instituts nationaux de l'IIA avant d'être publiée(s) ?
   I. Une nouvelle Modalité Pratique d'Application.
   II. Une nouvelle Norme.
   III. Une nouvelle prise de position.
   IV. Une nouvelle définition dans le glossaire des *Normes*.
   a. III uniquement.
   b. II et IV.
   c. II, III et IV.
   d. I, II, III et IV.

10. Lequel des éléments suivants est nécessaire pour que l'audit interne puisse fonctionner conformément aux *Normes* ?
   a. Évaluer tous les ans l'efficacité du comité d'audit.
   b. Publier tous les ans une opinion globale sur l'adéquation du système de contrôle interne de l'organisation.
   c. Obtenir une déclaration annuelle reconnaissant la responsabilité du management dans la conception et la mise en œuvre des contrôles destinés à empêcher les actes illégaux.
   d. Déterminer si la gouvernance des systèmes d'information vient étayer et renforcer les stratégies et objectifs de l'organisation.

Copyright © 2015 Eyrolles.

Thèmes de discussion

1. Pourquoi est-il important qu'une profession telle que l'audit interne publie des normes ?

2. Référez-vous à l'annexe A, « Le Code de déontologie », et répondez aux questions suivantes :
   a. Pourquoi est-il important que la profession d'audit interne se dote d'un code de déontologie ?
   b. En quoi les principes fondamentaux diffèrent-ils des règles de conduite ?
   c. Qui doit respecter le Code de déontologie ?
   d. Quelles sont les conséquences d'une violation du Code de déontologie ?

3. En quoi le Code de déontologie diffère-t-il des *Normes* dans la manière de régir le comportement et les activités des auditeurs internes ?

4. La participation d'un responsable de l'audit interne à un programme de stock-options constitue-t-elle une violation du Code de déontologie ou des *Normes* ? Expliquez votre réponse.

5. Le responsable de l'audit interne de Sargon Products est rattaché administrativement au directeur financier, et sur le plan fonctionnel, au comité d'audit. Le périmètre des activités d'assurance de l'audit interne inclut des missions financières, opérationnelles et sur la conformité.
   Y a-t-il atteinte à l'objectivité de l'auditeur interne dans chacune des situations décrites ci-dessous ? Explicitez brièvement votre réponse.
   a. On demande souvent aux auditeurs internes d'enregistrer des écritures comptables relatives à des transactions complexes, pour lesquelles les comptables de l'organisation n'ont pas l'expertise suffisante.
   b. Un comptable effectue le rapprochement des relevés bancaires mensuels de l'organisation. Un auditeur interne examine ces rapprochements afin de s'assurer qu'ils ont été réalisés correctement.

6. Examinez l'encadré 2-8 et répondez aux questions suivantes :
   a. Pourquoi est-il important que l'audit interne dispose d'une charte ?
   b. Quelles informations la charte d'audit interne doit-elle contenir ?

Copyright © 2015 Eyrolles.

7. Vous faites partie d'un service d'audit interne qui compte trois personnes et le directeur général de votre organisation vous demande d'auditer le contrôle interne des activités de négociation et de couverture sur les matières premières de l'organisation ; or, personne au sein du service ne dispose d'une formation dans ce domaine.
   a. Reportez-vous à l'annexe B, « Les *Normes internationales pour la pratique professionnelle de l'audit interne* ». Quelle(s) norme(s) consulteriez-vous pour obtenir des orientations par rapport à la situation décrite ci-dessus ? Expliquez.
   b. Reportez-vous à la liste des Modalités Pratiques d'Application sur le site Internet de l'IIA (www.theiia.org) ou d'autres Instituts (par exemple, www.ifaci.com). Quelle(s) Modalité(s) Pratique(s) d'Application consulteriez-vous pour obtenir des orientations ? Expliquez.

Copyright © 2015 Eyrolles.

CAS N° 1

En 1999, le *Wall Street Journal* (7 avril 1999, page c1) décrivait l'affaire (désormais réglée) U.S. Securities Exchange Commission (SEC) contre W.R. Grace & Co., la SEC affirmant que l'organisation s'était livrée à de la « gestion de bénéfices » dans son unité National Medical Care.

Au début des années 1990, les cadres de W.R. Grace & Co. ont eu des doutes quant aux performances de l'unité National Medical Care Inc. de l'organisation. Le problème était le suivant : les résultats progressaient trop vite. Les bénéfices augmentaient de plus de 30 % par an, dépassant donc l'objectif de croissance de l'unité. Alors que la plupart des organisations se seraient extasiées devant ces résultats, les cadres de Grace ont craint que l'unité ne puisse les pérenniser. Ils ont donc discrètement escamoté ces bénéfices excédentaires dans une réserve à usage général, dans laquelle ils pourraient puiser ultérieurement d'une façon qui masque les problèmes réels, notamment le ralentissement des bénéfices.

Cette accumulation de bénéfices a rapidement été découverte par les auditeurs externes, qui ont, à plusieurs reprises, indiqué à Grace que ce n'était pas bien, comme le montrent les notes internes du Cabinet d'audit. Mais au lieu de tenir bon, les comptables ont déclaré que les états financiers étaient satisfaisants…

Les notes internes de l'organisation et du Cabinet d'audit, ainsi que les extraits des dépositions, font apparaître un dysfonctionnement du contrôle interne chez Grace et des distorsions bien plus graves dans les bénéfices que ce qui avait été mis au jour précédemment. Au moins six auditeurs externes et Norman Eatough, ancien responsable de l'audit chez Grace, ont mis en doute la légalité des opérations comptables chez Grace…

Certains professionnels soulignent que l'initiative de la SEC revient à faire beaucoup de bruit pour très peu, remarquant que les organisations ont une certaine marge de manœuvre pour adopter les techniques comptables qui leur permettront d'afficher des bénéfices réguliers, tant que ces ajustements ne sont pas « importants ». C'est un élément assez flou des règles de présentation de l'information dans la législation sur les valeurs mobilières ; les comptables définissent souvent les ajustements importants comme les événements qui ont un impact sur les bénéfices supérieurs à 5 ou 10 %.

« N'importe quel directeur financier a géré les bénéfices d'une façon qui, aujourd'hui, mettrait la SEC dans tous ses états, et la pousserait à crier à la fraude », affirme Wallace Timmeny, juriste…

Pendant ce temps, M. Eatough, responsable de l'audit interne chez Grace, s'inquiétait de plus en plus (dans un rapport au directeur financier, il a mis en évidence ce qu'il a appelé un « report délibéré de revenus comptabilisés »). Cependant, craignant pour son poste, il s'est abstenu d'employer le mot « fraude »…[12]

Copyright © 2015 Eyrolles.

Que conseilleriez-vous à M. Eatough de faire dans cette situation ? Justifiez votre conseil par les orientations fournies dans le CRIPP, avec des renvois à des sections précises des *Normes* et du Code de déontologie, et en prenant en compte d'autres considérations pratiques.

CAS N° 2[13] Mark Hobson est un auditeur interne employé chez Comstock Industries. Il s'apprête à achever l'audit de la division Avil, mené sur les cinq premières semaines de l'année. La division Avil est l'une des trois divisions de production de Comstock ; elle fabrique des stocks permettant de fournir environ 50 % des ventes de Comstock. Outre les divisions de production, Comstock compte deux divisions de marketing (national et international) et une division de service technique qui offre un soutien technique à travers le monde. Chaque client est dirigé vers la division de production la mieux adaptée, qui fait office de fournisseur pour ce client. La division production décide ensuite du crédit à accorder à ce client, expédie la marchandise sur la base d'un bon de commande obtenu du représentant commercial et collecte les sommes à percevoir du client au moment où elles sont dues. Cette méthode permet de vérifier commande après commande que le plafond du crédit n'est pas dépassé sur la base des commandes reçues du client.

Deux observations potentielles

Deux éléments inquiètent Mark. Premièrement, un volume important (en valeur) du stock de pièces A2 était toujours dans les comptes Avil à la fin de l'exercice, alors que le composant de la machine Fasttac, dans lequel étaient utilisées les pièces A2, est désormais considéré comme faisant partie de la première génération, et n'est donc plus fabriqué. La politique de l'organisation requiert une sortie immédiate du bilan de tous les éléments de stock obsolètes. Deuxièmement, certains comptes clients toujours répertoriés comme recouvrables à la fin de l'exercice dataient de plus de 180 jours. Toutes les créances clients sont dues sous 30 jours, ce qui est la règle dans le secteur. Mark pense que nombre de ces créances anciennes sont irrécouvrables.

C'est l'assistante administrative du manager de la division, Brenda Wilson, qui a effectué le classement par échéance des créances clients et non le comptable de la division, comme c'est la pratique. Ce dernier a refusé de discuter des circonstances des actes de Brenda.

Commentaire de l'audité

Mark a programmé un rendez-vous avec Brenda pour discuter des points qui lui posent problème.

Copyright © 2015 Eyrolles.

« — Eh bien, Mark, répond Brenda, je sais que la politique requiert que les éléments de stock obsolètes soient sortis du bilan, mais en ce qui concerne la pièce A2, c'est juste qu'elle n'est pas utilisée en ce moment. Il se peut que nous recommencions à fabriquer ces composants du Fast-tac. Qui sait ? Les cravates larges sont de nouveau à la mode, n'est-ce pas ? Fast-tac pourrait bien en faire autant. Il y a beaucoup de clients, en particulier dans le tiers monde, qui trouvent que ces machines de deuxième et de troisième générations coûtent très cher à entretenir. Ce que je veux dire, c'est qu'il y a une politique qui indique qu'un élément de stock obsolète doit être sorti du bilan, mais qu'il n'y en a aucune qui définit ce qu'est une pièce obsolète.

— Et pour ce qui est de ces créances clients, poursuit-elle, c'est certainement là aussi une décision arbitraire. Qui sait si ces créances seront recouvrées ? On est un peu en récession, en ce moment, mais quand les choses commenceront à se redresser, nous parviendrons sûrement à en recouvrer quelques-unes. Il n'y a même pas une politique, dans cette division, sur les sorties de bilan, j'ai vérifié. Rien ne dit que je dois les sortir du bilan. Alors, de quel droit pouvez-vous me dire ce que j'ai à faire ?

— Brenda, soyez honnête. Vous savez bien que ces pièces ne seront plus jamais utilisées. Et vous savez que ces créances sont irrécouvrables.

— Écoutez, Mark, concède Brenda, on n'est qu'à deux semaines de la clôture de l'exercice. Laissons les choses en l'état jusqu'à après clôture, comme ça, tout le monde pourra avoir sa prime. Après, je le promets, je me pencherai à nouveau sur les stocks et les créances. Je les sortirai du bilan après la fin de l'exercice, après la publication des états financiers. Personne ne sera au courant. Et après tout, ça ne fait de mal à personne, n'est-ce pas ? »

Le manager de la division

Mark poursuit son audit, rédige son rapport avec les observations concernant le stock et les créances clients, et le passe en revue avec le manager de la division, Hal Wright. Hal est manifestement perturbé.

« — Dites donc, Mark, cela n'aurait pas pu tomber à un plus mauvais moment. Nos chiffres viennent d'être acceptés par les auditeurs externes. Il y avait un gars, là-bas, pour faire le dénombrement des stocks en novembre et Brenda a déjà envoyé son tableur sur les créances clients en fin d'exercice au siège. Personne là-haut, ni dans notre groupe ni dans l'équipe d'audit du cabinet d'experts-comptables, n'a émis la moindre critique. Si vous commencez à remuer tout ça, surtout maintenant, on va se faire attraper par les auditeurs externes avec nos sorties de bilan et nos créances clients, ils vont corriger les bénéfices et ça va coûter extrêmement cher à tout le monde. Et, Mark, admettez que la question n'est pas non plus vraiment tranchée. Je veux dire, vous pourriez rédiger un rapport qui appelle à une politique plus claire, mais pas à des sorties de bilan spécifiques. C'est à des kilomètres de votre

Copyright © 2015 Eyrolles.

champ d'intervention. Je vous le promets, nous regarderons tout cela après que nos états auront été acceptés. Mais pour le moment, je pense que les managers de la division ont travaillé dur et j'ai l'intention de me battre pour protéger la petite prime qu'ils vont bientôt recevoir. Si nous procédons aux sorties de bilan, comme vous le suggérez, ces primes partiront en fumée et les actionnaires vont y perdre aussi. Le bénéfice par action va dégringoler. Ils pourraient même fermer la division. Ce n'est pas ce que vous voulez, n'est-ce pas ?

— Eh bien, Hal, je pourrais formuler mes observations comme dans le projet de rapport, mais y ajouter votre réponse. » Soudain, Hal se met en colère. « Quoi ? Et laisser les membres du comité d'audit statuer sur cette question ? Ils n'ont rien à voir avec cela. Ils ont accepté le rapport du Cabinet d'audit. Si vous voulez que le comité d'audit soit content, écoutez-moi et laissez tomber cette histoire d'ajustement. »

La directrice de l'audit interne

Soucieux, Mark a repoussé la finalisation de son rapport et discuté de sa version préliminaire avec Gail Wu, directrice de l'audit interne. Gail n'est pas auditrice de formation : elle a été promue directrice de l'audit interne depuis le service financier de l'organisation, afin qu'elle comprenne mieux les relations opérationnelles. Gail est néanmoins très intelligente, et Mark a toujours respecté son opinion. La discussion s'est tenue par téléphone, Mark étant toujours au siège de la division Avil, et Gail dans les bureaux de l'organisation.

« — Mark, Hal a raison. Si, au final, vous dénoncez les primes du management, nous pouvons dire adieu à toute la survaleur que je me suis efforcée de bâtir pour ce service. Tout sera directement jeté par les fenêtres.

— Gail, je sais que vous essayez d'améliorer la situation, mais Hal est intraitable. En ce qui le concerne, la seule observation qu'il est prêt à accepter dans le rapport concernerait les déficiences de la politique, sans qu'il soit fait mention de l'ajustement nécessaire sur le stock ou les créances clients. »

Et Gail de mettre un terme à la discussion…

« Eh bien, faites ce que vous avez à faire. Mais j'insiste pour que vous soumettiez un rapport qu'Hal ait accepté et signé. Je ne veux pas mettre le feu aux poudres. Je ne veux pas avoir à expliquer au Conseil que je dois gérer des électrons libres alors que tout le monde pleure après sa prime. »

1. Référez-vous au Code de déontologie. Identifiez *trois* règles de conduite pertinentes dans ce cas. En prenant ces règles de conduite comme contexte, discutez des questions éthiques soulevées par cette affaire.

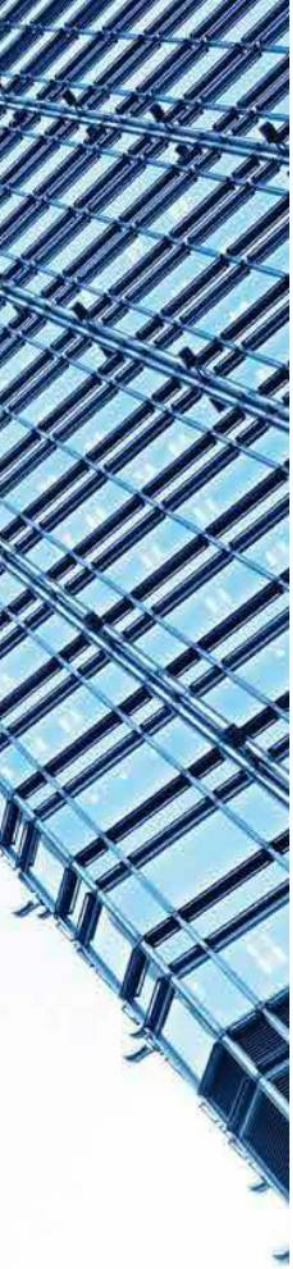
Copyright © 2015 Eyrolles.

2. Indiquez comment le dilemme déontologique auquel Mark est confronté aurait pu être évité. En d'autres termes, discutez de ce que le management de Comstock et/ou l'audit interne auraient pu faire pour réduire le risque de survenue d'une telle situation.

3. Indiquez clairement ce que vous feriez si vous vous trouviez à la place de Mark. Expliquez brièvement pourquoi.

Copyright © 2015 Eyrolles.





CHAPITRE 3
LA GOUVERNANCE

Objectifs pédagogiques

- Définir la gouvernance et comparer les différents rôles et responsabilités.
- Bien appréhender les divers principes de gouvernance applicables à toute l'organisation.
- Décrire les évolutions réglementaires et leur impact sur la gouvernance jusqu'à son état actuel.
- Décrire le rôle de la fonction d'audit interne dans le processus de gouvernance.
- Savoir où trouver l'information à propos des codes et de la réglementation relatifs à la gouvernance dans les pays du monde entier.

Commentaire du traducteur

Dans ce document, nous utilisons indifféremment les termes « gouvernement d'entreprise » et « gouvernance » pour traduire le terme governance.

ENCADRÉ 3-1

DISPOSITIONS DU CRIPP PERTINENTES RELATIVES AU CHAPITRE 3

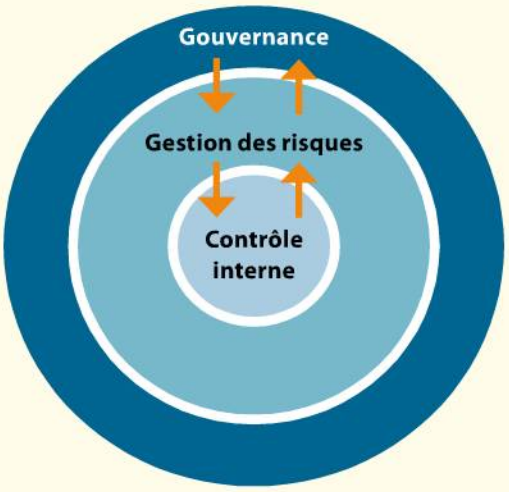
Norme 2010 – Planification
Norme 2100 – Nature du travail
Norme 2110 – Gouvernement d'entreprise
Guide pratique : *Interaction with the Board*
Guide pratique : *Assessing Organizational Governance in the Private Sector*

Pour réussir, toute organisation doit mettre en place un cadre de référence générique pour ses décisions, qu'elles soient à long terme ou au jour le jour. Pensez à la façon dont est structurée une université, ou l'organisation pour laquelle vous avez travaillé. Réfléchissez aux clubs ou aux équipes de sport dont vous avez fait partie. Tous avaient une forme de structure qui les a aidés à réussir.

Dans la plupart des organisations, l'audit interne peut constituer l'un des déterminants essentiels de ce succès. Mais pour bien comprendre comment, il vous faut au préalable appréhender la façon dont les organisations sont structurées et opèrent pour réussir. Certes, la structure effective de l'organisation varie d'une entité à l'autre, mais toutes doivent établir une structure de gouvernance d'ensemble afin de satisfaire les besoins des principales parties prenantes. Cette structure de gouvernance encadre les activités de ceux qui se chargent quotidiennement de la gestion des risques inhérents au modèle économique de leur organisation, à savoir le contrôle interne. Ces éléments sont illustrés dans l'encadré 3-2.

ENCADRÉ 3-2

PRINCIPAUX ÉLÉMENTS DE LA GOUVERNANCE



Comme le montre cette illustration, toutes les activités d'une organisation ont des enjeux de gouvernance. La structure de gouvernance peut être axée sur le respect des lois et règlements des juridictions dans lesquelles l'organisation opère. Les lois et règlements visent généralement la protection de l'intérêt général. En outre, le Conseil et la direction générale d'une organisation peuvent définir les structures de gouvernance de manière à ce que les besoins des principales parties prenantes soient satisfaits et que l'organisation opère dans les limites et conformément aux valeurs fixées par le Conseil et la direction générale.

La gestion des risques constitue la strate suivante de la structure de gouvernance. Elle vise à :

- détecter et à gérer les risques susceptibles d'entraver la réussite de l'organisation ;
- à exploiter les opportunités qui conduisent au succès.

Copyright © 2015 Eyrolles.

Le management élabore des stratégies afin d'optimiser la gestion des principaux risques et opportunités. Les activités de gestion des risques doivent suivre la direction globale imposée par la structure de gouvernance. La gestion des risques est traitée en détail au chapitre 4, intitulé *La gestion des risques*.

Dans l'encadré 3-2, le contrôle interne est représenté au centre, car le système de contrôle interne constitue une sous-catégorie, et fait partie intégrante, des activités de gestion des risques. Le traitement des risques, qui inclut les contrôles, a pour but de mettre en œuvre les stratégies de gestion des risques. Pour de plus amples informations sur les contrôles et le système de contrôle interne, voir le chapitre 6, *Le contrôle interne*.

Enfin, les flèches représentent la circulation de l'information à travers toute la structure de gouvernance. Le Conseil imprime une orientation à la direction générale, pour la guider dans l'exécution des activités de gestion des risques. La direction générale donne à son tour une orientation au niveau de management responsable des activités de contrôles spécifiques. Les managers intermédiaires rendent compte à la direction générale de la réussite de ces contrôles. Et il revient à la direction générale elle-même de fournir au Conseil une assurance concernant l'efficacité des activités de gestion des risques. Les flèches à l'intérieur de l'encadré montrent les flux d'orientation et de responsabilité d'un niveau à l'autre.

Le présent chapitre décrit précisément la gouvernance, dont il expose les composantes et principes clés, ainsi que les rôles et responsabilités qui y ont trait. Des illustrations permettent de décrire, de manière plus approfondie, comment envisager les principaux éléments de la gouvernance. Ce chapitre analyse aussi le rôle d'assurance de la fonction d'audit interne dans la gouvernance, ainsi que celui que peuvent jouer les autres missions d'assurance.

CONCEPTS LIÉS À LA GOUVERNANCE

Réaliser efficacement des activités internes d'assurance et de conseil requiert de bien comprendre l'activité de l'organisation. Pour ce faire, il est nécessaire de cerner le fonctionnement de l'organisation selon une perspective descendante. Habituellement, le dispositif global permettant ce fonctionnement est désigné par l'expression « gouvernement d'entreprise » ou « gouvernance ».

Gouvernance (ou gouvernement d'entreprise)

Dispositif comprenant les processus et les structures mis en place par le Conseil afin d'informer, de diriger, de gérer et de piloter les activités de l'organisation en vue de réaliser ses objectifs.

Définition de la gouvernance

Comme indiqué dans le chapitre 1, *Introduction à l'audit interne*, la gouvernance est un processus piloté par le Conseil qui consiste à autoriser, diriger et surveiller les activités de la direction générale

Copyright © 2015 Eyrolles.

en vue de réaliser les objectifs de l'organisation. La définition donnée par l'Organisation de coopération et de développement économiques (OCDE) est communément admise. Cette organisation, basée à Paris, regroupe les gouvernements de pays attachés aux principes de démocratie et d'économie de marché :

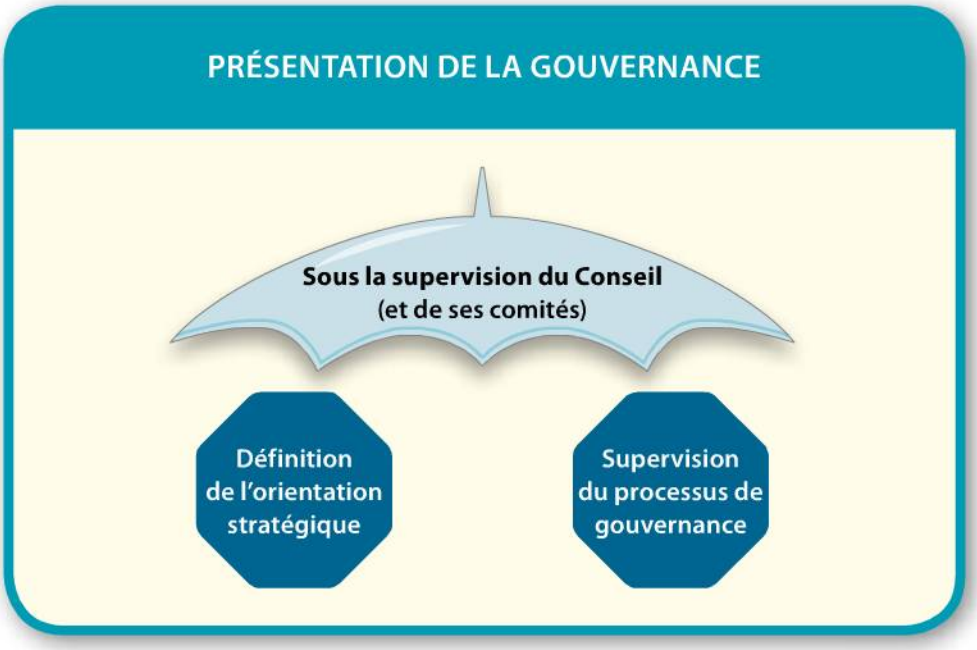
> *« Le gouvernement d'entreprise fait référence aux relations entre la direction d'une entreprise, son conseil d'administration, ses actionnaires et d'autres parties prenantes. Il détermine également la structure par laquelle sont définis les objectifs d'une entreprise, ainsi que les moyens de les atteindre et d'assurer une surveillance des résultats obtenus. »*[1]

Bien qu'il existe beaucoup d'autres définitions de la gouvernance, la plupart d'entre elles présentent des éléments communs. [Il est recommandé aux lecteurs de consulter http://www.ecgi.org/codes/all_codes.php pour une liste complète des codes en vigueur dans le monde entier, dont beaucoup ont trait à la gouvernance.] Le glossaire des *Normes internationales pour la pratique professionnelle de l'audit interne* (les *Normes*) de l'IIA décrit la gouvernance comme « le dispositif comprenant les processus et les structures mis en place par le Conseil afin d'informer, de diriger, de gérer et de piloter les activités de l'organisation en vue de réaliser ses objectifs ».[2]

Dans le cadre du rôle du Conseil en matière d'information et de direction des activités de l'organisation, les paragraphes qui suivent à propos de la gouvernance portent sur la façon dont l'organisation détermine ses objectifs et ses valeurs, et fixe les limites de sa conduite. Si l'on intègre les différentes définitions de la gouvernance ainsi que les éléments connexes, on peut décrire la gouvernance au moyen du diagramme présenté à l'encadré 3-3.

ENCADRÉ 3-3

PRÉSENTATION DE LA GOUVERNANCE



Copyright © 2015 Eyrolles.

Le premier domaine de la gouvernance concerne l'orientation stratégique de l'entité. Il revient au Conseil de donner l'orientation stratégique et les lignes directrices relatives à la définition des objectifs clés de l'organisation, qui doivent cadrer avec le modèle économique de l'organisation et les priorités des parties prenantes. Forts d'expériences diverses et variées, les administrateurs sont en position de fournir des informations et une orientation qui doivent permettre à l'organisation de réussir. Le Conseil peut également influencer la position de cette dernière vis-à-vis de la prise de risques et poser des limites en fonction de l'appétence générale pour le risque et des valeurs culturelles. Le Conseil doit, par ailleurs, suivre les avancées vers la réalisation des buts et objectifs de l'organisation.

Le deuxième domaine de la gouvernance décrit dans l'encadré est la supervision, qui concerne le rôle du Conseil en matière de gestion et de pilotage des activités de l'organisation. Prolongeant l'encadré 3-3, l'encadré 3-4 présente les principales composantes de la supervision de la gouvernance. Parce que c'est au niveau de cette supervision que la gestion des risques et les activités d'audit interne sont les plus pertinentes, cet aspect est approfondi à la suite de cet encadré.

Les principaux points à retenir de cette description de la gouvernance sont les suivants.

- Le Conseil et ses comités supervisent la gouvernance pour l'ensemble de l'organisation. Ils donnent une orientation à la direction générale, lui confèrent le pouvoir de prendre les mesures nécessaires pour suivre cette orientation et supervisent les résultats généraux des opérations.
- Après avoir cerné les besoins des principales parties prenantes, le Conseil s'attache à leur satisfaction. *In fine*, le Conseil a une responsabilité fiduciaire vis-à-vis des parties prenantes de l'organisation, auxquelles il doit rendre compte.
- Au quotidien, la gouvernance est exécutée par le management. La direction générale et les managers intermédiaires jouent un rôle important dans la gouvernance, quoique distinct. Ils exercent leur rôle *via* les activités de gestion des risques.
- Les activités d'assurance internes et externes fournissent à la direction générale et au Conseil une assurance quant à l'efficacité des activités de gouvernance.

Conseil

Organe de gouvernance d'une organisation. Il peut s'agir d'un Conseil d'administration, d'un Conseil de surveillance, de l'organe délibérant d'un organisme public ou d'une association ou de tout autre organe.

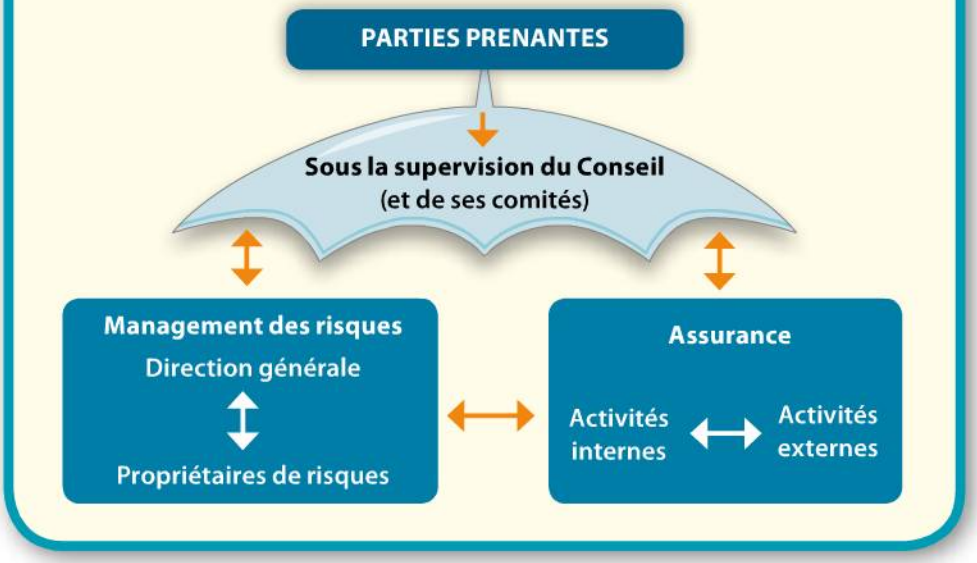
Stratégie

Manière dont la direction générale prévoit de réaliser les objectifs de l'organisation.

Copyright © 2015 Eyrolles.

ENCADRÉ 3-4

LES GRANDES COMPOSANTES DE LA SUPERVISION DE LA GOUVERNANCE



Rôles et responsabilités au sein de la gouvernance – Le Conseil et ses comités



La gouvernance relève de la responsabilité du Conseil, même si cette responsabilité est souvent exercée par le biais de ses divers comités (le comité d'audit, par exemple). La première des responsabilités du Conseil est d'identifier les principales parties prenantes d'une organisation, à savoir toute partie ayant un intérêt direct ou indirect dans les activités d'une organisation et leur résultat. On peut considérer que les parties prenantes présentent l'une ou plusieurs des caractéristiques suivantes :

- certaines parties prenantes *participent directement* au fonctionnement de l'organisation (ex. : collaborateurs) ;
- d'autres parties prenantes ne participent pas directement au fonctionnement de l'organisation, mais y ont *un intérêt*, ce qui signifie que la réussite ou toute autre résultante de l'activité a une incidence sur ces parties prenantes (ex. : clients, fournisseurs) ;
- certaines parties prenantes influentes ne sont pas directement impliquées dans le succès de l'organisation ni intéressées par celui-ci, mais peuvent néanmoins *influencer* certains aspects de l'activité de l'organisation et, par conséquent, la réussite de cette dernière (ex. : autorités de régulation).

Copyright © 2015 Eyrolles.

Types de parties prenantes

– Participation directe.
– Intérêt.
– Influence.

Les principales parties prenantes sont les suivantes.

- Les *collaborateurs* travaillent pour une organisation, et participent directement à sa réussite. Les collaborateurs ont intrinsèquement intérêt à ce que l'organisation soit prospère et viable, car si celle-ci fait faillite ou doit réduire ses effectifs par manque de succès sur le marché, ils risquent de perdre leur revenu. Le Conseil doit donc veiller à ce que l'organisation opère d'une façon qui serve au mieux les intérêts de ses collaborateurs.
- Les *clients* sont habituellement l'élément vital de l'activité de l'organisation et, en tant que tels, ils participent directement à sa réussite. Les clients ont également un intérêt au succès d'une organisation, car l'échec de cette dernière peut réduire le nombre d'options viables qu'ils auront à leur disposition pour obtenir un bien ou un service de qualité. Moyennant un paiement, les clients s'attendent à ce que l'organisation, pour fabriquer des produits sûrs et fiables, fournisse les services convenus et se conforme à d'autres aspects des contrats et accords de vente. Parce que l'organisation a des obligations vis-à-vis de ses clients, le Conseil a pour responsabilité de veiller au respect de ces obligations.
- Les *fournisseurs* procurent les biens et services nécessaires à l'organisation pour mener son activité et participent, par conséquent, directement à l'activité. Comme les clients, les fournisseurs ont un intérêt dans la viabilité de l'organisation, qui constitue pour eux un client. Une organisation a certaines obligations vis-à-vis de ses fournisseurs, la plus évidente étant celle de payer les biens et services reçus. Le Conseil doit donc exercer une responsabilité de supervision afin de s'assurer que l'organisation respecte ses obligations conformément aux contrats et accords conclus avec ses fournisseurs.
- Les *actionnaires*/les *investisseurs* ne participent pas directement à l'activité, mais ont un très grand intérêt dans le succès de l'organisation. En effet, ces parties prenantes ont investi dans l'organisation, que ce soit *via* des parts du capital, qui sont des unités de propriété, ou un autre instrument juridique. Les actionnaires peuvent être des particuliers, des organismes ou des fonds qui investissent pour le compte d'un groupe d'investisseurs. Habituellement, les actionnaires ont le droit d'élire au Conseil les personnes qu'ils jugent à même de servir et de protéger au mieux leurs intérêts. Donc, parce qu'ils sont en mesure d'influencer le Conseil, les actionnaires sont souvent considérés comme les parties prenantes les plus importantes et les plus puissantes du point de vue du Conseil.
- Les *autorités de régulation et de supervision* représentent des organismes publics qui peuvent avoir un intérêt dans la réussite de l'organisation ou être capables d'influencer cette réussite. Les règles et règlements qu'elles adoptent peuvent dicter à une organisation certains impératifs opérationnels et de

Copyright © 2015 Eyrolles.

reporting ou influencer les décisions prises par le management. Aux États-Unis par exemple, la *Securities and Exchange Commission* (SEC) exerce une influence sur l'ensemble des sociétés cotées. Parmi les autorités de régulation et de supervision qui exercent une influence sur la plupart des organisations américaines figurent le ministère du Travail (*Department of Labor*), l'Agence pour la protection de l'environnement (*Environmental Protection Agency*) et l'Administration de la sécurité et de la santé au travail (*Occupational Safety and Health Administration*). En outre, certains secteurs sont soumis à la surveillance de régulateurs spécifiques, notamment le secteur bancaire (*Federal Deposit Insurance Corporation et autres*) et le secteur des services publics (par exemple, la *Federal Energy Regulatory Commission* et des commissions d'État réglementaires chargées d'approuver les tarifs facturables aux clients).

Commentaire du traducteur

Les administrations fiscales ou chargées de l'application du Code du travail contrôlent l'application de règles auxquelles toutes les sociétés doivent se conformer.

Les sociétés cotées ont des exigences spécifiques, notamment en termes de gouvernance et de communication externe. En France, l'Autorité des marchés financiers (AMF) influe sur la gouvernance des sociétés cotées.

En outre, certains secteurs sont subordonnés à des instances de régulation spécifiques (par exemple, les banques et les assurances sont soumises à la supervision de l'Autorité de Contrôle Prudentiel et de Régulation – ACPR).

Ces autorités de régulation et de supervision veillent à ce que les organisations respectent les réglementations relatives au bien public et témoignent donc d'un grand intérêt pour les opérations des organisations. Quasiment tous les pays ou tous les territoires disposent d'autorités ou d'organes analogues qui adoptent des réglementations. Le Conseil doit comprendre les exigences imposées par ces organismes afin de pouvoir exercer ses responsabilités de supervision.

Les établissements financiers, comme des banques ou d'autres établissements, peuvent apporter un financement à une organisation. Les établissements financiers acceptent de financer une organisation en échange d'une rémunération, le plus fréquemment sous la forme d'un taux d'intérêt appliqué à l'encours. Toutefois, ces établissements imposent fréquemment d'autres clauses (covenant) auxquelles l'organisation doit se conformer. Celles-ci ont souvent trait à la santé financière et à la liquidité globale de l'organisation, si bien que les établissements financiers sont en permanence assurés de la capacité de l'organisation à rembourser ses dettes. Ils ont ainsi à la fois un intérêt dans le succès de l'organisation et une influence sur la manière dont l'organisation opérera pour respecter ses accords. Le Conseil doit donc exercer une supervision et veiller à ce que la direction générale soit attentive à toutes les clauses des

Copyright © 2015 Eyrolles.

accords financiers conclus avec ces parties prenantes influentes et s'y conforme.

Bien que les parties prenantes énumérées ci-dessus soient les plus courantes, il peut en exister d'autres qui ont aussi un intérêt dans l'organisation ou qui peuvent l'influencer. Il s'agit par exemple des agences de notation, des associations professionnelles, des analystes financiers et des concurrents. Il est essentiel que le Conseil fasse les efforts et consacre le temps qui sont nécessaires pour identifier l'ensemble des principales parties prenantes de l'organisation.

Une fois que les principales parties prenantes sont identifiées, le Conseil doit comprendre leurs besoins et leurs attentes. Certains sont évidents : par exemple, les clients attendent que les produits soient exempts de défauts et les fournisseurs attendent que les créances soient réglées dans les temps. Cependant, des recherches et analyses peuvent se révéler nécessaires pour cerner correctement d'autres attentes, telles que les *desiderata* des actionnaires (obtenir des dividendes ou plutôt une hausse du cours de l'action). Le Conseil peut être à même de définir ces attentes au moyen de discussions internes, mais il peut aussi avoir besoin de débattre de ces questions directement avec les principales parties prenantes.

Enfin, le Conseil doit identifier les éventualités qui seraient inacceptables pour les principales parties prenantes. Ainsi, certains investisseurs seraient insatisfaits si l'organisation était en dessous de ses objectifs de bénéfices par action sur un trimestre donné, mais considéreraient encore cela acceptable dans la mesure où ils admettent que certaines composantes des bénéfices sont plus volatiles que d'autres. En revanche, ces mêmes investisseurs pourraient trouver inacceptable que l'organisation n'atteigne pas ses objectifs de bénéfices sur plusieurs trimestres consécutifs et risqueraient de s'interroger sur l'opportunité d'un remaniement de la direction générale. Les éventualités inacceptables peuvent être aussi bien des résultats qui portent atteinte à l'organisation que des résultats qui témoignent de l'incapacité de saisir une opportunité.

Parce que les diverses parties prenantes auront vraisemblablement des attentes différentes, on observe aussi des écarts entre ce que chaque catégorie de partie prenante jugera inacceptable. Le Conseil devra prendre en compte plusieurs types de résultats.

- **Financiers.** Par exemple : bénéfice par action, ratio de trésorerie, note de solvabilité, retour sur investissement, disponibilité du capital, exposition fiscale, faiblesses importantes et transparence de la communication financière.
- **De conformité.** Par exemple : contentieux, violation du code de conduite, violation des normes environnementales et de sécurité, ordonnance restrictive, enquête publique, amendes et pénalités réglementaires, mise en accusation et arrestation.

Copyright © 2015 Eyrolles.

- **Opérationnels.** Par exemple : réalisation des objectifs, utilisation efficiente des actifs, protection des ressources (couverture par une assurance, dépréciation d'actifs, destruction d'actifs), protection des personnes (hygiène et sécurité, arrêts de travail), protection de l'information (intégrité des données, respect de la confidentialité des données) et protection de la population (répercussions sur l'environnement, fermetures d'usines).
- **Stratégiques.** Par exemple : réputation, viabilité de l'organisation, moral des collaborateurs et satisfaction de la clientèle.

Appétence pour le risque

Niveau de risque global qu'une organisation est prête à accepter en vue de la réalisation de ses objectifs.

Tolérance au risque

Niveau de risque et d'écart acceptable entre les objectifs et la performance réelle ; elle doit être en adéquation avec l'appétence pour le risque de l'organisation.

Une fois que le Conseil a posé les limites de ce qui est acceptable pour les principales parties prenantes, il peut établir quels sont les seuils de tolérance pour ces différents aspects en fonction de l'appétence pour le risque de l'organisation, et les communiquer à la direction générale : ces seuils fixent la marge de manœuvre au sein de laquelle l'organisation peut opérer. Les concepts d'appétence pour le risque et de tolérance au risque seront approfondis au chapitre 4, *La gestion des risques*, mais un exposé succinct de ces concepts facilitera ici la compréhension du rôle du Conseil.

L'appétence pour le risque* se prête bien à une métaphore alimentaire, car on peut facilement l'assimiler à l'envie de manger. Cette appétence représente le volume total de nourriture que l'on peut consommer pour atteindre certains objectifs, par exemple rester en bonne santé et conserver le poids souhaité. Il est possible d'être rassasié en consommant une seule catégorie d'aliment (le chocolat, par exemple). Cependant, si l'on peut se sentir repu, se nourrir exclusivement de chocolat ne permettra pas d'atteindre son objectif à long terme, à savoir rester en bonne santé et conserver le poids souhaité. Ainsi, le cerveau humain (que l'on peut comparer au Conseil d'une organisation) définit dans quelles quantités (y compris maximales et minimales) nous devons consommer certaines catégories d'aliments. Ces quantités sont analogues aux seuils de tolérance qui facilitent la réalisation des objectifs d'une organisation.

En s'appuyant sur les concepts décrits plus haut, le Conseil exercera au mieux ses responsabilités de gouvernance en :

- établissant un comité de gouvernance :
  - ce comité peut être une entité entièrement nouvelle ou bien une extension d'un comité existant (par exemple de nombreuses sociétés cotées ont élargi les attributions de leur comité de nomination pour en faire un comité de nomination et de gouvernance) ;
  - il doit être constitué d'administrateurs indépendants ;
  - ce comité doit exercer les responsabilités décrites plus haut ;

* NdT : Le terme *risk appetite* est traduit dans d'autres publications par « appétit pour le risque » (ou « goût pour le risque »).

Copyright © 2015 Eyrolles.

- précisant les exigences de reporting au Conseil :
  - le Conseil doit déléguer à la direction générale l'autorité de gérer l'organisation en respectant les limites de tolérance qu'il a fixées. La direction générale doit avoir le pouvoir de prendre les décisions relatives à l'activité quotidienne, mais doit également bien comprendre les seuils de tolérance fixés par le Conseil ;
  - dans le cadre de sa fonction de supervision, le Conseil doit également définir des seuils de reporting à l'intention de la direction générale, à savoir les événements qui doivent recevoir l'aval du Conseil, lui être directement communiqués ou simplement synthétisés lors des réunions trimestrielles ;
- réévaluant régulièrement (généralement tous les ans) les attentes concernant la gouvernance :
  - les attentes des principales parties prenantes peuvent évoluer et se transformer. Le Conseil doit donc identifier ces changements et réévaluer l'orientation qu'il donne à la gouvernance ;
  - à la suite de ces changements, les seuils de tolérance fixés par le Conseil doivent également être réévalués.

En résumé, le Conseil joue un rôle essentiel et incontournable dans la gouvernance. Si la gouvernance ne recouvre pas à la fois l'autorité, l'orientation et la supervision, elle ne sera pas suffisamment efficace sur le long terme.

La direction générale

Une fois que le Conseil a déterminé les seuils de tolérance et le champ des opérations, il doit déléguer aux membres de la direction générale le pouvoir de gérer les opérations dans le respect de ces seuils. La direction générale a alors pour responsabilité de mettre en œuvre les orientations données par le Conseil de façon à atteindre les objectifs de l'organisation, tout en respectant les seuils de tolérance que celui-ci a définis.

Pour exercer ses responsabilités de gouvernance, la direction générale est chargée :

- de veiller à ce que l'ensemble des orientations et des pouvoirs délégués soient bien compris. La direction générale doit cerner les attentes du Conseil concernant la gouvernance, le pouvoir que celui-ci lui a délégué, ses seuils de tolérance ainsi que les exigences de reporting au Conseil ;
- d'identifier les processus et activités qui, au sein de l'organisation, font partie intégrante de la mise en œuvre des orientations

Copyright © 2015 Eyrolles.

fixées par le Conseil pour la gouvernance. En d'autres termes, la direction générale doit déterminer :

- où gérer, au sein de l'organisation, les risques spécifiques susceptibles d'aboutir à des événements inacceptables ;
- qui est responsable de la gestion de ces risques (autrement dit, qui sont les « propriétaires de risques », ou *risk owners*) ;
- comment ces risques seront gérés.

- d'évaluer quels autres considérations et facteurs pourraient justifier de déléguer aux propriétaires de risques un seuil de tolérance inférieur à celui délégué par le Conseil. Le Conseil peut en effet spécifier que la direction générale doit réaliser les contrôles lui permettant de s'assurer qu'aucune faiblesse de contrôle ne dépasse un niveau de sévérité donné. Néanmoins, désireuse d'éviter une situation dans laquelle de multiples déficiences de contrôle significatives s'agrégeraient à un niveau inacceptable, la direction générale peut commander aux propriétaires de risques de veiller, par leurs contrôles, à ce qu'aucune déficience ne dépasse un niveau de sévérité moins élevé ;
- de veiller à ce que suffisamment d'informations soient recueillies auprès des propriétaires de risques pour satisfaire aux exigences de reporting au Conseil.

Risque

Possibilité qu'un événement survienne et ait un impact défavorable sur la réalisation des objectifs.

La direction générale exercera au mieux ses responsabilités de gouvernance en :

- instaurant un comité des risques :
  - ce comité est généralement dirigé par un cadre supérieur : le directeur des risques, s'il y en a un, ou bien un autre cadre qui a une vaste responsabilité de supervision des risques ;
  - il est chargé de déterminer si tous les principaux risques sont identifiés, mis en relation avec des activités de gestion des risques et assignés à un propriétaire de risques. Dans le cadre de cette responsabilité, le comité doit veiller à prendre en considération de manière exhaustive l'ensemble des éventuelles répercussions des principaux risques, et non les seuls impacts financiers ;
  - il évalue le niveau actuel d'appétence pour le risque de l'organisation et s'assure que les seuils de tolérance délégués aux propriétaires de risques permettent de le respecter ;
- précisant les exigences de reporting :
  - les propriétaires de risques doivent comprendre la nature, le format et le calendrier des communications requises à propos de l'efficacité des activités de gestion des risques. De manière générale, ces communications doivent correspondre au seuil de tolérance délégué aux propriétaires de risques ;

Copyright © 2015 Eyrolles.

- ce reporting peut intervenir lors des réunions du comité des risques programmées à intervalles réguliers ou dans le cadre de la synthèse des informations à communiquer au Conseil ;

- réévaluant régulièrement (généralement tous les ans) les attentes concernant la gouvernance :
  - à mesure qu'une organisation évolue et se transforme, la direction générale doit réexaminer les orientations qu'elle donne pour la gouvernance, ainsi que les seuils de tolérance correspondants qu'elle a délégués aux propriétaires de risques. Ces changements peuvent émaner du Conseil ou d'autres facteurs, externes ou internes. Ils peuvent appeler l'introduction de nouvelles activités de gestion des risques ou la modification des activités en place ;
  - à la suite de ces changements, les seuils de tolérance fixés par la direction générale doivent également être réévalués ;
  - cette situation donne également à la direction générale l'occasion d'évaluer l'efficacité globale du programme de gestion des risques de l'organisation.

La direction générale joue un rôle indispensable dans la gestion des risques, qui est une composante clé de la gouvernance. Pour une description plus précise de ces concepts relatifs à la gestion des risques, voir le chapitre 4, *La gestion des risques*.

Propriétaires de risques

On appelle propriétaires de risques les personnes qui ont la responsabilité, au quotidien, de veiller à ce que les activités de gestion des risques permettent de gérer efficacement les risques conformément aux seuils de tolérance au risque de l'organisation. Généralement, le directeur général et les autres dirigeants sont, en fin de compte, les propriétaires de risques au sein de l'organisation. Cependant, ce terme est utilisé ici pour faire référence aux personnes qui mènent des activités quotidiennes dans le but de gérer des risques spécifiques. Ces personnes doivent identifier, mesurer, gérer et piloter les risques, puis en rendre compte à leur hiérarchie, habituellement aux membres de la direction générale. Dans certains cas, les propriétaires de risques se situent à un niveau inférieur dans la hiérarchie de l'organisation. Cependant, ils collaborent avec la direction générale pour mener à bien les activités de gestion des risques.

Ils ont notamment pour responsabilité :

- d'évaluer si les activités de gestion des risques sont conçues de manière adéquate pour gérer les risques dans le respect des seuils de tolérance spécifiés par la direction générale. Bien que cette dernière imprime une orientation relative à ces activités,

Copyright © 2015 Eyrolles.

ce sont généralement les propriétaires de risques qui définissent les tâches spécifiques à accomplir ;

- d'évaluer les capacités actuelles de l'organisation à mener à bien ces activités de gestion des risques. Cette évaluation doit prendre en compte la maturité des procédures en place, la compétence et l'expérience des personnes qui les exécutent, le caractère suffisant de toutes les technologies d'appui (par exemple le système informatique) et la disponibilité d'informations internes et externes étayant la prise de décisions concernant la gestion des risques ;
- de déterminer si les activités de gestion des risques sont effectuées conformément à ce qui était prévu, c'est-à-dire si les personnes et les systèmes appliquent les processus de manière à permettre d'atteindre les objectifs visés ;
- de mener des activités quotidiennes de pilotage afin d'identifier rapidement toute anomalie ou tout écart par rapport aux résultats attendus ;
- de veiller à ce que les informations dont la direction générale et le Conseil ont besoin soient exactes, facilement accessibles et transmises à la direction générale en temps voulu.

Les propriétaires de risques exercent au mieux leurs responsabilités de gouvernance en :

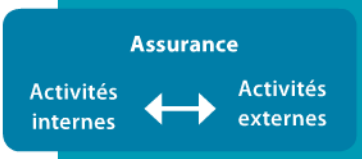
- présentant au comité des risques des propositions pour la gouvernance :
  - si une personne est désignée propriétaire de risques, ou si elle est responsable d'un risque qui, auparavant, ne faisait pas l'objet d'une gestion des risques et d'un reporting formels, elle doit élaborer une recommandation à l'intention du comité des risques. Cette recommandation doit couvrir la nature intrinsèque et la source du risque, son impact potentiel, les seuils de tolérance envisagés et les activités de gestion des risques prévues. Ces informations sont présentées au comité des risques, où elles sont débattues puis validées ;
- réévaluant régulièrement (au moins tous les ans, plus souvent si nécessaire) les activités de gestion des risques :
  - le contenu des activités de gestion des risques doit en permanence correspondre à la stratégie de gestion des risques appliquée à l'ensemble de l'organisation, et permettre que les risques soient gérés conformément aux seuils de tolérance délégués ;
  - les capacités de gestion des risques doivent être réévaluées en fonction de la rotation des effectifs, des changements de systèmes et des autres événements susceptibles d'avoir une incidence sur leur maturité et leur efficacité ;

Copyright © 2015 Eyrolles.

- les activités de surveillance de la gestion des risques doivent fournir, en temps opportun, aux propriétaires de risques, toute information sur l'efficacité des activités de gestion des risques ;
- le reporting des résultats de la gestion des risques à la direction générale, au moment opportun et dans les délais prévus, doit être périodiquement évalué avec la direction générale, afin d'assurer qu'il répond aux besoins de cette dernière.

Les propriétaires de risques sont en première ligne de la gestion des risques et, en tant que tels, sont des acteurs essentiels de la bonne gouvernance. Leur rôle dans l'exécution et le pilotage des activités de gestion des risques, ainsi que dans le reporting sur l'efficacité de ces activités, influence fortement la capacité de l'organisation à éviter ou atténuer l'impact des événements inacceptables. Pour une description plus précise de ces concepts relatifs à la gestion des risques, voir le chapitre 4, *La gestion des risques*.

Les activités d'assurance



Activités d'assurance

Examen objectif d'éléments probants, effectué en vue de fournir à l'organisation une évaluation indépendante des processus de gouvernement d'entreprise, de management des risques et de contrôle.

Les activités indépendantes d'assurance forment la dernière composante de la gouvernance : elles donnent au Conseil et à la direction générale une évaluation objective de l'efficacité des activités de gouvernance et de gestion des risques. Elles peuvent être effectuées par diverses parties, appartenant ou non à l'organisation. Le service qui donne le plus souvent ces assurances est l'audit interne.

La Norme IIA 2110, Gouvernement d'entreprise, précise à propos du rôle de l'audit interne :

« L'audit interne doit évaluer le processus de gouvernement d'entreprise et formuler des recommandations appropriées en vue de son amélioration. À cet effet, il détermine si le processus répond aux objectifs suivants :

- promouvoir des règles d'éthique et des valeurs appropriées au sein de l'organisation ;
- garantir une gestion efficace des performances de l'organisation, assortie d'une obligation de rendre compte ;
- communiquer aux services concernés de l'organisation les informations relatives aux risques et aux contrôles ;
- fournir une information adéquate au Conseil, aux auditeurs internes et externes et au management, et assurer une coordination de leurs activités. »

Copyright © 2015 Eyrolles.

La Norme IIA 2120, Management des risques, indique : « L'audit interne doit évaluer l'efficacité des processus de management des risques et contribuer à leur amélioration. » Ces deux normes partent du principe que l'audit interne peut réaliser à la fois des activités d'assurance et de conseil pour une organisation. Le champ des missions d'assurance exécutées par l'audit interne dépend (1) de la charte d'audit interne, qui précise le rôle de l'audit interne dans la gouvernance, et (2) des orientations spécifiques données par le Conseil s'agissant des attentes actuelles et à venir pour ces activités. En fonction de ces deux facteurs, les responsabilités de l'audit interne concernant la gouvernance peuvent comprendre un ou plusieurs des aspects suivants :

- déterminer si les diverses activités de gestion des risques sont conçues de manière adéquate au regard des événements susceptibles d'avoir des impacts inacceptables ;
- vérifier que les diverses activités de gestion des risques fonctionnent comme prévu ;
- évaluer l'adéquation de la conception et le fonctionnement effectif du programme/système de gestion des risques dans son ensemble ;
- vérifier si les déclarations faites par les propriétaires de risques à la direction générale au sujet de l'efficacité des activités de gestion des risques donnent une image exacte de l'efficacité actuelle de la gestion des risques ;
- vérifier si les déclarations faites par la direction générale au Conseil au sujet de l'efficacité des activités de gestion des risques lui apportent les informations qu'il désire concernant l'efficacité actuelle de la gestion des risques ;
- déterminer si les informations relatives à la tolérance au risque sont communiquées efficacement et rapidement par le Conseil à la direction générale, puis par la direction générale aux propriétaires de risques ;
- déterminer s'il existe des domaines de risques qui ne sont actuellement pas couverts par le processus de gouvernance, alors qu'ils le devraient (par exemple, un risque pour lequel la tolérance et les attentes de reporting n'ont pas été déléguées à un propriétaire de risques précis).

L'audit interne est un acteur efficace du processus de gouvernance s'il :

- s'efforce de comprendre pleinement les orientations et les attentes du Conseil s'agissant de la gouvernance :
  - l'audit interne doit comprendre l'orientation donnée à la direction générale, y compris les seuils de tolérance au risque et les attentes vis-à-vis du reporting ;

Copyright © 2015 Eyrolles.

- en outre, il est important qu'il comprenne ce que le Conseil attend de lui concernant les missions d'assurance ;

- soutient le programme de gestion des risques établi par le management :
  - compte tenu de certaines similarités avec les activités d'audit interne, la fonction d'audit interne contribue à la structuration et à la rigueur du programme de gestion des risques ;
  - elle peut contribuer à sensibiliser le management et les collaborateurs aux questions relatives au risque et au contrôle ;
  - l'audit interne peut faciliter ou piloter les évaluations des risques au niveau de l'organisation et des différentes divisions ;
  - l'audit interne peut apporter des contributions et mener une surveillance continue et formelle (par exemple par la participation à un comité directeur sur le risque) ou informelle (notamment par le biais de discussions régulières avec le management) ;
- élabore un plan d'audit interne qui englobe de manière appropriée les missions d'assurance concernant la gouvernance et prévoit des communications périodiques à la direction générale et au Conseil au sujet de l'efficacité des activités de gestion des risques.

Activités de conseil

Conseils et services y afférents rendus au client donneur d'ordre, dont la nature et le champ sont convenus au préalable avec lui. Ces activités ont pour objectif d'améliorer les processus de gouvernement d'entreprise, de management des risques et de contrôle d'une organisation sans que l'auditeur interne n'assume aucune responsabilité de management.

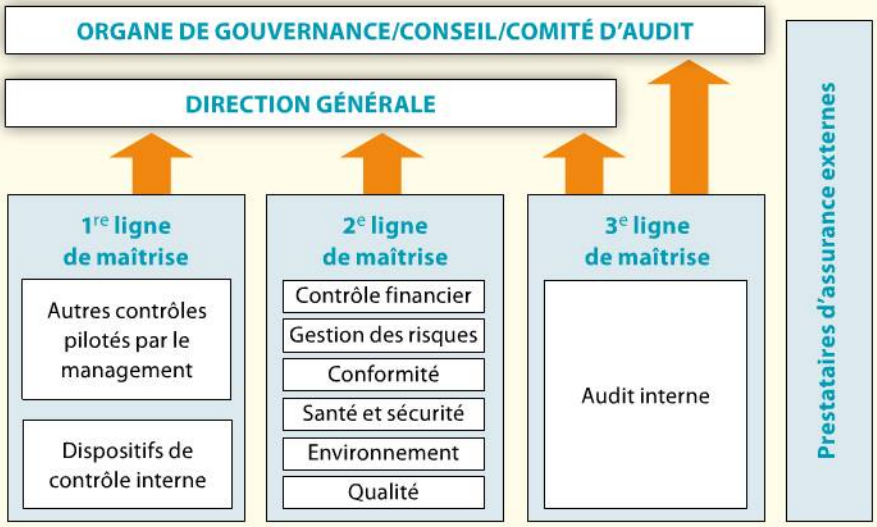
Modèle des trois lignes de maîtrise

Si, comme indiqué ci-dessus, l'audit interne donne une assurance précieuse, dans la plupart des organisations, d'autres catégories de parties prenantes fournissent également une certaine forme d'assurance (les services chargés de l'environnement et de la sécurité, les acteurs de l'assurance qualité, les services de contrôle des transactions, etc.) soit directement au Conseil, soit par des communications aux membres de la direction générale chargés de donner une assurance au Conseil. Conscientes que l'assurance peut émaner d'activités différentes, tant en interne qu'en externe, de nombreuses organisations ont mis en place différents niveaux d'assurance pour maîtriser les risques tel que requis ou souhaité ou pour opérer conformément aux seuils de tolérance au risque de l'organisation. Cette stratégie est souvent désignée comme un modèle de « lignes de maîtrise multiples ». Le Modèle des trois lignes de maîtrise illustré dans l'encadré 3-5 est un exemple classique.

Copyright © 2015 Eyrolles.

ENCADRÉ 3-5

MODÈLE DES TROIS LIGNES DE MAÎTRISE



Global Advocacy Platform (Altamonte Springs, Floride : *The Institute of Internal Auditors Global*, 2012), p. 9.

Dans ce modèle, le rôle du Conseil et de la direction générale n'est pas différent de celui décrit précédemment. En revanche, les trois lignes de maîtrise nécessitent une explication.

- La **première ligne de maîtrise** représente les activités de contrôle interne réalisées par des collaborateurs et le management. Elles comprennent à la fois les activités de contrôle interne spécifiques, ou « mesures de contrôle interne », et les contrôles de gestion qui permettent de superviser et de surveiller les activités individuelles. Les contrôles de la première ligne de maîtrise sont très importants. Néanmoins, ils sont réalisés par des collaborateurs et le management qui en sont directement responsables. C'est pourquoi ils constituent la ligne de maîtrise la moins indépendante et la moins objective des trois.
- La **deuxième ligne de maîtrise** représente les autres activités d'assurance, telles que celles qui figurent dans l'encadré. Ces activités sont réalisées par des collaborateurs rattachés à des niveaux hiérarchiques différents de celui qui est directement responsable des activités de contrôle interne. C'est pourquoi le degré d'indépendance et d'objectivité de cette ligne est supérieur à celui de la première ligne. Toutefois, les collaborateurs fournissant une assurance de la deuxième ligne de maîtrise exercent souvent d'autres responsabilités de gestion en sus de leurs responsabilités d'assurance.
- La **troisième ligne de maîtrise** représente la forme d'assurance la plus indépendante et la plus objective. L'audit interne

Copyright © 2015 Eyrolles.

est généralement le seul à être fonctionnellement rattaché au Conseil et n'exerce pas d'autres responsabilités de gestion. La troisième ligne de maîtrise est donc la plus indépendante et la plus objective des trois.

L'assurance peut également émaner de tiers. Bien que moins courante que les activités d'assurance internes, cette assurance demeure néanmoins importante pour le Conseil. Ainsi, même si les attestations délivrées par des auditeurs externes visent en premier lieu à satisfaire des exigences réglementaires ou contractuelles, ces opinions peuvent aussi procurer au Conseil et à la direction générale une assurance quant à l'efficacité des activités conçues pour maîtriser les risques liés au reporting financier. De même, des cabinets de conseil externes peuvent être sollicités et chargés de donner à la direction générale ou au Conseil une assurance concernant telle ou telle activité de gestion des risques. Enfin, les inspecteurs chargés de la vérification de la conformité aux règles en vigueur pour le compte d'une autorité de tutelle donnent aussi certaines formes d'assurance au management.

Si la multiplicité des niveaux d'assurance est bénéfique, les organisations doivent néanmoins veiller à éviter l'excès d'assurance, au risque d'entraîner une « usure de l'audit » ou une « fatigue de l'audit ». C'est notamment le cas lorsque les différentes activités d'assurance ne collaborent pas et ne sont pas suffisamment coordonnées, à tel point que certaines d'entre elles deviennent redondantes et superflues. Certains diront qu'il ne peut y avoir trop d'assurance. Les activités d'assurance ont cependant besoin de ressources précieuses au sein de l'organisation, qu'il s'agisse des activités qui fournissent l'assurance ou de celles qui sont évaluées. L'assurance a donc un coût qu'il convient de prendre en compte.

Afin de lutter contre l'« usure de l'audit », certaines organisations ont élaboré des modèles d'assurance « combinés » ou « intégrés ». Ces modèles varient d'une organisation à une autre et peuvent être mis en œuvre à grande ou petite échelle. En règle générale, ces modèles permettent d'appréhender les différents types d'assurance. Selon le niveau de risque évalué et le degré d'assurance fourni, un plan ou un calendrier coordonné est élaboré. Il indique quand et par quelle activité d'assurance les évaluations sont réalisées, et précise à quel moment et dans quelle mesure les autres activités pourront s'appuyer sur ses travaux.

Quelle que soit leur structure, les activités d'assurance indépendantes exécutées par des auditeurs internes, par d'autres lignes de maîtrise et par des tiers donnent à la direction générale et au Conseil de précieuses informations qui leur permettent de surveiller l'efficacité des activités de gouvernance et de gestion des risques. Ces activités d'assurance sont essentielles à la bonne gouvernance.

Auditeur externe

Cabinet d'experts-comptables agréé, chargé par le Conseil ou la direction générale de l'organisation de procéder à un audit des états financiers et de donner une assurance sous la forme d'une attestation écrite, indiquant son opinion quant à la sincérité des états financiers et à leur conformité aux principes comptables généralement admis.

Copyright © 2015 Eyrolles.

L'ÉVOLUTION DE LA GOUVERNANCE

Malgré la publicité dont bénéficie la gouvernance depuis quelques années, le concept de gouvernance efficace ne date pas d'hier. Les marchés d'actions reposent sur le postulat que les investisseurs procurent du capital aux organisations en échange d'un retour sur investissement potentiel. Pour avoir confiance dans les marchés de capitaux, les investisseurs ont besoin de disposer de suffisamment d'informations appropriées pour évaluer les risques et la rémunération potentiels de leurs investissements. Ils doivent aussi avoir l'assurance que les conditions sont équitables, c'est-à-dire que tous les investisseurs pourront effectuer des transactions de manière uniforme et juste. Diverses réglementations et normes ont été mises en place pour favoriser la réalisation de cet objectif et renforcer la transparence de l'information publiée. Souvent, il en est adopté de nouvelles en réaction à un événement qui s'est produit dans le monde des affaires, en vue d'éliminer ou de minimiser les répercussions indésirables de ces événements. L'encadré 3-6 présente certains des principaux événements qui se sont produits dans le monde des affaires aux États-Unis, ainsi que les lois qui en ont découlé. L'Annexe 3-B, « Synthèse des principaux textes en vigueur aux États-Unis », qui figure à la fin de ce chapitre, résume les principales réglementations américaines et décrit chaque loi présentée dans l'encadré 3-6.

Commentaire du traducteur

L'annexe 3-A présente la synthèse de l'évolution réglementaire communautaire, française et canadienne.

La réglementation dans d'autres régions du monde

Des événements du même ordre se sont produits dans les milieux d'affaires d'autres pays, qui ont incité à voter des textes de loi. Chaque élément de la législation a été élaboré dans le but d'améliorer la gouvernance générale, ainsi que les contrôles de l'établissement des états financiers, et de renforcer la sincérité et la transparence du reporting financier.

OPPORTUNITÉS POUR UN POINT DE VUE DE L'AUDIT INTERNE

Comme le montrent les réflexions précédentes, la notion de gouvernance est un large concept. Des organisations du monde entier ont publié leurs principes de gouvernance sur leur site Web afin de les rendre particulièrement visibles. Une visite de ces sites permet de comprendre que les conceptions de la gouvernance ne sont pas homogènes. Quel que soit le type de gouvernance adopté dans une

Copyright © 2015 Eyrolles.

LES PRINCIPAUX ÉVÉNEMENTS QUI SE SONT PRODUITS DANS LE MONDE DES AFFAIRES AUX ÉTATS-UNIS ET LES LOIS QUI EN ONT DÉCOULÉ

Principaux événements	Lois/Directives
Après l'effondrement des marchés boursiers américains en 1929 et les faillites de plusieurs grandes organisations causées par des fraudes, il a rapidement été nécessaire de restaurer la confiance des investisseurs. Les lois qui en ont découlé visaient à instaurer des conditions équitables pour les investisseurs *via* la publication, en temps voulu, d'informations financières cohérentes, complètes et pertinentes.	*Securities Act* de 1933 *Securities Exchange Act* de 1934
L'enquête sur l'affaire du Watergate a révélé qu'entre le début des années 1970 et 1976, plus de 450 organisations américaines ont versé des pots-de-vin ou effectué des paiements suspects à des fonctionnaires ou des partis politiques étrangers.	*Foreign Corrupt Practices Act* (FCPA) de 1977
Plusieurs cas de reporting financier inexact, incomplet ou trompeur ont été dénombrés.	Rapport de la *National Commission on Fraudulent Financial Reporting* (rapport de la *Treadway Commission*) – 1987
Plusieurs établissements d'épargne et de crédit ont réclamé la mise en place de plans de sauvetage par l'État, remettant en question la robustesse de leur système de contrôle interne, entre autres choses.	*Federal Deposit Insurance Corporation Improvement Act* (FDICIA) de 1991
Faillites et cas de fraude concernant de grandes organisations américaines (comme Enron Corporation et WorldCom)	Le *Sarbanes-Oxley Act* de 2002, qui amende les *Securities Acts* de 1933 et 1934 Les Normes américaines de cotation en bourse (NYSE, AMEX, NASDAQ)
La crise financière qui a éclaté fin 2007-2008 a aggravé la récession mondiale et entraîné la faillite de plusieurs organisations renommées.	*Dodd-Frank Wall Street Reform and Consumer Protection Act* de 2010

Copyright © 2015 Eyrolles.

organisation particulière, l'audit interne a la possibilité de créer de la valeur ajoutée en apportant son point de vue sur le processus. L'encadré 3-7 présente 10 opportunités.

ENCADRÉ 3-7

APPORTER SON POINT DE VUE SUR LA GOUVERNANCE 10 OPPORTUNITÉS POUR L'AUDIT INTERNE

- Apporter des conseils concernant la mise en adéquation des pratiques actuelles du Conseil avec les meilleures pratiques.
- Apporter une contribution et des conseils concernant la charte du comité d'audit et d'autres chartes si nécessaire.
- Apporter des conseils concernant la clarté et le caractère approprié du protocole de communication des problèmes au Conseil ou à ses comités.
- S'assurer que le Conseil et ses comités reçoivent les informations en temps voulu afin de leur permettre de se préparer plus efficacement pour leurs réunions.
- Contribuer à la préparation de l'ordre du jour des réunions du Conseil et de ses comités afin de s'assurer que les thèmes appropriés sont abordés en temps voulu.
- Déterminer si le reporting destiné au Conseil et à ses comités est suffisamment transparent afin de s'assurer qu'ils reçoivent les informations nécessaires pour mettre en œuvre une gouvernance efficace.
- Apporter des conseils concernant le processus d'auto-évaluation du Conseil et de ses comités ou le faciliter.
- Communiquer les informations nécessaires pour aider le comité d'audit à superviser l'audit interne, y compris les informations relatives à son indépendance dans l'organisation, à l'adéquation et aux compétences de ses ressources, à son périmètre d'activité et à l'attention accordée par le management.
- Proposer des publications ou des liens vers d'autres sources d'information qui peuvent aider le Conseil ou ses comités à se tenir informés sur les pratiques et risques émergents.
- Apporter une contribution afin d'aider le comité d'audit à superviser les auditeurs externes et à évaluer leur efficacité.

Commentaire du traducteur

Voir la prise de position « Le rôle de l'audit interne dans le gouvernement d'entreprise » publiée par l'IFACI et l'IFA (Institut Français des Administrateurs), et celle de l'ECIIA (Confédération européenne des instituts d'audit interne) et d'ecoDa (Confédération européenne des associations d'administrateurs) intitulée Making the Most of the Internal Audit Function.

RÉSUMÉ

Les organisations doivent veiller à mettre en œuvre des structures de gouvernance et un dispositif de gestion des risques efficaces. La structure de gouvernance encadre les activités de ceux qui se chargent quotidiennement de la gestion des risques inhérents au modèle économique de leur organisation. Il convient de piloter ces activités afin d'en assurer la cohérence. Les trois éléments qui composent la gouvernance peuvent être représentés comme dans l'encadré 3-8.

Copyright © 2015 Eyrolles.

ENCADRÉ 3-8

PRINCIPAUX ÉLÉMENTS DE LA GOUVERNANCE



La gouvernance fait référence aux relations entre la direction générale de l'organisation, son Conseil et ses parties prenantes. Le Conseil « supervise » la gouvernance. Il doit comprendre les besoins et les attentes des diverses parties prenantes et s'efforcer d'y répondre. Il doit donc bien préciser ses orientations, apporter ses conseils pour la fixation des objectifs de l'organisation, instaurer des limites à la conduite de l'organisation et inciter la direction générale à concrétiser son orientation. La direction générale exécute les activités de gestion des risques afin de respecter les orientations données par le Conseil. Ces activités peuvent être menées à bien par les propriétaires de risques à un niveau inférieur de l'organisation, mais la direction générale est responsable en dernier ressort de l'efficacité des activités de gestion des risques. Enfin, les acteurs internes et externes des activités d'assurance, et en particulier les auditeurs, peuvent donner à la direction générale et au Conseil plusieurs niveaux d'assurance concernant l'efficacité des activités de gestion des risques. Ces niveaux d'assurance peuvent être considérés comme étant inclus dans un « modèle de lignes de maîtrise multiples ». Il convient néanmoins de veiller à ne pas donner un excès d'assurance, au risque d'entraîner une « usure de l'audit » car, selon l'expression bien connue, « trop de contrôle tue le contrôle ».

Pour finir, le rôle de l'audit interne dans la gouvernance apparaît essentiel. Ce rôle sera davantage mis en évidence au chapitre 4, *La gestion des risques* et au chapitre 6, *Le contrôle interne*. Pour illustrer le fait que l'audit interne est un élément clé de la gouvernance, l'encadré 3-8 comprend un intitulé supplémentaire.

Copyright © 2015 Eyrolles.

ANNEXES

ANNEXE 3-A : SYNTHÈSE DE L'ÉVOLUTION DE LA RÉGLEMENTATION COMMUNAUTAIRE, FRANÇAISE ET CANADIENNE

Les directives européennes

Des textes relatifs à la gouvernance et au contrôle interne ont été adoptés au niveau européen.

- La directive 2014/56/CE du 16 avril 2014 modifie la directive 2006/43/CE dite huitième directive sur le contrôle légal des comptes annuels et consolidés. Cette directive vise notamment :
  - l'instauration d'un comité d'audit et la définition de son rôle ;
  - l'établissement d'un rapport par le contrôleur légal des comptes au comité d'audit sur les aspects touchant au contrôle, en particulier les faiblesses significatives du contrôle interne au regard du processus d'information financière.

Les mesures précisées en 2014 concernent plus particulièrement le renforcement de l'indépendance des contrôleurs légaux et l'amélioration de la valeur informative du rapport d'audit.

- La directive 2006/46/CE du 14 juin 2006 modifiant notamment la 4e et la 7e Directives relatives aux comptes annuels et aux comptes consolidés des sociétés prévoit que « toute société dont les titres sont admis à la négociation sur un marché réglementé inclut une déclaration sur le gouvernement d'entreprise dans son rapport de gestion. Cette déclaration forme une section spécifique du rapport de gestion et contient (…) une description des principales caractéristiques des systèmes de contrôle interne et de gestion des risques de la société dans le cadre du processus d'établissement de l'information financière » (…) Les sociétés concernées doivent préciser à quel code de gouvernement d'entreprise elles sont soumises et doivent rendre compte de l'application de ce code selon le principe « appliquer ou expliquer » (« *comply or explain* »).
- La directive 2009/138/CE « Solvabilité 2 » du 25 novembre 2009, concerne les sociétés d'assurance et de réassurance opérant dans l'Union européenne. Au-delà des exigences quantitatives portant sur la solvabilité des entreprises assujetties et des normes de reporting réglementaire, elle précise les attentes du législateur en termes de système de gouvernance auxquelles devront se soumettre les sociétés concernées. L'article 47 de cette directive vise explicitement la mise en place d'une fonction d'audit interne qui a pour mission d'évaluer l'adéquation et l'efficacité du système de contrôle interne et les autres éléments du système de gouvernance.

Le cadre réglementaire international du secteur bancaire (Bâle III)

« Bâle III » est un ensemble de mesures faisant suite au dispositif Bâle II, publié en 2004, que le Comité de Bâle sur le contrôle bancaire a élaboré pour renforcer la réglementation, le contrôle et la gestion des risques dans le secteur bancaire. « Ces mesures ont pour objet :

- d'améliorer la capacité du secteur bancaire à absorber les chocs résultant des tensions financières et économiques, quelle qu'en soit la source ;
- d'améliorer la gestion des risques et la gouvernance ;
- de renforcer la transparence et la communication des banques. »

Copyright © 2015 Eyrolles.

ANNEXES

Les lois et le code de gouvernement d'entreprise publiés en France

- La *loi sur les Nouvelles Régulations Économiques* (*NRE*) de mai 2001 a sensiblement modifié le fonctionnement du conseil d'administration, en dissociant les fonctions exécutive et de contrôle. Elle a eu pour effet de renforcer l'indépendance des administrateurs par rapport au président. Corrélativement, elle a accru la transparence par rapport aux actionnaires (par exemple en matière de rémunération des dirigeants, ou sur les conséquences sociales et environnementales de leurs activités).
- La *Loi de Sécurité Financière* (*LSF*, 1er août 2003) couvre trois volets principaux : la modernisation des autorités de contrôle des marchés financiers, la sécurité des épargnants et le contrôle légal des comptes ainsi que la transparence et la gouvernance d'entreprise. Ce dernier volet s'adresse non seulement aux sociétés faisant appel public à l'épargne, mais à toutes les sociétés anonymes ; comme la loi américaine Sarbanes-Oxley, la LSF repose principalement, en la matière, sur :
  - une responsabilité accrue des dirigeants ;
  - un renforcement du contrôle interne : le président du conseil d'administration ou du conseil de surveillance doit rendre compte, dans un rapport, des procédures de contrôle interne mises en place dans l'entreprise ;
  - une réduction des sources de conflits d'intérêts.
- L'*ordonnance (n° 2008-1278) du 8 décembre 2008* transpose en droit français la directive (n° 2006/43/CE, *cf.* sup.), dite huitième directive sur le contrôle légal des comptes. Cette ordonnance consacre pour les sociétés faisant appel public à l'épargne l'obligation d'un comité d'audit, dont la mission est : d'assurer le suivi du processus d'élaboration de l'information financière et de l'efficacité des systèmes de contrôle interne et de gestion des risques, de suivre le contrôle légal des comptes annuels et, le cas échéant, des comptes consolidés, et de suivre le respect du principe d'indépendance des commissaires aux comptes.
- La loi du 3 juillet 2008 portant diverses dispositions d'adaptation du droit des sociétés au droit communautaire (dite « loi DDAC ») transpose la directive 2006/46CE du 14 juin 2006 en précisant les obligations des organes d'administration et de surveillance des sociétés faisant appel public à l'épargne de rendre compte, dans un rapport, de la composition, des conditions de préparation et d'organisation des travaux du conseil, ainsi que des procédures de contrôle interne et de gestion des risques mises en place par la société, en détaillant notamment les procédures qui sont relatives à l'élaboration et au traitement de l'information comptable et financière pour les comptes sociaux et, le cas échéant, pour les comptes consolidés.
- Le *code AFEP-MEDEF* de gouvernement d'entreprise des sociétés cotées révisé en 2013. Ce code a été élaboré à la demande de l'Association Française des Entreprises Privées (AFEP) et du Mouvement des Entreprises de France (MEDEF). Il complète et actualise les recommandations du rapport « Vienot » et vise à préciser certains principes de bon fonctionnement et de transparence propres à améliorer la gestion des entreprises et à répondre à la demande des investisseurs et du public. (http://www.code-afep-medef.com)

Des réglementations similaires dans d'autres pays

En Belgique

- *La loi du 08 janvier 2009* transpose la directive 2006/43/CE
- *La loi du 06 avril 2010* transpose la directive 2006/46/CE

Copyright © 2015 Eyrolles.

ANNEXES

Au Luxembourg

- *La loi du 18 décembre 2009* transpose la directive 2006/43/CE
- *La loi du 29 mai 2009 et la loi du 10 décembre 2010* transposent la directive 2006/46/CE

En Suisse

- *La directive sur la corporate governance* : Dans le même esprit que la directive européenne 2006/46/CE, la Suisse a publié en 2014 une directive qui contraint les entreprises à fournir des informations sur la « *corporate governance* » et notamment des données sur la direction et le contrôle de l'émetteur à l'échelon le plus élevé de l'entreprise. Elle présente les thèmes qui doivent être abordés par les entreprises dans leur rapport de gestion tels que la structure du groupe et l'actionnariat, la structure du capital, la composition, l'organisation et les rémunérations du conseil d'administration et de la direction générale, l'organe de révision (commissaires aux comptes) et la politique d'information. Le principe du « *comply or explain* » est repris dans cette directive.

Au Canada

- *Loi sur les sociétés par actions Québec* : la loi sur les sociétés par actions (LSA) est entrée en vigueur le 14 février 2011. Cette nouvelle loi, s'inspirant de son équivalent fédéral (Loi canadienne sur les sociétés par actions) modernise le cadre législatif en vigueur au Québec en matière de droit des entreprises en remplaçant certaines parties de l'ancienne loi sur les compagnies. Elle confie au conseil d'administration tous les pouvoirs nécessaires à la gestion de la société mais permet également aux actionnaires de s'approprier tout ou partie des pouvoirs du conseil d'administration par le biais d'une convention unanime d'actionnaires. S'ils exercent ce droit, les actionnaires assument directement la conduite des activités de l'entreprise et la surveillance des dirigeants de la société.
- Entre 2004 et 2005, à l'initiative des ACVM (Autorités canadiennes en valeurs mobilières), plusieurs règlements sont entrés en vigueur :
  - *Règlement 52-108* sur la surveillance des vérificateurs ;
  - *Règlement 52-109* sur l'attestation de l'information présentée dans les documents annuels et intermédiaires des émetteurs ;
  - *Règlement 52-110* sur le comité de vérification ;
  - *Règlement 58-101* sur l'information concernant les pratiques en matière de gouvernance ;
  - *Instruction générale 58-201* relative à la gouvernance ;
  - *Politique sur la vérification interne* : selon cette politique du Conseil du Trésor du Canada (CT) en vigueur depuis le 1er avril 2012, « les administrateurs généraux reçoivent pour leur ministère, et le contrôleur général, pour l'ensemble du gouvernement, une assurance indépendante de la vérification interne et des conseils du comité de vérification, au sujet de l'efficacité des processus de gestion des risques, de contrôle et de gouvernance mis en place ». Les exigences liées à la mise en œuvre de cette politique sont reprises dans la Directive sur la vérification interne qui précise les rôles et les responsabilités des principaux acteurs de la vérification interne, la composition des comités de vérification et le contenu des rapports annuels.

Au Maroc

- *La loi 20-05* publiée en 2008 modifie la loi 17-95 promulguée en 1996 et concerne les sociétés anonymes. Elle définit les fonctions et pouvoirs des organes de direction et de surveillance des sociétés ainsi que les informations à destination des actionnaires et les modalités de contrôles

Copyright © 2015 Eyrolles.

des sociétés anonymes notamment le rôle et la désignation des commissaires aux comptes. Ainsi, l'article 76 précise que : « Les administrateurs non dirigeants sont particulièrement chargés, au sein du conseil, du contrôle de la gestion et du suivi des audits internes et externes. Ils peuvent constituer entre eux un comité des investissements et un comité des traitements et rémunérations. »

ANNEXE 3-B : SYNTHÈSE DES PRINCIPAUX TEXTES EN VIGUEUR AUX ÉTATS-UNIS

Securities Act de 1933

Cette loi fédérale a été votée après l'effondrement des marchés de 1929 et la crise qui a suivi. Le krach a soulevé de graves questions sur l'efficacité de la gouvernance concernant la cession des valeurs mobilières. Cette loi a été promulguée par le président Franklin D. Roosevelt dans le cadre du « New deal », qui était destiné à restaurer la stabilité et la confiance des investisseurs sur les marchés des valeurs mobilières. Cette législation avait deux grands objectifs :

- renforcer la transparence des états financiers afin que les investisseurs puissent prendre des décisions éclairées à propos des titres échangés en bourse ;
- introduire des textes visant à prévenir la fraude, les déclarations mensongères et autres manœuvres frauduleuses dans la vente de valeurs mobilières sur les marchés ouverts au public.

Securities Exchange Act de 1934

Le *Securities Exchange Act* de 1934 était destiné à définir la gouvernance des transactions sur les valeurs mobilières sur le marché secondaire (après l'émission) et à régir les différentes bourses afin de protéger les investisseurs. C'est à partir de cette loi que la *Securities and Exchange Commission* (SEC) a été créée. La SEC a pour mission de faire appliquer la législation sur les valeurs mobilières, qui prévoit des obligations portant sur l'enregistrement de toute valeur cotée sur les bourses aux États-Unis, le reporting financier, la sollicitation de procurations pour le vote des actionnaires, les dépôts de garantie et l'audit. Contrairement au *Securities Act* de 1933, qui régit les émissions primaires, le *Securities Exchange Act* de 1934 régit les opérations secondaires sur titres entre des personnes généralement indépendantes de l'émetteur. Les gains et les pertes sur le marché secondaire se comptent en plusieurs centaines de milliards.

Foreign Corrupt Practices Act

En raison de pratiques douteuses de financement des campagnes électorales par des organisations ou de corruption d'agents étrangers, au milieu des années 1970, la SEC et le Congrès des États-Unis ont adopté une réforme du financement des campagnes électorales et le *Foreign Corrupt Practices Act* (FCPA) de 1977, qui pénalise la corruption internationale et impose aux organisations de mettre en œuvre des programmes de contrôle interne. Plus particulièrement, le FCPA impose aux sociétés cotées « d'établir et de tenir à jour des livres, des registres et des comptes qui, avec un degré de détail raisonnable, doivent être le reflet exact et équitable des transactions et cessions d'actifs de l'émetteur »[3]. Cette loi élargit le champ des contrôles internes, qui doivent donner l'assurance

Copyright © 2015 Eyrolles.

raisonnable que les transactions sont dûment autorisées et correctement enregistrées, que la sécurité physique des actifs est assurée et qu'un contrôle périodique est effectué sur les actifs enregistrés.

Rapport de la *National Commission on Fraudulent Financial Reporting* (rapport de la *Treadway Commission*)

Une initiative du secteur privé, appelée la *National Commission on Fraudulent Financial Reporting* (ou *Treadway Commission*) a été lancée en octobre 1985. Sa mission consistait à identifier les facteurs susceptibles de favoriser le reporting financier frauduleux et les mesures de nature à faire reculer l'incidence de ces facteurs. La Commission a étudié les affaires portées devant la SEC pendant les années qui ont précédé la présentation de son premier rapport, en 1987. Ce rapport préconisait que les organisations membres de la *Treadway Commission* collaborent à l'élaboration d'un référentiel intégré, et formulait des recommandations à l'intention des sociétés cotées, des cabinets d'experts comptables indépendants, de la SEC et d'autres autorités de régulation et de supervision, ainsi que les établissements de formation.

À la suite de ce rapport, le *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) a été créé. Le COSO se composait de l'*American Institute of Certified Public Accountants* (AICPA), de l'*American Accounting Association* (AAA), de *Financial Executives International* (FEI), de l'IIA et de l'*Institute of Management Accountants* (IMA). Le COSO a commandité l'élaboration d'un référentiel de contrôle interne, qui a été rendu public en 1992 sous le titre *Internal Control – Integrated Framework*. Ce référentiel est devenu le seul référentiel de contrôle interne accepté de tous aux États-Unis, et constitue le principal cadre de référence utilisé au plan mondial. Une version actualisée de ce référentiel, mis à jour en 2012, a été publiée au premier trimestre 2013. Elle formalise les 17 principes associés aux cinq composantes du contrôle interne présentées dans le référentiel initial.

FDICIA

Le *Federal Deposit Insurance Corporation Improvement Act* de 1991 impose aux établissements de dépôts assurés par la FDIC dont les actifs dépassent 500 millions de certifier que leur système de contrôle interne est efficace. Il demande aussi aux auditeurs externes d'attester de la véracité des critères de qualité retenus par le management concernant l'efficacité du système de contrôle interne. De nombreux aspects de cette loi ont ultérieurement été repris dans la loi Sarbanes-Oxley de 2002.

Sarbanes-Oxley Act de 2002

Après une succession de faillites retentissantes et de cas de reporting financier frauduleux concernant de grandes organisations américaines (par exemple Enron Corp., Tyco, WorldCom), le Congrès américain a voté une loi dont l'objectif global est de renforcer la responsabilité du directeur général et des directeurs financiers concernant l'intégrité du reporting financier et de restaurer la confiance des investisseurs dans les marchés financiers. Cette loi, le *Sarbanes-Oxley Act*, contient de nombreuses sections qui définissent des règles pour divers aspects de la gouvernance des sociétés cotées. Les deux sections qui ont le plus attiré l'attention du public sont les sections 302 et 404.

Copyright © 2015 Eyrolles.

- La section 302 impose au directeur général (CEO) et aux directeurs financiers (CFO) des sociétés cotées de certifier chaque trimestre, dans le cadre de la présentation des résultats trimestriels (rapport 10-K), l'efficacité des contrôles et procédures liés à la communication externe qui ont été mis en place en vue de la préparation de cette déclaration.
- La section 404 requiert que, dans le cadre de la présentation des résultats financiers annuels (rapport 10-K), l'organisation précise les critères de qualité concernant l'efficacité du contrôle interne relatif au reporting financier. Plus particulièrement, cette section impose à la plupart des organisations de renforcer la documentation et les tests relatifs aux dispositifs de contrôle interne pour étayer les critères de qualité requis.

Normes américaines de cotation en bourse

Les principales places boursières américaines (le NYSE [*New York Stock Exchange*] et le NASDAQ [*National Association of Securities Dealers Automated Quotations*]) ont publié des normes que toute organisation publique désireuse d'être cotée sur ces marchés doit respecter. Ces normes de cotation en bourse couvrent des sujets tels que l'organisation et les responsabilités du Conseil et du comité d'audit, le code de conduite, les prêts personnels aux cadres dirigeants, la nécessité d'une fonction d'audit interne et les *stock options*.

Dodd-Frank Act

Selon le résumé de cette loi de large portée, l'objectif du *Dodd-Frank Act* consiste à « instaurer un environnement économique solide afin de créer des emplois, protéger les consommateurs, restreindre l'influence de Wall Street, limiter les primes démesurées, mettre fin aux plans de sauvetage et à l'importance systémique des établissements financiers, [et] éviter une autre crise financière »[4]. À la date de publication de la troisième édition du présent manuel, les règles relatives à sa mise en œuvre sont encore en cours de rédaction.

Copyright © 2015 Eyrolles.

Questions de révision

1. Pourquoi y a-t-il des flèches partant dans les deux sens entre les différentes composantes de la gouvernance décrites à l'encadré 3-2 ?

2. Comment l'OCDE définit-elle la gouvernance ?

3. Quelle est la différence entre les deux domaines de gouvernance décrits à l'encadré 3-3 ?

4. Comment l'IIA définit-il la gouvernance ? En quoi le schéma de l'encadré 3-3 illustre-t-il cette définition ?

5. Quelles sont les trois différentes catégories de parties prenantes que le Conseil doit comprendre ? Donnez des exemples pour chaque catégorie.

6. Quels types de résultats le Conseil doit-il prendre en compte pour comprendre les attentes des parties prenantes ?

7. Dans la gouvernance, quelles sont les principales responsabilités :
   a. du Conseil ?
   b. de la direction générale ?
   c. des propriétaires de risques ?

8. Quel rôle joue l'audit interne dans la gouvernance ?

9. Outre l'audit interne, quelles sont les autres fonctions internes qui peuvent donner une assurance indépendante au Conseil ou à la direction générale ?

10. Quelles sont les trois lignes qui composent le modèle des trois lignes de maîtrise ?

11. Qu'est-ce qu'un modèle d'assurance combiné ? Pourquoi certaines organisations utilisent-elles un tel modèle ?

12. Citez quelques-uns des principaux textes en vigueur aux États-Unis qui ont été adoptés en réponse à des événements défavorables survenus dans le monde des affaires.

Copyright © 2015 Eyrolles.

Questions à choix multiples

Sélectionnez la meilleure réponse pour chacune des questions suivantes.

1. Parmi les éléments suivants, lequel ne désigne pas un rôle approprié pour le Conseil d'une organisation ?
   a. Évaluer et valider les objectifs stratégiques.
   b. Influencer la philosophie de prise de risque de l'organisation.
   c. Donner une assurance directement à des tiers quant à l'efficacité des processus de gouvernance de l'organisation.
   d. Instaurer des limites générales de conduite en dehors desquelles l'organisation ne doit pas s'aventurer.

2. Parmi les éléments suivants, lesquels relèvent normalement des responsabilités de gouvernance de la direction générale ?
   I. Déléguer des seuils de tolérance au risque directement aux managers des risques.
   II. Piloter quotidiennement les performances des activités spécifiques de gestion des risques.
   III. Instaurer un comité de gouvernance au sein du Conseil.
   IV. Veiller à ce que des informations suffisantes soient collectées pour étayer les rapports remis au Conseil.
   a. I et IV.
   b. II et III.
   c. I, II et IV
   d. I, II, III et IV.

3. La compagnie d'électricité ABC vend de l'électricité à des clients résidentiels et fait partie d'une association sectorielle qui donne des orientations aux compagnies d'électricité et aux groupes de pression de ce secteur et facilite la coopération entre ses membres. Du point de vue d'ABC, cette association sectorielle est une partie prenante de quel type ?
   a. Elle *participe* directement au fonctionnement de l'organisation.
   b. Elle a un *intérêt* dans le succès de l'organisation.
   c. Elle *influence* l'organisation.
   d. Ce n'est pas une partie prenante.

Copyright © 2015 Eyrolles.

4. Qui a la responsabilité de définir les objectifs *stratégiques* d'une organisation ?
   a. Le Conseil.
   b. La direction générale.
   c. Un consensus entre les niveaux hiérarchiques.
   d. Le Conseil et la direction générale conjointement.

5. Qui doit, en dernier ressort, repérer les principaux risques nouveaux ou émergents qui doivent être couverts par le processus de gouvernance de l'organisation ?
   a. Le Conseil.
   b. La direction générale.
   c. Les propriétaires de risques.
   d. L'audit interne.

6. L'audit interne ne devrait pas :
   a. Évaluer les processus de gouvernance et de gestion des risques de l'organisation.
   b. Apporter des conseils sur la façon d'améliorer les processus de gouvernance et de gestion des risques de l'organisation.
   c. Superviser les processus de gouvernance et de gestion des risques de l'organisation.
   d. Coordonner ses activités en matière de gouvernance et de gestion des risques avec celles de l'auditeur externe.

7. Parmi les propositions suivantes, laquelle ne pourrait être considérée comme une première ligne de maîtrise selon le Modèle des trois lignes de maîtrise ?
   a. Un contrôleur de gestion au niveau des divisions effectue une revue réciproque pour s'assurer de la conformité aux normes de contrôle financier.
   b. Un collaborateur du service de la comptabilité fournisseurs examine les pièces justificatives avant de traiter une facture à régler.
   c. Un superviseur du service de la comptabilité effectue une revue mensuelle afin de s'assurer que tous les rapprochements ont été réalisés correctement.
   d. Un ouvrier de la chaîne de production inspecte les produits finis afin de s'assurer que les normes de qualité de l'organisation ont été respectées.

Copyright © 2015 Eyrolles.

Thèmes de discussion

1. Décrivez de quelles manières le modèle économique d'une organisation peut influer sur son approche de la surveillance de la gouvernance. Donnez des exemples en mettant en évidence les différences entre les sociétés cotées et les autres.

2. Expliquez pourquoi il est important, du point de vue de la gouvernance, que des administrateurs externes indépendants siègent au Conseil.

3. Étant donné qu'habituellement les administrateurs n'ont aucune interface directe avec les principales parties prenantes, comment le Conseil peut-il faire pour comprendre les attentes de ces dernières ? Comment ce processus peut-il varier entre les différentes catégories de parties prenantes décrites dans ce chapitre ?

4. Dans l'encadré 3-4, l'audit interne est inclus dans le cadre des activités d'assurance. Étant donné ce rôle d'assurance, décrivez les avantages et les inconvénients d'une situation dans laquelle le responsable de l'audit interne rend compte au Conseil (ou à l'un de ses comités), par comparaison à la situation dans laquelle il rend compte au directeur financier. Étayez votre réponse avec les concepts décrits dans la Norme 1100, Indépendance et objectivité.

5. La gouvernance des systèmes d'information (SI) est devenue un thème à la mode ces dernières années. En vous aidant du cadre de référence de la gouvernance présenté dans l'encadré 3-4, personnalisez chacune des composantes afin de décrire comment elles pourraient spécifiquement être liées aux objectifs et aux risques d'une organisation concernant la gouvernance des SI.

6. La Cour des comptes du pays ABC a publié un rapport sur la coopérative électrique XYZ, grand producteur d'électricité détenu par ses membres. Ce rapport examine le travail effectué par MNO Consulting, qui a constaté de nombreuses faiblesses dans le contrôle interne. La Cour des comptes confirme la conclusion de MNO, et rejoint ses recommandations concernant le manque général de contrôle interne efficace. La Cour des comptes recommande en particulier que l'assemblée législative du pays adopte une loi contraignant les coopératives à :
   - former un Conseil et se doter d'un comité d'audit distinct ;
   - employer un auditeur interne qui rend compte au Conseil.

   Le journaliste d'un quotidien local a quelques questions à vous poser :

   a. Normalement, quelles sont les responsabilités du Conseil concernant le contrôle interne ?

   b. Pourquoi la Cour des comptes souhaite-t-elle que le Conseil de toutes les coopératives emploie un auditeur interne ?

Copyright © 2015 Eyrolles.



Thèmes de discussion

7. Le responsable de l'audit interne de l'organisation PJS collabore avec la direction générale et le Conseil pour élaborer un modèle d'assurance combiné et vous demande des conseils. Il souhaite notamment que vous répondiez aux questions suivantes.
   a. Dans un modèle d'assurance combiné, l'audit interne devrait-il reporter les missions d'assurance dans les domaines déjà couverts par d'autres prestataires d'activités d'assurance ?
   b. Quels sont les facteurs susceptibles d'influencer la décision du responsable de l'audit interne quant au report d'une mission d'assurance ?
   c. Quels services l'audit interne peut-il fournir en remplacement d'une mission d'assurance ?

8. Indiquez comment les textes de loi contribuent à améliorer la gouvernance. Expliquez en quoi certains textes peuvent avoir des conséquences inattendues en matière de gouvernance.

Copyright © 2015 Eyrolles.

ÉTUDES DE CAS

CAS N° 1 Étudiez les règles régissant la gouvernance en Australie, en Afrique du Sud et en Europe (plus particulièrement au Royaume-Uni et en France). Effectuez des recherches supplémentaires sur Internet afin de répondre aux questions suivantes.

1. Quels événements ont poussé chacun de ces pays à adopter ces règles ?
2. Expliquez en quoi ces textes sont similaires.
3. Décrivez au moins une différence notable entre chacun de ces textes.
4. Selon vous, parmi ces textes, lequel pose les exigences les plus complètes concernant la gouvernance ? Pourquoi ?

CAS N° 2 Le site Internet de l'IIA comprend différents blogs. L'un d'entre eux est consacré à la gouvernance (www.theiia.org/blogs/marks). Rendez-vous sur ce blog, consultez les trois dernières publications, ainsi que les commentaires y afférents, et préparez-vous à en discuter en cours.

Copyright © 2015 Eyrolles.



Copyright © 2015 Eyrolles.



Copyright © 2015 Eyrolles.

CHAPITRE 4
LA GESTION DES RISQUES

Objectifs pédagogiques

- Définir le risque et le management des risques de l'entreprise (*Entreprise Risk Management* – ERM).
- Débattre des différentes composantes du référentiel « Le Management des risques de l'entreprise » du *Committee of Sponsoring Organizations of the Treadway Commission* (COSO II).
- Débattre des différentes composantes de la norme ISO 31000:2009 : Management du risque – Principes et lignes directrices.
- Définir la relation entre gouvernance et management des risques de l'entreprise.
- Décrire les différents rôles attribués à l'audit interne dans le management des risques de l'entreprise.
- Évaluer l'impact du management des risques de l'entreprise sur les activités d'audit interne.

Dans la vie, les incertitudes sont omniprésentes dans nos activités quotidiennes. Il est souvent impossible de connaître à l'avance le résultat exact de nos actions. C'est au quotidien que vous agissez face à ces incertitudes qui peuvent déterminer votre réussite dans la vie.

Il en va de même quand il s'agit de faire fonctionner une organisation. Les incertitudes sont nombreuses, et la réussite des organisations dépend de la manière dont ces incertitudes sont gérées. L'audit interne peut y jouer un rôle important.

Revenons à l'encadré 3-2 du chapitre 3, *La gouvernance*. La gestion des risques y est décrite comme la strate intermédiaire de la structure de gouvernance. Elle vise :

- à détecter et à maîtriser les risques susceptibles d'entraver la réussite de l'organisation ;
- à exploiter les opportunités susceptibles de conduire à cette réussite.

Le management élabore des stratégies afin d'optimiser la gestion des principaux risques et opportunités. Les activités de gestion des risques doivent suivre la direction donnée par la structure de gouvernance.

Comme dans l'analyse de la gouvernance au chapitre 3, le présent chapitre décrit en détail la gestion des risques et en expose les composantes et principes clés ainsi que les divers rôles et responsabilités s'y rapportant. D'autres illustrations permettront de décrire, de manière plus approfondie, comment envisager les principaux éléments de la gestion des risques.

Ce chapitre se terminera par une analyse sur la manière dont l'audit interne peut faire partie intégrante de la gestion des risques. Il traite des rôles spécifiques de l'audit interne, ainsi que de l'impact que la gestion des risques peut avoir sur le plan d'audit interne.

Avant d'engager l'étude de la gestion des risques, il importe de comprendre pourquoi il s'agit là d'un sujet de débat fréquent dans le monde des affaires. Bon nombre d'organisations ont constaté que mettre en œuvre une gestion des risques efficace est plus difficile qu'elles ne le pensaient. Cependant, elles ont de plus en plus de raisons de se doter de capacités solides dans ce domaine qui participe à la réussite des organisations. D'ailleurs, aux États-Unis, les agences de notation accordent désormais une large place à la gestion des risques dans leurs évaluations. *Moody's Investors Services* intègre la gouvernance dans ses notes et tient également compte de la gestion des risques. Depuis 2008, Standard & Poor's évalue certains éléments de la gestion des risques dans l'intention de les intégrer formellement dans ses notes.

Commentaire du traducteur

En Europe, un cadre de référence de la gestion des risques a été élaboré sous l'égide de la FERMA (Federation of European Risk Management).

ENCADRÉ 4-1

DISPOSITIONS DU CRIPP PERTINENTES RELATIVES AU CHAPITRE 4

Norme 2010 – Planification
Norme 2100 – Nature du travail
Norme 2120 – Management des risques
Modalité Pratique d'Application 2010-1 : La prise en compte des risques et des menaces pour l'élaboration du plan d'audit
Modalité Pratique d'Application 2120-1 : Évaluer la pertinence des processus de management des risques
Modalité Pratique d'Application 2210.A1-1 : Évaluation des risques dans la planification de la mission
Guide pratique : Évaluer l'adéquation du management des risques
Guide pratique : *Coordinating Risk Management and Assurance*

Copyright © 2015 Eyrolles.

PRÉSENTATION DE LA GESTION DES RISQUES

Bref historique du risque

La gestion des risques n'est pas un phénomène récent, ni un axe inédit pour aborder la gestion d'une organisation. Dans *Plus fort que les dieux, la remarquable histoire du risque*, Peter L. Bernstein propose une histoire complète du risque, qui montre comment ont évolué au fil des siècles l'acceptation et la compréhension du risque.

- Il est fait mention des jeux de hasard dans des documents datant de plusieurs siècles, qui remontent aux civilisations grecque et égyptienne, ainsi que dans la Bible (par exemple, les soldats de Ponce Pilate ont tiré au sort la tunique de Jésus Christ après l'avoir crucifié). Si les jeux de hasard sont aussi vieux que l'humanité, la théorie des probabilités n'a été découverte qu'à la Renaissance, au milieu du XVII^e siècle. Par la suite, elle est passée du statut d'exercice mathématique permettant d'expliquer les résultats des jeux de hasard à celui d'outil crucial dans le monde de l'entreprise pour étayer la prise de décision.
- Dès les III^e et II^e siècles avant J.-C., les négociants chinois et babyloniens recouraient à des pratiques de transfert et de répartition des risques. Ce sont les Grecs et les Romains qui ont introduit les premières formes d'assurance maladie et d'assurance vie, aux environs de l'an 600 de notre ère. Vers la fin du XVII^e siècle, Londres devenant un pôle commercial de plus en plus important, il s'y est développé une demande croissante d'assurance maritime. À la fin des années 1680, Edward Lloyd a ouvert un café qui est devenu un repaire populaire auprès des armateurs, marchands et capitaines de navires, ce qui en faisait une source fiable où trouver les dernières nouvelles du transport maritime. C'est devenu le lieu de rencontre entre les différentes parties désireuses de faire assurer cargaisons et navires et celles qui étaient prêtes à assurer ces entreprises risquées. À l'heure actuelle, la Lloyd's of London est encore l'une des plus grandes sociétés d'assurance au monde.
- Tout comme dans l'assurance, les banques et autres établissements financiers ont toujours été confrontés au risque dans tous les aspects de leur activité. Les premières banques ont probablement été les temples religieux de l'Antiquité. On trouve mention de prêts au XVIII^e siècle avant J.-C. à Babylone, concédés par des prêtres des temples à des marchands. Quant aux empires grec et romain, ils ont contribué à faire évoluer les pratiques bancaires des prêts, des dépôts et du change. Les banques utilisent le concept de risque pour déterminer les taux qu'ils peuvent appliquer aux prêts en fonction de leur propre coût de financement et de la probabilité de défaut. Les établissements financiers ont également élaboré des instruments financiers, tels que les options, les contrats d'échange (*swaps*) et les dérivés, qui créent de la valeur selon la probabilité de réalisation d'événements à venir[1].

Copyright © 2015 Eyrolles.

Risque (définition du COSO)

Possibilité qu'un événement survienne et ait un impact défavorable sur la réalisation des objectifs.

Opportunité

Événement susceptible d'avoir un impact positif sur la réalisation des objectifs.

Les définitions du risque

Le mot français risque dérive du latin *resecare*, qui a donné l'italien *rischiare*, verbe qui signifie « oser » ; il s'agit de faire un choix dans des contextes d'incertitude, plutôt que d'adopter un comportement fataliste[2]. La clé de cette définition est la notion d'incertitude. Partant de cette définition, le *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) définit le risque comme « la possibilité qu'un événement survienne et ait un impact défavorable sur la réalisation des objectifs »[3]. L'Organisation internationale de normalisation (ISO), située en Suisse, définit tout simplement le risque comme « l'effet de l'incertitude sur les objectifs »[4].

Des définitions du risque proposées par le COSO et l'ISO peuvent se dégager un certain nombre de points clés fondamentaux.

- Le risque est inhérent à la formulation de la stratégie et à la fixation des objectifs. Une organisation mène ses activités dans le but de mettre en œuvre des stratégies et d'atteindre des objectifs précis, et les risques correspondent aux obstacles qui sont susceptibles d'affecter la réalisation de ces objectifs. En conséquence, puisque chaque organisation a des stratégies et des objectifs différents, chacune sera confrontée à des risques propres.
- Le risque ne représente pas une estimation à un moment précis (par exemple l'issue la plus probable), mais plutôt un éventail d'issues possibles. Parce que de nombreuses issues différentes sont possibles, l'idée d'éventail est ce qui crée l'incertitude lorsque l'on cherche à comprendre et à évaluer les risques.
- La notion de risque peut renvoyer à la volonté d'empêcher que des événements négatifs ne surviennent (maîtrise des risques), ou la capacité de faire en sorte que des choses positives se produisent (c'est-à-dire exploiter des opportunités ou en tirer parti). La plupart des gens se concentrent sur la première de ces deux idées, par exemple sur un danger qui doit être écarté ou éliminé. Certes, de nombreux risques présentent effectivement une menace pour une organisation, mais ne pas aboutir à une issue positive peut également générer un obstacle à la réalisation d'un objectif, et constitue donc aussi un risque.
- Les risques sont inhérents à tous les aspects de la vie : partout où il y a de l'incertitude, il existe un ou plusieurs risques. Les exemples présentés plus haut dans la section historique montrent comment a évolué la compréhension du risque. Les risques spécifiquement associés à une organisation selon sa structure ou son activité commerciale sont généralement appelés risques opérationnels. Pour le formuler plus simplement, les incertitudes relatives aux menaces pesant sur la réalisation des objectifs de l'organisation sont considérées comme des risques opérationnels.

Copyright © 2015 Eyrolles.

À la lumière de cette définition du risque, il devient évident qu'une organisation rencontre un grand nombre de risques lorsqu'elle s'efforce d'appliquer sa stratégie et d'atteindre ses objectifs. Cette multitude de risques pouvant entraver significativement la bonne marche de l'organisation, il apparaît d'autant plus nécessaire de disposer d'un processus qui permette de comprendre et de gérer efficacement les risques dans l'ensemble de l'organisation. Tel est le but du management des risques de l'entreprise (*Entreprise Risk Management* – ERM).

Risques opérationnels

Risques spécifiquement associés à une organisation selon sa structure ou son activité commerciale : incertitudes relatives aux menaces pesant sur la réalisation des objectifs de l'organisation.

LE CADRE DE RÉFÉRENCE RELATIF AU MANAGEMENT DES RISQUES DE L'ENTREPRISE ÉLABORÉ PAR LE COSO

Aux États-Unis, le COSO a publié en 2004 *Enterprise Risk Management – Integrated Framework* (dispositif de management des risques du COSO ou cadre de référence relatif au management des risques de l'entreprise) traduit en français par l'IFACI et *PricewaterhouseCoopers* en 2005 sous le titre « Le Management des risques de l'entreprise, Cadre de référence – Techniques d'application ». Le COSO a perçu la nécessité d'établir un cadre de référence solide permettant d'aider les organisations à identifier, évaluer et gérer efficacement le risque. Le cadre de référence qui en résulte prend pour base l'ouvrage *Internal Control – Integrated Framework* publié précédemment (traduit en français par l'IFACI et *PricewaterhouseCoopers* sous le titre « La Pratique du contrôle interne »), intégrant tous les aspects essentiels de ce premier cadre de référence dans le contexte plus large du management des risques de l'entreprise.

Le COSO définit le management des risques de l'entreprise en ces termes :

> *« Processus mis en œuvre par le Conseil d'administration, la direction générale, le management et l'ensemble des collaborateurs de l'organisation. Il est pris en compte dans l'élaboration de la stratégie ainsi que dans toutes les activités de l'organisation. Il est conçu pour identifier les événements potentiels susceptibles d'affecter l'organisation et pour gérer les risques dans les limites de son appétence pour le risque. Il vise à fournir une assurance raisonnable quant à l'atteinte des objectifs de l'organisation. »*[5]

Le COSO explique que cette définition contient certains concepts fondamentaux. Le management des risques de l'entreprise :

- est un processus permanent qui irrigue toute l'organisation ;
- est mis en œuvre par l'ensemble des collaborateurs, à tous les niveaux de l'organisation ;
- est pris en compte dans l'élaboration de la stratégie ;
- est mis en œuvre à chaque niveau et dans chaque entité de l'organisation ;

Copyright © 2015 Eyrolles.

- permet d'obtenir une vision globale de l'exposition aux risques à l'échelle de l'entité ;
- est destiné à identifier les événements potentiels susceptibles d'affecter l'organisation ;
- permet de gérer les risques en fonction de l'appétence pour le risque de l'organisation ;
- donne à la direction générale et au Conseil une assurance raisonnable quant à la réalisation des objectifs ;
- est orienté vers l'atteinte d'objectifs appartenant à une ou plusieurs catégories indépendantes susceptibles de se recouper.

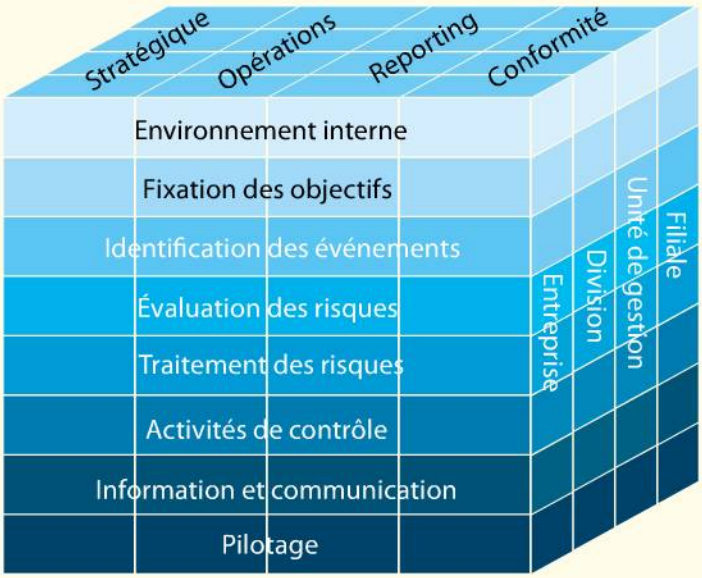
Management des risques de l'entreprise

Processus piloté par le management qui consiste à appréhender et à traiter les incertitudes (risques et opportunités) susceptibles d'affecter la capacité de l'organisation à réaliser ses objectifs.

Le cadre de référence relatif au management des risques de l'entreprise est illustré graphiquement au moyen d'une matrice en trois dimensions en forme de cube, présentée à l'encadré 4-2. Cette représentation montre qu'il existe des relations entre les différentes catégories d'objectifs (les colonnes verticales), les éléments du management des risques de l'entreprise (les lignes horizontales) et la structure de l'organisation (sur le côté du cube). Elle illustre le management des risques de l'entreprise dans sa globalité et permet de se concentrer sur une ou plusieurs catégories d'objectifs, un ou plusieurs éléments, ou une ou plusieurs entités de l'organisation ou sous-ensemble de ces entités.

ENCADRÉ 4-2

LE CUBE DU DISPOSITIF DE MANAGEMENT DES RISQUES DU COSO



Copyright 2004, *The Committee of Sponsoring Organizations of the Treadway Commission*. Reproduit avec l'aimable autorisation de l'AICPA agissant au titre d'administrateur des droits d'auteurs pour le COSO.

Copyright © 2015 Eyrolles.

Les catégories d'objectifs

Lorsque l'organisation se dote d'une mission et d'une vision, le management fixe également divers objectifs qui favorisent la réalisation de la mission, sont cohérents et se déploient dans toute l'organisation. Comme nous l'avons vu au chapitre 1, *Introduction à l'audit interne*, le cadre de référence relatif au management des risques de l'entreprise répartit les objectifs d'une organisation en quatre catégories.

- **Objectifs liés à la stratégie :** objectifs de haut niveau (liés à la stratégie de l'organisation). Ils sont en ligne avec sa mission et la soutienne.
- **Objectifs liés aux opérations :** objectifs vastes visant l'utilisation efficace et efficiente des ressources.
- **Objectifs liés au reporting :** objectifs axés sur la fiabilité du reporting (tant externe qu'interne).
- **Objectifs liés à la conformité :** objectifs visant la conformité aux lois et règlements applicables.

Le rattachement des objectifs d'une organisation à des catégories distinctes permet de se concentrer sur les différents aspects, d'égale importance, du management des risques de l'entreprise. Tout en étant distinctes, ces catégories se recoupent – un objectif donné peut relever de plusieurs d'entre elles – et répondent aux divers besoins de l'organisation. Elles peuvent relever de la responsabilité directe de différents membres de la direction générale.

Le COSO décrit ainsi la réalisation des objectifs : « L'organisation ayant le contrôle sur les objectifs relatifs à la fiabilité du reporting et à la conformité aux lois et aux règlements, il est légitime d'attendre du processus de management des risques une assurance raisonnable quant à l'atteinte de ces objectifs. En revanche, l'atteinte des objectifs stratégiques et opérationnels dépend parfois d'événements extérieurs qui peuvent échapper au contrôle de l'organisation. Par conséquent, dans ce cas, le management des risques ne peut donner qu'une assurance raisonnable que la direction et le Conseil d'administration, dans son rôle de supervision, sont informés en temps utile de l'état de progression de l'organisation vers l'atteinte de ses objectifs »[6].

Les éléments du management des risques de l'entreprise

Le dispositif de management des risques du COSO comprend huit éléments. Ils traduisent la façon dont l'organisation est gérée et sont intégrés au processus de gestion. Ces éléments sont décrits ci-après :

- **L'environnement interne.** « La direction expose sa conception en matière de management des risques et détermine

Objectifs

Ce qu'une organisation souhaite réaliser. On parle alors des objectifs de l'organisation. Ces objectifs peuvent être liés à la stratégie, aux opérations, au reporting et à la conformité

Culture du risque

Ensemble de croyances et d'attitudes partagées, caractéristiques de la façon dont l'organisation appréhende les risques dans toutes ses activités.

Copyright © 2015 Eyrolles.

l'appétence de l'organisation pour le risque. [L'environnement interne englobe la culture et l'esprit de l'organisation.] Il pose les bases qui vont déterminer la façon dont les risques et les contrôles sont appréhendés et considérés par les collaborateurs de l'entité. Les collaborateurs – avec leurs qualités individuelles, notamment l'intégrité, les valeurs éthiques, la compétence – et l'environnement dans lequel ils travaillent sont au cœur de toute organisation »[7].

Le COSO poursuit : « L'environnement interne constitue le fondement structurel de tous les autres éléments du dispositif de management des risques. Il exerce une influence sur la façon dont les stratégies et les objectifs sont définis, sur la façon dont les activités sont structurées et les risques identifiés, évalués et gérés. Il a également une influence sur la conception et le fonctionnement des activités de contrôle, sur les systèmes d'information et de communication ainsi que sur le suivi des opérations »[8].

L'environnement interne est influencé par l'histoire et la culture de l'organisation. Il englobe de nombreux éléments, dont les suivants, qui sont décrits plus en détail dans le cadre de référence du COSO.

Appétence pour le risque

Niveau de risque global qu'une organisation est prête à accepter en vue de la réalisation de ses objectifs.

- **La culture du risque**, qui représente un ensemble de croyances et d'attitudes partagées, caractéristiques de la façon dont l'organisation appréhende les risques dans toutes ses activités.
- **L'appétence pour le risque**, ou l'appétit pour le risque, c'est-à-dire le niveau de risque global qu'une organisation accepte de prendre.
- **Le Conseil d'administration**, à savoir le principal organe de gouvernance de l'organisation, qui apporte sa structure, son expérience, son indépendance et son rôle de supervision.
- **L'intégrité et les valeurs éthiques**, reflétant les choix, jugements de valeur et styles de management.
- **L'engagement de compétence**, portant sur les connaissances et les aptitudes nécessaires à l'accomplissement des tâches requises.
- **La structure organisationnelle**, à savoir l'infrastructure permettant de planifier, d'exécuter, de contrôler et de faire un suivi des activités.
- **La délégation de pouvoirs et de responsabilités**, c'est-à-dire la manière dont les individus et les équipes sont autorisés et incités à prendre des initiatives pour aborder et résoudre des problèmes, ainsi que les limites de leurs pouvoirs.
- **La politique de ressources humaines**, qui englobe les activités relatives au recrutement, à la gestion de carrière, à

Copyright © 2015 Eyrolles.

la formation, aux évaluations individuelles, au conseil, à la promotion, à la rémunération et aux actions d'amélioration.

- **La fixation des objectifs.** « Les objectifs opérationnels, de reporting et de conformité découlent des objectifs définis au niveau stratégique. Chaque organisation est confrontée à une grande variété de risques d'origines externes et internes. La condition préalable pour pouvoir identifier les opportunités et les menaces, les évaluer et y répondre efficacement est la fixation d'objectifs ».[9]

  Les objectifs doivent être alignés sur l'appétence pour le risque de l'organisation, qui détermine le niveau de risque qu'elle accepte de prendre pour atteindre ses objectifs. La tolérance au risque désigne le niveau de risque et d'écart acceptable entre les objectifs et la performance réelle ; elle doit être en adéquation avec l'appétence pour le risque de l'organisation.

Tolérance au risque

Niveau de risque et d'écart acceptable entre les objectifs et la performance réelle ; elle doit être en adéquation avec l'appétence pour le risque de l'organisation.

- **L'identification des événements.** « Le management identifie les événements potentiels qui, s'ils se réalisent, pourront affecter l'organisation. Il détermine s'ils représentent une opportunité ou s'ils sont susceptibles de nuire sérieusement à la capacité de l'entité à mettre en œuvre, avec succès, sa stratégie et à atteindre ses objectifs. Les événements ayant un impact négatif constituent des risques qui demandent une évaluation du management et un traitement. Les événements ayant un impact positif représentent des opportunités que le management doit intégrer à la stratégie et au processus de définition des objectifs. Lors de la phase d'identification des événements, le management prend en compte, à l'échelle de l'organisation dans sa globalité, différents facteurs externes et internes pouvant se traduire par des menaces et des opportunités »[10].

Le COSO cite plusieurs facteurs externes, ainsi que des exemples d'événements qui leur sont liés. Il s'agit des facteurs suivants.

- **Économiques**, tels que les fluctuations de prix, la disponibilité des capitaux ou l'abaissement des barrières à l'entrée du marché.
- **Environnementaux**, comme les inondations, les incendies, les séismes ou autres événements météorologiques.
- **Politiques**, tels que l'élection de nouveaux responsables politiques ayant des priorités différentes, la promulgation de nouvelles lois et règlements.
- **Sociaux**, à savoir les évolutions démographiques, les coutumes sociales, les structures familiales, l'équilibre entre priorités professionnelles et familiales.
- **Technologiques**, comme les nouveaux modes de commerce électronique, de stockage ou de traitement[11].

Copyright © 2015 Eyrolles.

Le COSO cite également des facteurs internes, ainsi que des exemples d'événements pouvant les accompagner.

- **Infrastructure**, par exemple l'augmentation des capitaux alloués à la prévention ou aux centres d'appels.
- **Personnel**, par exemple les accidents du travail, les activités frauduleuses ou l'expiration des accords collectifs.
- **Processus**, par exemple la modification des processus, les erreurs d'exécution ou l'externalisation.
- **Technologie**, par exemple l'augmentation des ressources pour gérer la volatilité des volumes, les violations de la sécurité ou l'interruption des systèmes[12].
- **L'évaluation des risques.** « L'évaluation des risques consiste à déterminer dans quelle mesure des événements potentiels sont susceptibles d'avoir un impact sur la réalisation des objectifs. Le management évalue la probabilité d'occurrence et l'impact de ces événements. Pour ce faire, il recourt habituellement à une combinaison de méthodes qualitatives et quantitatives. Les impacts d'un événement, qu'ils soient positifs ou négatifs, doivent être analysés individuellement ou par catégorie, à l'échelle de l'organisation. Il convient d'évaluer à la fois les risques inhérents et les risques résiduels »[13].

Risque inhérent

Combinaison de facteurs de risque internes et externes à leur état d'origine, en l'absence de contrôle, ou risque brut s'il n'existe aucun dispositif de contrôle interne.

Pour simplifier à l'extrême, le risque inhérent représente le risque « brut », tandis que le risque résiduel est le risque « net ». Le risque inhérent est celui auquel l'organisation est exposée en l'absence d'actions correctives du management pour en modifier la probabilité d'occurrence ou l'impact. Il peut être inhérent au modèle économique de l'organisation ou découler des décisions prises par le management sur la manière d'appliquer ce modèle. Le risque résiduel est défini comme le risque qui subsiste après prise en compte des modalités de traitement des risques mises en œuvre par le management (par exemple, en vue de réduire ou de transférer le risque). Le risque inhérent est évalué dans un premier temps. Le risque résiduel sera évalué à partir des modalités de traitement des risques mises en œuvre par le management dans un deuxième temps.

Il existe de multiples manières d'évaluer l'impact et la probabilité d'occurrence d'un risque, allant du recueil d'avis généraux et des points de vue de différentes personnes au *benchmarking* et à l'utilisation de modèles probabilistes sophistiqués. Quelle que soit l'option (ou la combinaison d'options) retenue, il est important que ces évaluations prennent en compte les liens entre les événements. De fait, l'impact et la probabilité des scénarios extrêmes peuvent dépendre de la manière dont différents risques sont reliés entre eux. En évaluant chaque risque individuellement, il arrive que l'organisation sous-estime le scénario extrême, qu'il est pourtant important qu'elle prenne en compte.

Copyright © 2015 Eyrolles.

Le traitement des risques. Selon le COSO, « une fois les risques évalués, le management détermine quels traitements appliquer à chacun de ces risques. Les différentes solutions possibles sont : l'évitement, la réduction, le partage et l'acceptation. En fonction de la solution retenue, il convient de considérer l'effet des différentes solutions en termes de probabilité et d'impact, ainsi que de coûts et bénéfices. Le choix doit porter sur une solution ramenant le risque résiduel en deçà du seuil de tolérance souhaité par la direction. Les opportunités potentielles sont également identifiées. Les risques et opportunités sont appréhendés de manière transversale ou agrégés de façon à déterminer si le risque résiduel global correspond à l'appétence de l'organisation pour le risque. »[14]

Les différentes modalités de traitement proposées par le COSO sont les suivantes.

- **L'évitement.** Cesser les activités à l'origine du risque. L'évitement du risque peut aussi bien avoir pour conséquence d'interrompre une ligne de produits, de ralentir l'expansion prévue sur un nouveau marché géographique ou de vendre une activité.
- **La réduction.** Prendre des mesures afin de réduire la probabilité d'occurrence, ou l'impact du risque, ou encore les deux à la fois. Il s'agit habituellement d'une multitude de décisions prises quotidiennement telle la mise en place de contrôles.
- **Le partage.** Diminuer la probabilité ou l'impact d'un risque en transférant ou en partageant le risque. Parmi les techniques courantes, citons l'achat de produits d'assurance, les opérations de couverture ou l'externalisation d'une activité.
- **L'acceptation.** Ne prendre aucune mesure pour modifier la probabilité d'occurrence du risque et son impact.[15]
- Dans les faits, l'organisation préfère accepter le risque à son niveau actuel plutôt que de dépenser de précieuses ressources pour appliquer l'une des autres modalités de traitement des risques.

Il est important de considérer les effets du traitement des risques de façon globale, ou agrégée. Dans certains cas, un traitement donné peut ne pas apparaître comme le meilleur ou le plus rentable pour un risque en particulier. Cependant si ce traitement contribue à gérer d'autres risques, l'avantage qui en découle pour l'organisation peut justifier le choix de cette option. C'est en analysant les risques selon une perspective globale que le management sera le mieux à même de les gérer de manière optimale en respectant l'appétence pour le risque définie par l'organisation.

- **Activités de contrôle.** « Les activités de contrôle sont constituées des politiques et procédures qui permettent de s'assurer que les traitements des risques souhaités par la direction ont été effectivement mis en place. Les activités de contrôle sont présentes partout dans l'organisation, à tout niveau et dans toute fonction. »[16]

Risque résiduel

Part du risque inhérent qui subsiste après prise en compte des modalités de traitement des risques mises en œuvre par le management (on parle parfois de risque net).

Contrôle

Toute mesure prise par le management, le Conseil et d'autres parties afin de gérer les risques et d'accroître la probabilité que les buts et objectifs fixés seront atteints.

Copyright © 2015 Eyrolles.

Si elles sont le plus souvent associées aux stratégies de réduction du risque, certaines peuvent aussi se révéler nécessaires lorsqu'on exécute d'autres types de traitement des risques. Elles sont classées de diverses manières et englobent diverses activités qui peuvent être préventives ou détectives, manuelles ou automatisées, et intervenir au niveau du processus ou au niveau du management. Voir le chapitre 6, *Le contrôle interne*, pour une analyse plus détaillée des différentes catégories de contrôles. Voici quelques exemples des activités de contrôle les plus courantes décrites par le COSO.

- **Revues du management.** Contrôles normalement exécutés au niveau de l'entité, tels des examens du respect du budget, l'actualisation des prévisions, la surveillance des actions de la concurrence ou des initiatives de maîtrise des coûts.
- **Supervision directe d'une activité ou d'une fonction.** Contrôles exécutés par les responsables de fonctions ou d'activités spécifiques, par exemple vérification des rapports analytiques de gestion dans leur domaine ou supervision de l'exécution des contrôles de niveau détaillé (tels des rapprochements).
- **Traitement de l'information.** Contrôles conçus pour vérifier l'exactitude, l'exhaustivité et la validation des transactions. Ce domaine englobe aussi habituellement les contrôles généraux de l'infrastructure, tels que la sécurité physique et logique, les contrôles sur la mise en œuvre des systèmes, les évolutions de versions ou les modifications, la reprise après sinistre et les contrôles des opérations issues des systèmes.
- **Contrôles physiques.** Ces contrôles englobent (1) le décompte physique des espèces, des titres, des stocks, du matériel et des autres immobilisations, et la comparaison du résultat de ce décompte avec les chiffres enregistrés dans les livres et les registres, et (2) les obstacles ou restrictions physiques, tels que les barrières et les verrous.
- **Indicateurs de performance.** Analyse et suite donnée aux écarts observés par rapport aux normes de performance ciblées ou attendues.
- **Séparation des tâches.** Séparation des tâches entre différentes personnes afin de limiter le risque d'erreur ou de fraude. Par exemple, les personnes qui entrent les nouveaux fournisseurs dans le système ne devraient pas avoir la possibilité d'autoriser une transaction de paiement en faveur de ces fournisseurs.[17]

- **Information et communication.** « Les informations pertinentes sont identifiées, saisies et communiquées dans un format et dans des délais permettant à chacun de s'acquitter de ses responsabilités. »[18] Elles doivent être suffisamment étoffées pour répondre aux besoins qu'a l'organisation de repérer, d'évaluer et de traiter le risque tout en restant dans ses différents seuils

Copyright © 2015 Eyrolles.

de tolérance au risque. Les systèmes d'information traitent des données générées en interne et en externe notamment pour que les informations soient utiles à la gestion des risques. Enfin, l'information doit être de qualité suffisante pour étayer la prise de décisions. Le COSO précise que l'information doit être :

- appropriée et aussi détaillée que nécessaire ;
- disponible dès que nécessaire ;
- actualisée, reflétant les données opérationnelles et financières les plus récentes ;
- exacte et fiable ;
- accessible à ceux qui en ont besoin.

Le COSO poursuit : « Pour être efficace, la circulation de l'information doit être multidirectionnelle, ascendante, descendante et transversale au sein d'une organisation. Tous les collaborateurs reçoivent un message clair de la direction indiquant que les responsabilités en matière de management des risques doivent être prises au sérieux. Ils comprennent le rôle qu'ils ont à jouer dans le dispositif de management des risques et les interactions entre leurs activités et celles des autres membres du personnel. Ils doivent disposer de moyens de communication leur permettant de faire remonter les informations importantes. La communication avec les partenaires externes tels que les clients, les fournisseurs, les régulateurs et les actionnaires doit également être efficace. »[19]

La communication peut revêtir des formes très diverses : manuels de politique de l'organisation, notes internes, courriels, sites Internet et Intranet, avis sur des panneaux d'affichage et messages vidéo. Lorsque les messages sont transmis oralement, le ton de la voix et la gestuelle peuvent aussi influer sur la manière dont les messages sont interprétés.

- **Pilotage.** « Le dispositif de management des risques fait l'objet d'un pilotage qui repose sur l'évaluation de l'existence et du fonctionnement de ses éléments au fil du temps. »[20] Ce type de contrôle descendant peut s'opérer par le biais d'opérations courantes de pilotage, d'évaluations spécifiques ou d'une combinaison des deux. Les opérations courantes de pilotage s'inscrivent généralement dans le cadre des activités quotidiennes du management. La nature, l'étendue et la fréquence des évaluations spécifiques dépendent principalement de l'appréciation, par le management, des risques sous-jacents et de l'efficacité des procédures de pilotage existantes. Les déficiences relevées grâce à ce pilotage sont remontées à la hiérarchie. Les problèmes les plus graves sont portés à l'attention de la direction générale et du Conseil.

  En dehors des activités courantes de pilotage effectuées par le management, d'autres activités peuvent participer au processus de pilotage. Ainsi, les personnes chargées d'exécuter des activités importantes peuvent procéder à une auto-évaluation afin de

Pilotage

Processus qui évalue la mise en place et le fonctionnement de la gouvernance, de la gestion des risques et des contrôles au fil du temps. Il existe trois types de pilotage :
– opérations courantes ;
– évaluations spécifiques ;
– combinaison des deux.

Copyright © 2015 Eyrolles.

déterminer l'efficacité de leurs activités de gestion des risques. Généralement, les auditeurs internes font partie du système global de pilotage, et les résultats de chaque audit permettent d'évaluer l'efficacité des activités de gestion des risques y afférentes. Dans certaines circonstances, les travaux des auditeurs externes peuvent aussi influer sur l'évaluation par le management de l'efficacité de ses activités courantes de gestion des risques.

Par nature, les éléments du management des risques de l'entreprise constituent un environnement qui permet de répondre à quelques questions courantes et quotidiennes résumant la philosophie de la gestion des risques (liée au cadre de référence relatif au management des risques de l'entreprise) :

1. Qu'essayons-nous d'accomplir (quels sont nos objectifs) ?
2. Qu'est-ce qui pourrait nous empêcher de les accomplir (quels sont les risques, quelle que soit leur gravité, et comment sont-ils susceptibles de se produire) ?
3. Quelles options avons-nous pour que cela ne se produise pas (quelles sont les stratégies de gestion des risques, donc les modalités de traitement, disponibles) ?
4. Sommes-nous en mesure de mettre en œuvre ces options (avons-nous élaboré et instauré des activités de contrôle permettant de déployer les stratégies de gestion des risques) ?
5. Comment saurons-nous que nous avons atteint nos objectifs (existe-t-il des informations qui permettront d'attester de la réussite et pouvons-nous suivre les performances de manière à vérifier que nous avons réussi) ?

Ces cinq questions ne s'appliquent pas uniquement à la gestion des risques d'une organisation. Elles peuvent s'appliquer à presque tout objectif et décision. Le fait de répondre à ces questions instaure une réflexion et des approches orientées sur la gestion des risques en ligne avec le dispositif de management des risques du COSO et d'autres cadres de référence relatifs à la gestion des risques.

Rôles et responsabilités dans le cadre du management des risques de l'entreprise

Le Conseil, la direction générale, le management, les directeurs des risques, les directeurs financiers, les auditeurs internes et même chaque personne au sein d'une organisation contribuent à l'efficacité du management des risques de l'entreprise. Les rôles et les responsabilités de chacune de ces catégories concordent avec ceux évoqués au chapitre 3, *La gouvernance*.

- **Le Conseil.** Le Conseil surveille et dirige la direction générale d'une organisation. Il peut jouer un rôle dans la définition de

Copyright © 2015 Eyrolles.

la stratégie, la formulation des objectifs de haut niveau, l'affectation globale des ressources et la création de l'environnement éthique. Le COSO précise que, pour avoir une vue globale du dispositif de management des risques de l'organisation, le Conseil d'administration doit :

- avoir connaissance des limites de l'efficacité du dispositif de management des risques mis en place par le management au sein de l'organisation ;
- avoir connaissance et accepter l'appétence de l'organisation pour le risque ;
- revoir les risques auxquels l'entité est soumise par rapport à son appétence pour ceux-ci ;
- être informé des principaux risques et savoir que le management les gère de façon appropriée.[21]

Le Conseil est l'un des éléments de l'environnement interne du management des risques de l'entreprise. Il doit donc être composé de façon à permettre un dispositif de management des risques efficace. Il contribue à définir l'environnement dans lequel s'inscrit le management des risques de l'entreprise, apporte des conseils sur les principaux critères de risque de l'organisation et les approuve. Le Conseil exerce ses responsabilités *via* différents comités, tels que le comité d'audit, le comité de nomination et le comité de gouvernance.

- **Le management.** Le management est responsable de toutes les activités d'une organisation, y compris du management des risques de l'entreprise. Cependant, ses responsabilités varient suivant le niveau hiérarchique et les caractéristiques de l'organisation.

  Le directeur général (DG) a la responsabilité ultime de l'efficacité et de l'efficience du management des risques de l'entreprise. L'un des aspects les plus importants de sa responsabilité consiste à veiller à l'existence d'un environnement interne propice. Le DG fait preuve d'exemplarité au plus haut niveau de l'organisation, est force de proposition sur la composition et les activités du Conseil, exerce un leadership, définit une orientation aux managers. Il pilote l'ensemble des activités de l'organisation liées au risque, en fonction de l'appétence pour le risque définie par l'organisation et d'autres critères de risque tels que la capacité à assumer le risque et la tolérance au risque. Si des changements importants de l'environnement, l'émergence de nouveaux risques, la mise en œuvre de la stratégie ou d'actions préventives écartent l'organisation de ces critères de risque, le DG prend les mesures nécessaires pour recadrer l'activité.

  Les managers en charge des différentes unités sont responsables de la gestion des risques liés aux objectifs spécifiques de ces unités. Ils traduisent la stratégie globale de l'organisation en activités relatives aux opérations courantes, identifient

Copyright © 2015 Eyrolles.

les événements présentant un risque potentiel, évaluent ce risque et y apportent un traitement afin de le gérer. Les managers orientent l'application des éléments du management des risques de l'entreprise au sein de leur sphère de responsabilité, en s'assurant que cette application est conforme aux seuils de tolérance au risque définis. Ils délèguent aux managers des processus fonctionnels la responsabilité de certaines procédures de management des risques de l'entreprise. En conséquence, ces managers jouent habituellement un rôle actif dans la définition et l'exécution des procédures applicables aux objectifs de leur unité (techniques d'identification des événements et d'évaluation du risque, par exemple), ainsi que dans la conception des traitements spécifiques des risques (stratégies de gestion des risques). C'est le cas, par exemple, lorsque le management développe des règles et procédures applicables à l'achat de matières premières ou à l'acceptation de nouveaux clients.

Les fonctions transverses telles les ressources humaines, la comptabilité, la gestion de la conformité ou les services juridiques jouent également un rôle de soutien important dans la conception et l'exécution des pratiques efficaces de management des risques de l'entreprise. Ces fonctions peuvent concevoir et aider à la mise en œuvre de programmes permettant de gérer certains des principaux risques dans toute l'organisation.

- **Le directeur des risques.** Certaines organisations ont instauré un poste de direction qui sert de point de coordination centralisé pour faciliter le management des risques de l'entreprise. Ce directeur des risques, encore appelé dans certaines organisations « *risk manager* » ou « *chief risk officer* » ou « responsable des risques », travaille avec les managers opérationnels pour établir un management des risques de l'entreprise efficace au sein de leur sphère de responsabilité. Le directeur des risques dispose des ressources nécessaires à la gestion du management des risques de l'entreprise dans l'ensemble des filiales, branches, services, fonctions et activités. Il peut avoir la responsabilité du pilotage de la mise en œuvre du dispositif et aider les autres managers à communiquer les informations pertinentes relatives aux risques de manière ascendante, descendante et transversale au sein de l'organisation.

Le COSO décrit les responsabilités spécifiques de ce directeur des risques :

- définir des politiques de management des risques, y compris les rôles, responsabilités, et les objectifs de mise en œuvre ;
- délimiter, au sein de l'organisation, des personnes ayant la responsabilité du dispositif de management des risques ;
- promouvoir une compétence en matière de management des risques au sein de l'entité, en développant un savoir-faire et une expertise et en aidant les managers opérationnels à mettre

Directeur des risques

Poste de direction instauré dans de nombreuses organisations, qui sert de point de coordination centralisé pour faciliter la gestion des risques.

Copyright © 2015 Eyrolles.

en adéquation les traitements des risques avec la tolérance au risque, ainsi qu'en définissant les contrôles appropriés ;

- aider à intégrer le dispositif de management des risques dans les activités de planification et de management ;
- établir un langage commun en matière de management des risques qui intègre des mesures communes relatives à la probabilité et à l'impact et qui définisse des catégories communes de risques ;
- faciliter le développement par les managers de protocoles de reporting qui tiennent compte de seuils quantitatifs et qualitatifs et superviser le processus de reporting ;
- rendre compte au Directeur général des progrès et améliorations et recommander les actions nécessaires.[22]

- **La direction financière.** Les cadres rattachés à la Direction financière (comptabilité, contrôle de gestion, etc.) ainsi que leurs équipes s'occupent d'activités qui concernent toute l'organisation. Ils participent souvent à l'établissement des budgets et des plans à l'échelle de l'organisation et ils suivent et analysent leur exécution sous l'angle de l'exploitation, de la conformité et du reporting. Ils jouent un rôle majeur dans la prévention et la détection du reporting frauduleux et influent sur la conception, la mise en œuvre et le pilotage du système de contrôle interne relatif au reporting financier et des systèmes annexes.

- **Les auditeurs internes.** Les auditeurs internes occupent une place importante dans l'évaluation de l'efficacité du management des risques de l'entreprise et dans la formulation de recommandations sur les améliorations à y apporter. Les *Normes internationales pour la pratique professionnelle de l'audit interne* (les *Normes*) établies par l'*Institute of Internal Auditors* précisent que le périmètre des activités de l'audit interne doit englober la gouvernance, la gestion des risques et les systèmes de contrôle. Cela comprend l'évaluation de la fiabilité du reporting, de l'efficacité et de l'efficience des opérations et de la conformité aux lois et règlements. Dans l'exercice de leurs responsabilités, les auditeurs internes assistent la direction générale et le Conseil par l'examen, l'évaluation, le reporting et les recommandations visant à améliorer l'adéquation et l'efficacité du management des risques de l'organisation.

- **Les autres collaborateurs.** En réalité, le management des risques de l'entreprise relève de la responsabilité de l'ensemble des collaborateurs de l'organisation et devrait donc, à ce titre, faire partie intégrante du descriptif de chaque poste, de façon explicite (fiche de poste) ou implicite. Cet aspect est important pour au moins deux raisons :

  - si tous les collaborateurs ne peuvent pas être considérés intrinsèquement comme des propriétaires de risques, presque tous jouent un rôle dans le management des risques

Copyright © 2015 Eyrolles.

de l'entreprise, allant de la production d'informations utilisées pour l'identification ou l'évaluation des risques à la mise en œuvre des stratégies et des actions nécessaires à la gestion de ces risques ;

- tous les collaborateurs sont responsables des flux d'informations et de communication inhérents au management des risques de l'entreprise et font partie intégrante de ce dispositif.

- **Les auditeurs externes.** Les auditeurs externes d'une organisation peuvent fournir à la direction générale et au Conseil un point de vue éclairé, indépendant et objectif sur la gestion des risques qui peut contribuer, entre autres, à la réalisation, par l'organisation, de ses objectifs liés au reporting financier externe. Les constats issus de leurs audits peuvent porter sur les déficiences relatives à la gestion des risques, les informations analytiques et autres recommandations d'amélioration, qui sont autant d'informations précieuses pour le renforcement du programme de gestion des risques.

- **Le législateur et le régulateur.** Ils exercent une influence sur le management des risques de nombreuses organisations, soit en leur imposant la mise en place de mécanismes de gestion des risques ou de contrôle interne (c'est par exemple le cas du *Sarbanes-Oxley Act* voté en 2002 aux États-Unis), soit en soumettant certaines entités à un examen (effectué par des inspecteurs bancaires fédéraux et d'État par exemple).

Commentaire du traducteur

En Europe, la 8e directive (modifiée par la directive 2014/56/UE du 16 avril 2014) concernant les contrôles légaux des comptes annuels et des comptes consolidés charge le comité d'audit d'assurer le suivi de l'efficacité des systèmes de contrôle interne et de gestion des risques.

Le législateur et le régulateur peuvent établir des règles contraignant le management à s'assurer que son système de gestion des risques et de contrôle interne répond à certaines exigences législatives et réglementaires minimales. De plus, ils peuvent procéder par la suite à un examen obligatoire qui fera apparaître des informations utiles à l'organisation dans l'application du management des risques de l'entreprise et émettre des recommandations à l'attention du management concernant les améliorations à apporter.

- **Les autres tiers extérieurs.** Enfin, d'autres parties prenantes extérieures peuvent influer sur les activités relatives au management des risques d'une organisation :

  - les clients, fournisseurs, partenaires et autres tiers qui ont une relation d'affaires avec l'organisation constituent une source importante d'informations à utiliser dans le cadre du management des risques de l'entreprise ;

Copyright © 2015 Eyrolles.

- les créanciers peuvent surveiller et influencer la manière dont les organisations atteignent leurs objectifs. Ainsi, certains contrats de prêts imposent aux organisations de procéder à un pilotage et à un reporting différents de ceux qu'elles auraient effectués spontanément ;
- les analystes financiers, les agences de notation, les médias et autres tiers extérieurs peuvent influer sur les activités de gestion des risques. Ils mènent des activités d'investigation et de surveillance qui sont susceptibles de donner des indications sur la manière dont les tiers perçoivent les performances d'une organisation, sur les risques sectoriels et économiques auxquels elle est confrontée, sur des stratégies d'exploitation ou de financement innovantes et sur les tendances du secteur. Le management doit tenir compte des observations et commentaires formulés par ces tiers et, si nécessaire, ajuster les activités de gestion des risques correspondantes ;
- les prestataires de services externalisés permettent de plus en plus aux organisations de déléguer la gestion quotidienne de certaines fonctions non essentielles. Les tiers extérieurs évoqués ci-dessus peuvent influencer directement les activités de management des risques d'une organisation, mais le recours à des prestataires extérieurs peut également entraîner des risques et des modalités de traitement différents de ceux que l'organisation rencontrerait et appliquerait si elle n'externalisait pas la prestation. Bien que ces tiers extérieurs puissent exécuter des activités pour le compte de l'organisation, le management ne peut pas se décharger de sa responsabilité quant à la gestion des risques y afférents et doit donc instaurer un programme de pilotage des activités externalisées. Voir le chapitre 5, *Les processus et les risques*, qui traite plus en détail des enjeux liés à l'externalisation des processus opérationnels.

Les dispositifs formels de management des risques de l'entreprise ne font pas encore partie des pratiques de la plupart des organisations, mais ces dernières ont de plus en plus tendance soit à se doter d'un tel dispositif, soit au moins à en appliquer les grands principes. Le COSO énumère les avantages potentiels d'un tel dispositif de management des risques :

- aligner la stratégie de l'organisation avec son appétence pour le risque ;
- renforcer les modes de traitement du risque ;
- diminuer les incidents et les pertes opérationnelles ;
- identifier et gérer les risques transverses ;
- traiter, de manière intégrée, les risques multiples ;
- saisir les opportunités ;
- améliorer l'utilisation du capital.[23]

Copyright © 2015 Eyrolles.

Risque (définition de la norme ISO 31000)

Effet de l'incertitude sur les objectifs.

NORME ISO 31000:2009, MANAGEMENT DU RISQUE – PRINCIPES ET LIGNES DIRECTRICES

En 2009, l'Organisation internationale de normalisation a publié la norme ISO 31000:2009 (la « norme ISO 31000 »), la première norme relative à la gestion des risques reconnue à l'échelle mondiale. Cette norme a été élaborée afin de proposer une approche de la gestion des risques universellement acceptée, qui tienne compte de principes, de cadres de référence, de modèles et de pratiques qui évoluent à travers le monde. Elle comprend trois sections : des principes, un cadre organisationnel et un processus. Chacune de ces sections est décrite ci-après.

Principes de la norme ISO 31000

La norme ISO 31000 fournit 11 principes que l'Organisation internationale de normalisation juge nécessaires pour mettre en œuvre un management du risque efficace. Selon ces principes, le management du risque :

- crée de la valeur et la préserve ;
- fait partie intégrante des processus organisationnels ;
- est un élément de la prise de décision ;
- traite explicitement de l'incertitude ;
- est systématique, structuré et en temps utile ;
- s'appuie sur la meilleure information disponible ;
- est adapté ;
- tient compte des facteurs humains et culturels ;
- est transparent et participatif ;
- est dynamique, itératif et réactif au changement ;
- facilite l'amélioration continue de l'organisation.[24]

La non-conformité à l'un de ces principes complique la mise en œuvre d'un management du risque efficace et durable et, par conséquent, la réalisation des objectifs.

Cadre organisationnel de la norme ISO 31000

Selon l'Organisation internationale de normalisation, le succès du management du risque dépend de la mise en place d'un cadre organisationnel qui sert de base au processus dans l'ensemble de l'organisation. Les éléments de ce cadre sont les suivants.

Mandat et engagement

Attentes envers le Conseil et la direction générale afin de garantir l'alignement avec les objectifs de l'organisation et l'engagement des ressources suffisantes pour contribuer à la réalisation de ces objectifs.

- **Mandat et engagement** du Conseil et de la direction générale afin de garantir l'alignement avec les objectifs de l'organisation

Copyright © 2015 Eyrolles.

et l'engagement des ressources suffisantes pour contribuer à la réalisation de ces objectifs.

- **Conception du cadre organisationnel de management du risque**, afin de s'assurer que la base établie est propice à l'efficacité des processus de management du risque. Ceci implique de prendre les mesures suivantes :
  - comprendre l'organisation et son environnement ;
  - définir une politique de management du risque ;
  - déléguer les pouvoirs et le devoir de rendre compte ;
  - intégrer le management du risque aux processus organisationnels ;
  - allouer les ressources nécessaires ;
  - mettre en place des mécanismes de reporting et de communication internes et externes.
- **Mise en œuvre du processus et du cadre organisationnel de management du risque**, afin d'aider l'organisation à atteindre ses objectifs.
- **Surveillance du cadre organisationnel**, afin d'évaluer son efficacité en permanence.
- **Amélioration continue du cadre organisationnel**, afin de garantir sa pérennité.[25]

Si les éléments spécifiques du cadre organisationnel de management du risque peuvent être adaptés en fonction des besoins de l'organisation, le manque de structure peut néanmoins entraîner une baisse d'efficacité et d'efficience du management du risque.

Processus de la norme ISO 31000

Enfin, il est nécessaire de mettre en place, dans l'ensemble de l'organisation, un processus qui permette au management du risque de fonctionner de manière cohérente. Le processus de management du risque établi par la norme ISO 31000 comprend les activités suivantes.

- **L'établissement du contexte**, qui consiste à comprendre et à accepter les facteurs tant internes qu'externes qui influeront sur le management du risque. Cette activité intègre également la définition des critères de risque qui correspondent aux « termes de référence vis-à-vis desquels l'importance d'un risque est évaluée »[26]. Ces termes peuvent inclure l'appétence pour le risque de l'organisation, les seuils de tolérance au risque et les critères au regard desquels un risque peut être évalué (comme l'impact et la probabilité).
- **L'appréciation du risque**, qui consiste à identifier les risques, à les analyser en tenant compte de leurs causes, leurs origines et leurs conséquences, et à les évaluer afin de déterminer lesquels devraient être traités en premier.

Copyright © 2015 Eyrolles.

- **Le traitement des risques**, qui consiste à prendre des décisions similaires à celles du COSO présentées précédemment dans ce chapitre.
- **La surveillance du risque**, afin d'identifier la survenue d'un événement comportant un risque et de déterminer si les modalités de traitement des risques ont les effets escomptés. En ce sens, il est également important de s'assurer que les activités de management du risque sont correctement enregistrées pour faciliter cette surveillance.
- **L'établissement d'un processus de communication et de concertation**, afin de s'assurer que l'information circule de manière ascendante, descendante et transversale au sein de l'organisation et contribue ainsi au processus de management du risque.[27]

Contrôle à l'échelle de l'entité

Contrôle au niveau de toute une entité et qui, par conséquent, n'est ni lié ni associé à un processus en particulier.

Le processus de management du risque fonctionne en continu et est intégré dans l'ensemble des activités de prise de décision. Un processus efficace contribuera à assurer le succès permanent du management du risque.

Autres référentiels

Bien que le dispositif de management des risques du COSO soit largement reconnu aux États-Unis, de même que la norme ISO 31000 au niveau international, certains pays ont élaboré leur propre cadre de référence en matière de gestion des risques. La situation des organisations et les initiatives de réglementation ont débouché sur divers codes et réglementations visant à répondre aux besoins locaux des marchés financiers et des organisations. Si la plupart de ces référentiels sont fondamentalement analogues à celui du COSO et à la norme ISO 31000, chacun présente néanmoins des spécificités, que le lecteur est invité à étudier. Selon les cultures et les organisations, certains de ces référentiels pourront s'avérer plus adaptés.

Une vision descendante du risque

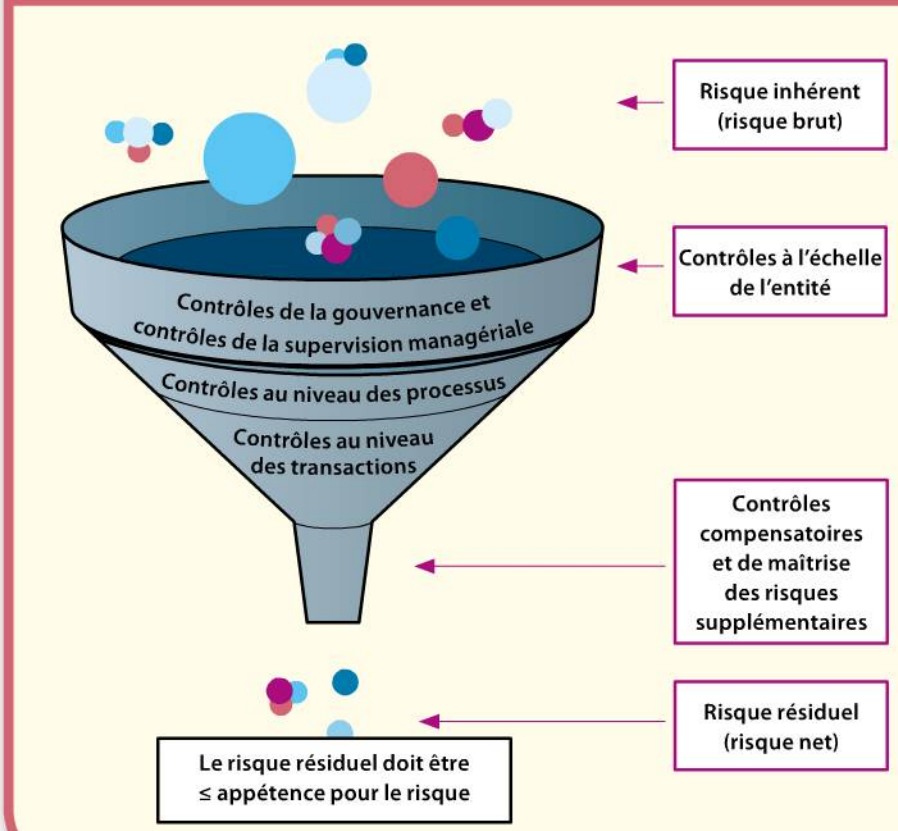
L'encadré 4-3 résume le rôle du management des risques de l'entreprise. Il recourt à la métaphore de l'entonnoir pour décrire le rôle descendant que joue le management des risques de l'entreprise afin d'aider l'organisation à ramener ses principaux risques à un niveau acceptable. Les grands points à comprendre dans ce graphique sont traités plus en détail dans l'étude de cas. Nous présentons ci-après les éléments clés.

- Chaque organisation doit faire face à des risques divers, suivant sa stratégie et ses objectifs. Certains de ces objectifs peuvent décrire la situation-cible opérationnelle résultant d'un système de contrôle interne efficace.

Copyright © 2015 Eyrolles.

ENCADRÉ 4-3

LE MANAGEMENT DES RISQUES DE L'ENTREPRISE : UN PROCESSUS DESCENDANT



- L'encadré 4-3 représente les risques qui compromettent la capacité de l'organisation à réaliser ses objectifs sous la forme de balles colorées de tailles différentes, ce qui signifie que certains risques auront plus d'impact que d'autres. De plus, certains risques sont concentrés dans une zone donnée, ce qui illustre le fait qu'un risque considéré isolément peut ne pas être grave. Cependant, la conjonction de plusieurs risques suite à un événement donné peut considérablement aggraver l'impact. Au départ, il n'existe aucun contrôle sur ces risques, qui sont dans leur état premier, ou brut.
- Le système de contrôle interne est représenté sous la forme d'un entonnoir, qui illustre le « filtrage » des principaux risques opérés à divers niveaux du système. Les risques les plus importants doivent faire l'objet de contrôles à l'échelle de l'entité, au sommet de l'entonnoir. Ceux qui passent à travers ce filtre sont ensuite soumis à des contrôles au niveau des processus et des transactions. Comme l'indique le chapitre 6, *Le contrôle interne*, les contrôles peuvent être considérés comme essentiels ou secondaires, selon qu'ils réduisent le risque associé à des objectifs critiques ou non. Dans certains cas, le management peut, en outre, recourir à des contrôles compensatoires et de maîtrise

Contrôle compensatoire

Activité qui, si les contrôles clés ne fonctionnent pas de manière effective, peut contribuer à réduire le risque considéré. Un contrôle compensatoire ne peut pas, en tant que tel, ramener le risque à un niveau acceptable.

Copyright © 2015 Eyrolles.

des risques supplémentaires afin de limiter davantage l'impact des risques.

- Si le système de contrôle interne est conçu de manière adéquate et fonctionne de manière effective, les risques qui se situent au bas de l'entonnoir devraient être d'un niveau acceptable pour l'organisation. Autrement dit, le risque résiduel, ou risque net, ne doit pas excéder l'appétence pour le risque de l'organisation.

LE RÔLE DE L'AUDIT INTERNE DANS LE MANAGEMENT DES RISQUES DE L'ENTREPRISE

La Norme 2120, Management des risques, précise que « l'audit interne doit évaluer l'efficacité des processus de management des risques et contribuer à leur amélioration »[28]. Grâce à leur éventail de compétences et à leur expérience, les auditeurs internes sont bien placés pour jouer un rôle précieux dans le management des risques de l'entreprise. En fait, étant donné la large portée de la plupart des fonctions d'audit interne, ainsi que leur rôle dans le processus global de pilotage, ne pas associer la fonction d'audit interne au management des risques de l'entreprise reviendrait à en compromettre la réussite. La discussion ci-après s'attache au rôle que l'audit interne peut jouer dans un tel dispositif, selon que l'organisation dispose ou non d'une fonction spécifique dédiée au management des risques de l'entreprise.

Organisations dotées d'un dispositif de management des risques

Le Cadre de référence international des pratiques professionnelles de l'audit interne comprend une prise de position intitulée, *Le rôle de l'audit interne dans le management des risques de l'entreprise*, qui expose les différentes possibilités d'action pour les auditeurs internes dans ce domaine. Dans son résumé, ce document précise : « Concernant le management des risques de l'entreprise, le rôle essentiel de l'audit interne consiste à apporter au Conseil une assurance objective quant à l'efficacité de cette activité, afin que les principaux risques de l'entreprise soient gérés correctement et que le système de contrôle interne fonctionne bien »[29].

Cette prise de position est présentée dans un diagramme en éventail qui précise les différents rôles que l'audit interne doit ou ne doit pas jouer (encadré 4-4). Voici les catégories qui sont évoquées :

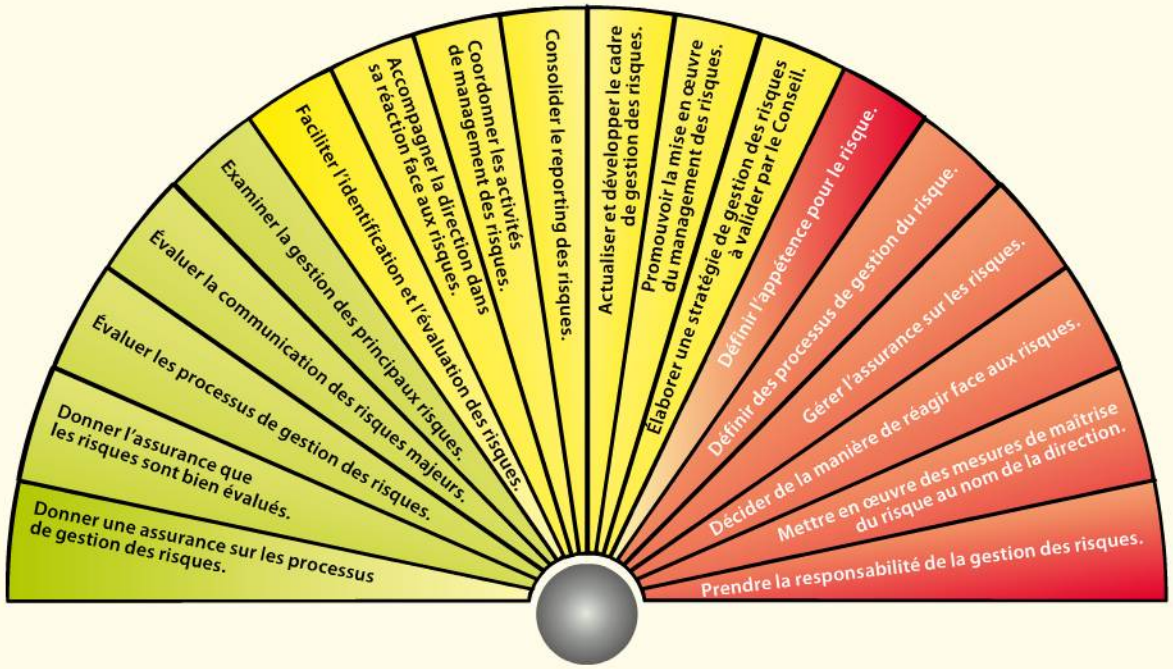
Principaux rôles de l'audit interne. Ces rôles, qui se situent à gauche de l'éventail, dans la section verte présentée dans l'encadré 4-4, correspondent aux activités d'assurance. Ils s'inscrivent

Activités de conseil

Conseils et services y afférents rendus au client donneur d'ordre, dont la nature et le champ sont convenus au préalable avec lui. Ces activités ont pour objectif d'améliorer les processus de gouvernement d'entreprise, de management des risques et de contrôle d'une organisation sans que l'auditeur interne n'assume aucune responsabilité de management.

Copyright © 2015 Eyrolles.

LE RÔLE DE L'AUDIT INTERNE DANS LE MANAGEMENT DES RISQUES DE L'ENTREPRISE



Ce diagramme est extrait de la prise de position intitulée « Le rôle de l'audit interne dans le management des risques de l'entreprise », traduite par l'IFACI, et reproduit avec l'autorisation de l'*Institute of Internal Auditors – United Kingdom and Ireland*. Pour consulter l'intégralité du texte de cette prise de position en anglais, vous pouvez consulter le site www.iia.org.uk. © *The Institute of Internal Auditors – UK and Ireland Ltd.*, juillet 2004.

ENCADRÉ 4-4

dans l'objectif plus large de donner une assurance sur les activités de gestion des risques. Ces activités sont les suivantes :

- donner une assurance sur les processus de gestion des risques ;
- donner l'assurance que les risques sont bien évalués ;
- évaluer les processus de gestion des risques ;
- évaluer la communication des risques majeurs ;
- examiner la gestion des principaux risques.[30]

Rôles légitimes de l'audit interne, sous réserve de prendre les précautions nécessaires. L'audit interne peut réaliser des activités de conseil qui améliorent les processus de gouvernance, de gestion des risques et de contrôle de l'organisation. L'étendue de l'activité de conseil de l'audit interne dans le cadre du dispositif de management des risques dépendra des autres ressources, internes

Copyright © 2015 Eyrolles.

et externes, dont dispose le Conseil et de la maturité de l'organisation sur la question du risque. Ces rôles de conseil sont énumérés dans la section jaune au centre de l'éventail de l'encadré 4-4. De manière générale, plus l'auditeur s'aventure vers la droite, plus il doit prendre des précautions pour préserver son indépendance et son objectivité. Ces activités sont les suivantes :

- faciliter l'identification et l'évaluation des risques ;
- accompagner la direction dans sa réaction face aux risques ;
- coordonner les activités de management des risques ;
- consolider le reporting des risques ;
- actualiser et développer le cadre de gestion des risques ;
- promouvoir la mise en œuvre du management des risques ;
- élaborer une stratégie de gestion des risques à valider par le Conseil.[31]

Rôles que l'audit interne ne doit pas jouer. L'audit interne ne doit pas assumer les rôles présentés dans la section rouge, dans la partie droite de l'éventail de l'encadré 4-4, car ils relèvent de la responsabilité du management et compromettraient l'indépendance et l'objectivité des auditeurs internes. Ces activités sont les suivantes :

- définir l'appétence pour le risque ;
- définir des processus de gestion des risques ;
- gérer l'assurance sur les risques [autrement dit, constituer la seule source d'assurance pour le management que les risques sont correctement gérés, ce qui reviendrait à exécuter une fonction de gestion] ;
- décider de la manière de réagir face aux risques ;
- mettre en œuvre des mesures de maîtrise du risque au nom de la direction ;
- prendre la responsabilité de la gestion des risques.[32]

Lors de la définition du rôle de l'audit interne dans le processus de management des risques de l'entreprise, le responsable de l'audit interne doit principalement se demander si l'activité constitue une menace pour l'indépendance et l'objectivité des auditeurs internes. Il importe que l'organisation comprenne bien que le management reste pleinement responsable de la gestion des risques. Plus l'audit interne étend son rôle vers la droite de l'éventail, plus il convient de prendre les précautions suivantes :

- il doit être clair que la direction demeure responsable de la gestion des risques ;
- la nature des responsabilités de l'audit interne doit être consignée dans la charte d'audit et validée par le Comité d'audit ;

Copyright © 2015 Eyrolles.

- l'audit interne ne doit pas gérer de risque au nom de la direction ;
- l'audit interne doit formuler des conseils, contester ou au contraire appuyer les décisions du management, mais en aucun cas prendre lui-même des décisions concernant la gestion des risques ;
- l'audit interne ne peut pas donner d'assurance objective quant à tout volet du cadre de référence de gestion des risques dont il est responsable. Ce sont d'autres parties qualifiées [internes ou externes à l'organisation] qui devront donner une telle assurance ;
- toute tâche sortant du cadre des activités d'assurance doit être considérée comme une mission de conseil, qui donne lieu au respect des normes régissant ce type de missions.[33]

Organisations dotées d'un dispositif de management des risques piloté par l'audit

La Modalité Pratique d'Application 2120-1, Évaluer la pertinence des processus de management des risques, indique que « le management et le Conseil sont responsables des processus de management des risques et de contrôle de leur organisation. Toutefois, les auditeurs internes peuvent, dans le cadre d'une mission de conseil, aider l'organisation à identifier, à évaluer et à mettre en place des méthodes de management des risques et des contrôles permettant de maîtriser ces risques »[34]. Lorsqu'une organisation ne s'est pas dotée d'un processus de management des risques, cette Modalité Pratique d'Application recommande la démarche suivante :

« Dans l'hypothèse où l'organisation n'a pas mis en place de processus de management des risques, le responsable de l'audit interne examine formellement avec la direction générale et le comité d'audit : leurs responsabilités en matière de compréhension, de gestion et de surveillance des risques dans l'organisation ; leur besoin d'informations sur le caractère opérationnel des processus (y compris les processus informels) qui donnent une visibilité appropriée des risques majeurs, de leur gestion et de leur surveillance.

Le responsable de l'audit interne recueille les attentes de la direction générale et du Conseil en ce qui concerne le rôle de l'audit interne dans le processus de management des risques de l'organisation. Ce rôle est précisé dans la charte d'audit interne ainsi que dans la charte du Conseil. Les responsabilités de l'audit interne doivent être coordonnées avec tous les groupes ou les personnes qui interviennent dans le processus de management des risques de l'organisation. Le rôle de l'audit interne dans le processus de management des risques d'une organisation peut évoluer dans le temps et revêtir les formes suivantes :

- aucune intervention ;
- audit de processus de management des risques dans le cadre du programme d'audit interne ;

Atteintes à l'indépendance ou à l'objectivité

Survenue de menaces risquant de limiter de manière significative, dans les faits ou en apparence, la capacité de l'auditeur interne à mener une mission sans parti pris ni entrave.

Copyright © 2015 Eyrolles.

- soutien actif et continu, et participation au processus de management des risques, notamment dans le cadre de comités de surveillance, d'activités de suivi et de rapports officiels ;
- gestion et coordination du processus de management des risques.

En définitive, il incombe à la direction générale et au Conseil de déterminer le rôle de l'audit interne dans le processus de management des risques. Leur vision dans ce domaine dépendra de facteurs tels que la culture de l'organisation, la compétence de l'équipe d'audit interne, les us et coutumes du pays. Cependant, la responsabilité dans le processus de gestion des risques, son impact potentiel sur l'indépendance de l'audit interne nécessitent une discussion approfondie et une approbation de la part du Conseil. »[35]

Ces orientations mettent en évidence la nécessité de porter à la connaissance du management l'absence de gestion des risques, et de formuler des suggestions en vue de la mise en place d'un tel processus. Les auditeurs internes peuvent, s'ils y sont invités, jouer un rôle proactif en participant à la mise en place initiale d'un processus de gestion des risques au sein de l'organisation. Outre leur mission classique d'assurance, ils assument alors un rôle de conseil en vue de l'amélioration des processus fondamentaux. Si cette assistance dépasse le cadre des missions d'assurance et de conseil généralement confiées aux auditeurs internes, l'indépendance des auditeurs peut être altérée. Dans ce cas, ils doivent respecter l'obligation d'information prévue par les *Normes*.

Univers d'audit

Ensemble des filiales, unités opérationnelles, services, groupes, processus ou autres subdivisions en place dans une organisation qui gèrent un ou plusieurs risques opérationnels.

IMPACT DU MANAGEMENT DES RISQUES DE L'ENTREPRISE SUR L'ASSURANCE APPORTÉE PAR L'AUDIT INTERNE

Selon la Norme 2010 de l'IIA, Planification, « le responsable de l'audit interne doit établir un plan d'audit fondé sur les risques afin de définir des priorités cohérentes avec les objectifs de l'organisation »[36]. Venant appuyer cette norme, la Modalité Pratique d'Application 2010-1, La prise en compte des risques et des menaces pour l'élaboration du plan d'audit, apporte des orientations aux responsables de l'audit interne qui élaborent le plan d'audit interne annuel. Cette Modalité Pratique d'Application formule les recommandations suivantes pour la prise en compte des risques et des menaces dans la planification :

- « en élaborant le plan d'audit, la plupart des responsables de l'audit interne choisissent d'abord de développer ou d'actualiser l'univers d'audit. […] Le responsable de l'audit interne peut recueillir la contribution de la direction générale et du Conseil pour constituer l'univers d'audit ;
- l'univers d'audit peut intégrer certaines composantes du plan stratégique de l'organisation, de façon à tenir compte de ses objectifs globaux. Par ailleurs, selon toute vraisemblance, les

Copyright © 2015 Eyrolles.

plans stratégiques reflètent l'attitude de l'organisation face aux risques et le degré de difficulté que comporte la réalisation des objectifs fixés. L'univers d'audit prend généralement en compte les résultats du processus de management des risques. En principe, le plan stratégique de l'organisation tient compte de l'environnement dans lequel elle opère. Les facteurs liés à cet environnement influeront vraisemblablement sur l'univers d'audit et l'évaluation des risques ;

- le responsable de l'audit interne prépare le plan d'audit à partir de l'univers d'audit, des contributions de la direction générale et du Conseil, d'une évaluation des risques et des menaces [...] ainsi que des informations, notamment en ce qui concerne l'évaluation de l'efficacité de la gestion des risques par le management [à destination de la direction générale et du Conseil], afin de les aider à atteindre les objectifs de l'organisation ;
- l'univers et la planification d'audit sont actualisés afin d'intégrer tout type de changement ;
- le plan des missions d'audit est établi, entre autres, sur la base d'une évaluation des principaux risques et menaces [...]. Le responsable de l'audit interne a, à sa disposition, divers modèles de risques [...]. La plupart de ces modèles utilisent des facteurs de risque tels que l'impact, la probabilité d'occurrence, la matérialité, la liquidité des actifs, la compétence du management, la qualité et le respect des contrôles internes, le niveau de changement ou de stabilité, la date et les résultats de la dernière mission d'audit, la complexité, les relations avec le personnel et l'administration, etc. »[37]

  Les points énumérés ci-dessus, qui s'appliquent à l'élaboration du plan d'audit interne annuel, s'appliquent également dans le cadre d'une mission d'audit. Ainsi, le périmètre et l'approche de chaque mission seront influencés par :

- la façon dont les risques attachés aux différents processus sont liés aux plans et aux objectifs stratégiques de l'organisation. Les risques de niveau processus sont traités plus en détail au chapitre 13, *Le déroulement de la mission d'assurance* ;
- les changements apportés aux processus (objectifs, procédures, collaborateurs et mesure des performances, par exemple) au cours de l'année passée ou depuis le dernier audit du processus concerné ;
- les facteurs liés aux modèles de risques pertinents (par exemple l'impact financier et la liquidité des actifs) ;
- l'impact et la probabilité d'occurrence des risques attachés aux différents processus.

En résumé, le fait que le management ait doté l'organisation d'un dispositif de management des risques influe de manière significative sur le contenu de la charte d'audit interne et le plan d'audit annuel.

Copyright © 2015 Eyrolles.

OPPORTUNITÉS POUR UN POINT DE VUE DE L'AUDIT INTERNE

L'audit interne peut contribuer à créer de la valeur ajoutée en apportant son point de vue sur le dispositif de gestion des risques. L'encadré 4-5 présente 10 opportunités pour l'audit interne d'apporter son point de vue à différents niveaux du processus de gestion des risques.

ENCADRÉ 4-5

APPORTER SON POINT DE VUE SUR LA GESTION DES RISQUES
10 OPPORTUNITÉS POUR L'AUDIT INTERNE

- Déterminer si les objectifs de l'organisation, qui constituent le point de départ de la gestion des risques, sont clairement définis et suffisamment compris dans l'ensemble de l'organisation.
- Apporter un point de vue sur la nature et l'efficacité de l'environnement de contrôle afin de donner une assurance à la direction générale et au Conseil quant à l'absence de facteurs, répandus à l'échelle de l'entité, susceptibles de compromettre l'efficacité de la gestion des risques.
- Faciliter la détermination de l'appétence pour le risque et des seuils de tolérance au risque de l'organisation afin de s'assurer que ces critères sont définis, approuvés par le Conseil et compris dans l'ensemble de l'organisation.
- Identifier les événements susceptibles de comporter des risques et compléter la liste établie par le management.
- Faciliter l'évaluation et la hiérarchisation des risques afin d'aider le management à s'assurer que les risques appropriés sont traités.
- Apporter des conseils sur les critères d'évaluation des risques autres que l'impact et la probabilité, à savoir la vitesse et la volatilité, qui peuvent influencer la hiérarchisation des risques.
- Apporter des conseils sur le choix des modalités de traitement des risques afin d'aider le management à déterminer si les solutions choisies permettront d'optimiser la gestion des risques prioritaires.
- Aider le management à surveiller les environnements interne et externe afin d'identifier les risques nouveaux ou émergents.
- Présenter les constats d'audit sous une forme qui permette au management de comprendre l'adéquation de la conception et le fonctionnement effectif des activités de gestion des risques.
- Réaliser une évaluation globale du système de gestion des risques (référentiel et processus) afin de donner une assurance quant à l'adéquation de sa conception et à son fonctionnement effectif.

RÉSUMÉ

Selon la définition du COSO, « le management des risques est un processus mis en œuvre par le Conseil d'administration, la direction générale, le management et l'ensemble des collaborateurs de l'organisation. […] Il est conçu pour identifier les événements potentiels susceptibles d'affecter l'organisation et pour gérer les risques dans les limites de son appétence pour le risque »[38].

Copyright © 2015 Eyrolles.

Les objectifs de l'organisation peuvent être liés à la stratégie, aux opérations, au reporting ou à la conformité. Le management des risques de l'entreprise peut être évalué sur la base de plusieurs éléments : environnement interne, fixation des objectifs, identification des événements, évaluation des risques, traitement des risques, activités de contrôle, information et communication, et pilotage.

La norme ISO 31000 donne une vue d'ensemble de la gestion des risques, qui comprend des principes, un cadre organisationnel et un processus de gestion des risques. Elle est de plus en plus reconnue sur le plan mondial et est, en règle générale, cohérente avec le dispositif de management des risques du COSO.

Grâce à leur éventail de compétences et à leur expérience, les auditeurs internes sont bien placés pour jouer un rôle précieux dans le management des risques de l'entreprise. La fonction d'audit interne peut assumer divers rôles dans le cadre de ce dispositif, dont certains correspondent aux activités d'assurance définies dans la charte, et d'autres peuvent être des activités de conseil visant à aider l'organisation à améliorer ses processus de gouvernance, de gestion des risques et de contrôle. Toutefois, l'audit interne doit mettre en place des mesures de précaution appropriées afin d'éviter d'accepter des rôles qui reviendraient à assumer des responsabilités de management, ce qui compromettrait l'objectivité et l'indépendance des auditeurs internes.

Le plan stratégique et les risques inhérents à l'organisation ont un impact direct et conséquent sur la charte d'une fonction d'audit interne, ainsi que sur le plan d'audit annuel. Les changements apportés aux orientations, aux objectifs, aux priorités et aux centres d'intérêts du management peuvent aussi influer sur ce plan d'audit. Le responsable de l'audit interne doit tenir compte des risques lorsqu'il établit ses priorités et planifie les missions d'audit à venir.

Copyright © 2015 Eyrolles.



Questions de révision

1. Quelle est la définition du risque donnée par le COSO ? Comment l'ISO définit-elle le risque ?

2. Quels sont les quatre points fondamentaux de la définition du risque donnée par le COSO et l'ISO ?

3. Quels sont les concepts fondamentaux de la définition du management des risques de l'entreprise établie par le COSO ?

4. Quelles sont les quatre catégories d'objectifs du cadre de référence relatif management des risques de l'entreprise élaboré par le COSO ? Décrivez-les.

5. Quels sont les huit éléments du cadre de référence relatif au management des risques de l'entreprise élaboré par le COSO ?

6. Quelles sont les quatre catégories de traitement des risques définies par le COSO ?

7. Citez quelques exemples d'activités de contrôle courantes.

8. Que regroupent les activités courantes de pilotage ? Que sont les évaluations spécifiques ?

9. Quels sont les 11 principes de la gestion des risques définis par la norme ISO 31000 ?

10. Quels sont les cinq éléments du cadre organisationnel de management du risque établi par la norme ISO 31000 ?

11. Quelles sont les cinq activités incluses dans le processus de gestion des risques de la norme ISO 31000 ?

12. Quelles sont les responsabilités habituelles des personnes suivantes en matière de management des risques de l'entreprise :
    a. le Conseil ?
    b. la direction générale ?
    c. le directeur des risques ?
    d. la direction financière ?
    e. les auditeurs internes ?
    f. les auditeurs externes ?

Copyright © 2015 Eyrolles.

Questions de révision

13. À l'encadré 4-3, pourquoi certaines des petites boules représentant des risques sont-elles concentrées alors que d'autres ne le sont pas ?

14. Citez quelques exemples d'activités d'assurance que l'audit interne peut réaliser dans le cadre du management des risques de l'entreprise. Citez quelques exemples d'activités de conseil que l'audit interne peut réaliser dans le cadre du management des risques de l'entreprise sous réserve que des mesures de précaution appropriées aient été mises en œuvre. Quelles sont les activités de management des risques de l'entreprise que l'audit interne ne devrait pas réaliser ?

15. Selon la Modalité Pratique d'Application 2010-1, La prise en compte des risques et des menaces pour l'élaboration du plan d'audit, comment le plan d'audit de la fonction d'audit interne doit-il être défini ?

Copyright © 2015 Eyrolles.

Questions à choix multiples

Sélectionnez la meilleure réponse pour chacune des questions suivantes.

1. Selon le dispositif de management des risques du COSO, tous les éléments suivants font partie de l'environnement interne d'une organisation sauf un, lequel ?
   a. Fixer les objectifs de l'organisation.
   b. Déterminer l'appétence pour le risque.
   c. Assigner des pouvoirs et des responsabilités.
   d. Faire siéger surtout des administrateurs indépendants au Conseil.

2. Parmi les événements extérieurs suivants, lequel aura le plus probablement un impact sur une entreprise de fabrication d'armement qui est tributaire des commandes importantes de l'État ?
   a. Un événement économique.
   b. Un événement dans l'environnement naturel.
   c. Un événement politique.
   d. Un événement social.

3. Parmi les éléments suivants, lequel ne constitue pas un exemple de stratégie de partage des risques ?
   a. Externaliser un domaine à haut risque non essentiel.
   b. Vendre une unité opérationnelle non stratégique.
   c. Se couvrir contre les fluctuations des taux d'intérêt.
   d. Souscrire une police d'assurance pour se protéger contre les aléas météorologiques.

4. Une organisation surveille un site Web qui accueille des blogs anonymes consacrés à son secteur. Récemment, des *posts* (messages) anonymes ont évoqué l'adoption éventuelle d'une législation susceptible d'avoir un effet considérable sur le secteur en question. Parmi les éléments suivants, lequel pourrait engendrer le risque le plus élevé si cette organisation prenait des décisions fondées sur les informations contenues sur ce site Web ?
   a. La pertinence de l'information.
   b. La disponibilité de l'information en temps utile.
   c. L'accessibilité de l'information.
   d. L'exactitude et la fiabilité de l'information.

5. Quelle réponse est placée dans le mauvais ordre dans le processus de gestion des risques ?
   a. Identifier, évaluer et hiérarchiser les risques.
   b. Déterminer des modalités de traitement des risques.

Copyright © 2015 Eyrolles.

c. Définir les principaux objectifs de l'organisation.
d. Surveiller l'efficacité des modalités de traitement des risques.

6. Qui est responsable de la mise en œuvre du dispositif de management des risques ?
   a. Le directeur financier.
   b. Le responsable de l'audit interne.
   c. Le responsable de la conformité.
   d. Le management dans toute l'organisation.

7. Parmi les éléments suivants, lequel ne constitue pas un avantage potentiel de la mise en œuvre d'un dispositif de management des risques ?
   a. L'amélioration des résultats financiers à court terme.
   b. La réduction des aléas d'une année sur l'autre.
   c. L'amélioration de la qualité de l'information disponible pour la prise de décision relative aux risques.
   d. L'alignement de l'appétence pour le risque de l'organisation sur la planification stratégique.

8. Parmi les propositions suivantes, laquelle constitue le meilleur argument pour inciter le responsable de l'audit interne à tenir compte du plan stratégique de l'organisation dans l'élaboration du plan d'audit interne annuel ?
   a. Insister sur l'importance de la fonction d'audit interne pour l'organisation.
   b. Veiller à ce que le plan d'audit interne soit validé par la direction générale.
   c. Formuler des recommandations visant à améliorer le plan stratégique.
   d. Veiller à ce que le plan d'audit interne favorise la réalisation des objectifs généraux de l'organisation.

9. Lorsque la direction générale accepte un niveau de risque résiduel que le responsable de l'audit interne juge inacceptable pour l'organisation, le responsable de l'audit interne doit :
   a. Faire immédiatement état du niveau de risque inacceptable au président du comité d'audit et au cabinet d'audit externe.
   b. Démissionner.
   c. En discuter avec les membres de la direction générale qui sont bien informés et, si la question n'est pas tranchée, la soumettre au comité d'audit.
   d. Accepter la position de la direction générale, car c'est elle qui définit l'appétence pour le risque de l'organisation.

Copyright © 2015 Eyrolles.

10. Dans le cadre de la mise en œuvre du dispositif de management des risques d'une organisation, on demande au responsable de l'audit interne de diriger l'évaluation des risques de l'organisation. Parmi les situations suivantes, laquelle ne serait pas pertinente pour protéger l'indépendance et l'objectivité de la fonction d'audit interne ?
    a. Une partie du management participe à l'évaluation de la probabilité et de l'impact de chaque risque.
    b. Les propriétaires de risques reçoivent une responsabilité pour chaque risque principal.
    c. Un membre de la direction générale présente les résultats de l'évaluation des risques au Conseil et précise qu'ils représentent le profil de risque de l'organisation.
    d. La fonction d'audit interne obtient l'aide d'un consultant externe pour mener à bien la session d'évaluation formelle des risques.

11. Une mission d'audit interne a été définie dans le cadre du plan d'audit interne annuel. D'après le modèle de risque de la fonction d'audit interne, cet audit est considéré comme étant à risque modéré. Le cycle d'audit en cours s'étend sur deux ans. Parmi les situations suivantes, laquelle aura certainement l'impact le plus fort sur la planification et la durée de cette mission d'audit interne ?
    a. Le domaine audité requiert le traitement d'un volume important de transactions.
    b. Certains éléments du processus sont externalisés.
    c. Un nouveau système a été mis en œuvre en cours d'année et a changé le mode de traitement des transactions.
    d. Les montants traités ne sont pas négligeables.

12. Une entreprise industrielle a identifié le risque suivant : « Les collaborateurs n'exécutent pas les procédures de contrôle qualité requises, ce qui peut se traduire par un niveau élevé de retours de la part des clients. » À quelle catégorie d'objectifs ce risque est-il le plus directement lié ?
    a. Objectifs liés à la stratégie.
    b. Objectifs liés aux opérations.
    c. Objectifs liés au reporting.
    d. Objectifs liés à la conformité.

13. Le risque qu'un nouveau concurrent réduise significativement la part de marché des produits d'une organisation est lié le plus directement à quelle catégorie d'objectifs ?
    a. Objectifs liés à la stratégie.
    b. Objectifs liés aux opérations.
    c. Objectifs liés au reporting.
    d. Objectifs liés à la conformité.

Copyright © 2015 Eyrolles.

Thèmes de discussion

1. Décrivez la différence entre la culture du risque, l'appétence pour le risque et la tolérance au risque en citant des exemples dans chaque cas.

2. Le dispositif de management des risques du COSO reconnaît quatre catégories d'objectifs (liés à la stratégie, aux opérations, au reporting et à la conformité). Si une organisation n'est pas capable de gérer efficacement les risques qui entourent l'une de ces catégories d'objectifs, pour quelle catégorie l'impact sur l'organisation serait-il le plus fort ?

3. Définissez le risque inhérent et le risque résiduel. De ces deux catégories de risques, laquelle devrait avoir l'impact le plus fort sur le plan annuel d'audit interne ?

4. Le cadre organisationnel de management du risque établi par la norme ISO 31000 comprend cinq éléments. Le premier est « mandat et engagement ». Expliquez de quoi il s'agit et indiquez en quoi cet élément est crucial pour garantir le succès de la gestion des risques.

5. Dans le cas d'une organisation qui ne s'est pas dotée d'un dispositif de management des risques, décrivez les mesures que peut prendre l'audit interne pour introduire un tel dispositif sans compromettre son indépendance et/ou son objectivité.

6. L'évaluation des risques s'attache le plus souvent à deux critères, l'impact et la probabilité. À mesure que le processus d'évaluation des risques d'une organisation progresse, quels autres critères serait-il utile de prendre en compte, et pourquoi ?

7. L'une de vos connaissances, étudiant à l'université, suit un double cursus pour obtenir deux diplômes. Il suit de nombreux cours. En plus de cet emploi du temps déjà chargé, il projette de poser sa candidature pour un stage en qualité d'auditeur interne dans une organisation locale. Décrivez les opportunités et les risques découlant de cette décision.

8. Souvenez-vous des cinq questions quotidiennes énumérées plus haut dans ce chapitre, qui peuvent s'appliquer à la philosophie de gestion des risques :
   a. Qu'essayons-nous d'accomplir (quels sont nos objectifs) ?
   b. Qu'est-ce qui pourrait nous empêcher de l'accomplir (quels sont les risques, quelle que soit leur gravité, et comment sont-ils susceptibles de se produire) ?
   c. Quelles options avons-nous pour que cela ne se produise pas (quelles sont les stratégies de gestion des risques, donc les modalités de traitement, disponibles) ?

Copyright © 2015 Eyrolles.



d. Sommes-nous en mesure de mettre en œuvre ces options (avons-nous élaboré et instauré des activités de contrôle permettant de déployer les stratégies de gestion des risques) ?

e. Comment saurons-nous que nous avons atteint nos objectifs (existe-t-il des informations qui permettront d'attester de la réussite et pouvons-nous suivre les performances de manière à vérifier que nous avons réussi) ?

Pensez aux raisons qui vous ont incité à étudier à partir du présent ouvrage et répondez à chacune de ces questions en pensant au niveau de réussite que vous souhaitez atteindre.

Copyright © 2015 Eyrolles.

ÉTUDES DE CAS

CAS N° 1

Le COSO énonce un ensemble d'orientations utiles pour les auditeurs internes. Cette étude de cas a pour objet de vous familiariser avec le COSO et ses orientations. Rendez-vous sur le site www.coso.org et répondez aux questions suivantes.

1. D'après la page d'accueil du COSO, quels sont les objectifs de cette organisation ?

2. Quelles sont les cinq organisations qui le composent ?

3. Quels types d'orientations sur le contrôle interne le COSO propose-t-il ? Une grande partie de ces orientations est décrite au chapitre 6, *Le contrôle interne*.

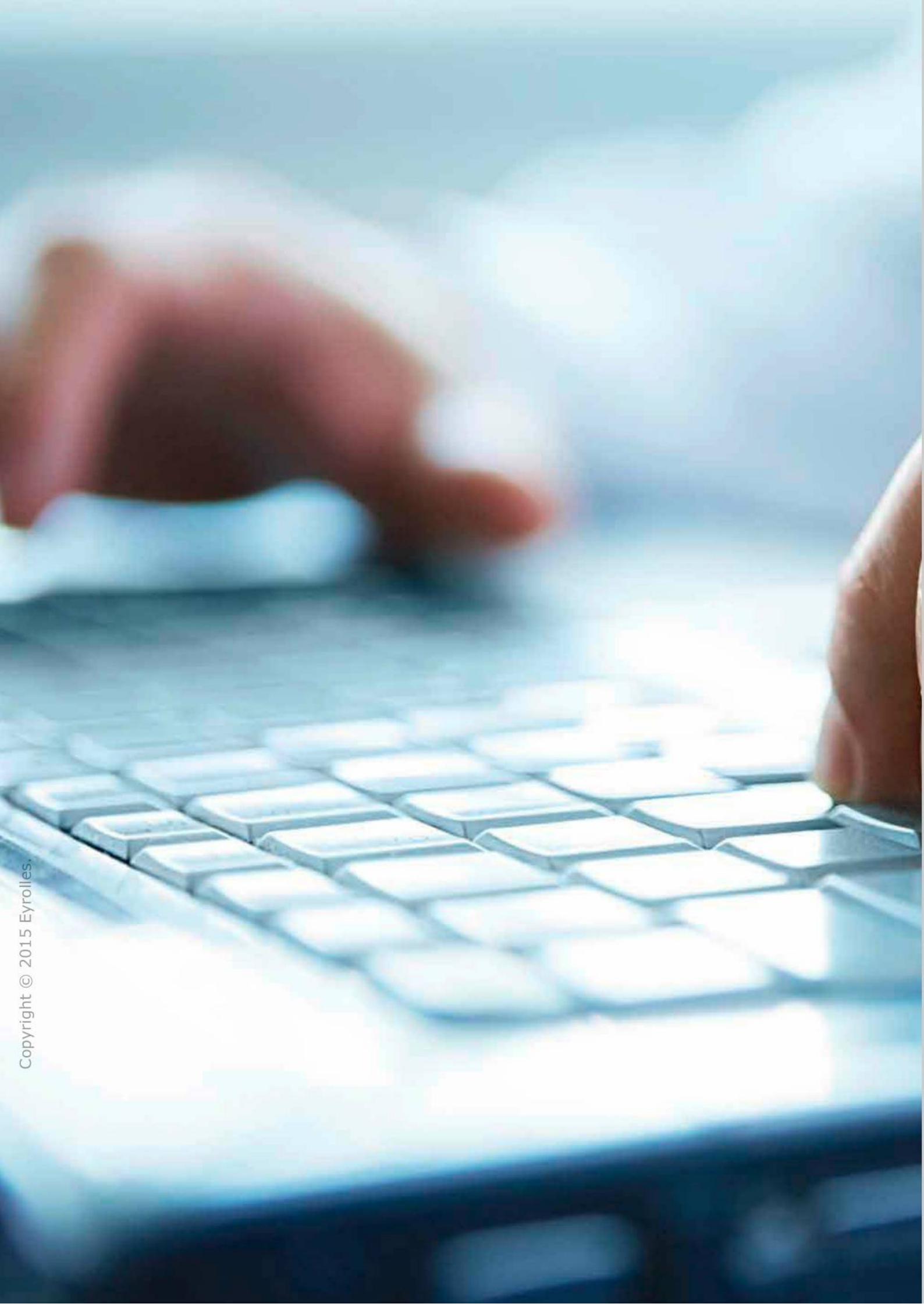
4. Téléchargez la synthèse du dispositif de management des risques du COSO (gratuitement). D'après la première page de ce résumé, qu'englobe le management des risques de l'entreprise ?

5. Téléchargez un article à partir de la page « Ressources » indiquée par votre enseignant. En quoi trouvez-vous cet article intéressant ?

CAS N° 2

Votre organisation a mis en place un programme de management des risques solide, analogue à celui décrit dans ce chapitre. Le comité d'audit vous demande d'évaluer l'adéquation de la conception et le fonctionnement effectif de ce programme. Les membres du comité connaissent bien le dispositif de management des risques du COSO et souhaiteraient que vous évaluiez ce programme au regard des huit éléments de ce dispositif. Pour répondre à cette demande, élaborez une liste d'étapes à suivre pour vérifier chaque élément du dispositif, avec au moins deux étapes de travail par élément.

Copyright © 2015 Eyrolles.



Copyright © 2015 Eyrolles.



CHAPITRE 5
LES PROCESSUS ET LES RISQUES

Objectifs pédagogiques

- Comprendre comment les organisations structurent leurs activités pour atteindre leurs objectifs.
- Identifier les processus opérationnels clés d'une organisation.
- Comprendre un processus opérationnel donné et savoir le documenter.
- Appréhender les risques opérationnels génériques auxquels sont confrontées les organisations.
- Identifier et évaluer les principaux risques pesant sur la réalisation des objectifs de l'organisation et leur relation avec les processus opérationnels.
- Élaborer un univers d'audit pour une organisation et définir un plan d'audit interne annuel reposant sur les principaux risques opérationnels.
- Comprendre comment utiliser les techniques d'évaluation des risques dans le cadre des missions d'assurance.
- Être sensibilisé aux nouveaux risques qui apparaissent lorsqu'une organisation externalise une partie de ses processus clés.

ENCADRÉ 5-1

DISPOSITIONS DU CRIPP PERTINENTES RELATIVES AU CHAPITRE 5

Norme 2010 – Planification.
Norme 2120 – Management des risques.
Norme 2200 – Planification de la mission.
Norme 2210 – Objectifs de la mission.
Modalité Pratique d'Application 2010-1 : La prise en compte des risques et des menaces pour l'élaboration du plan d'audit.
Modalité Pratique d'Application 2010-2 : Prise en compte du management des risques dans la planification de l'audit interne.
Modalité Pratique d'Application 2120-1 : Évaluer la pertinence des processus de management des risques.
Modalité Pratique d'Application 2200-1 : Planification de la mission.
Modalité Pratique d'Application 2200-2 : Utilisation d'une approche « *Top-Down* », fondée sur les risques, pour identifier les contrôles à évaluer dans le cadre d'une mission d'audit interne.
Modalité Pratique d'Application 2210-1 : Objectifs de la mission.
Modalité Pratique d'Application 2210.A1-1 : Évaluation des risques dans la planification de la mission.

Copyright © 2015 Eyrolles

Prenons un objectif simple : arriver à l'heure au cours de 8 h demain matin. Détaillons maintenant les étapes conduisant à cet objectif :

Vous pouvez :

- mettre dans votre sac les notes, les exercices et les livres dont vous aurez besoin demain, ainsi que votre téléphone portable et votre ordinateur portable ;
- mettre votre réveil à sonner pour 6 h, et aller vous coucher ;
- vous lever quand votre réveil sonne ;
- vous habiller et prendre votre petit déjeuner ;
- à 7 h, monter dans votre voiture et vous rendre à l'université ;
- chercher une place de stationnement ;
- marcher jusqu'au bâtiment ;
- prendre un café ;
- marcher jusqu'à la salle de cours et prendre place.

Processus opérationnel

Ensemble d'activités reliées entre elles qui ont pour but d'atteindre un ou plusieurs objectifs.

Voilà une liste de ce que vous devez faire pour atteindre votre objectif à savoir : « arriver à l'heure en cours ». Pour y parvenir, vous avez procédé à un certain nombre de choix, parmi différentes options que vous auriez pu prendre. Ainsi, vous auriez pu préparer votre sac le matin et non la veille ou décider de prendre le bus plutôt que la voiture. Pourquoi avez-vous fait ces choix-là ?

Dans certains cas, il peut s'agir de préférences personnelles. Ainsi, si vous faites votre sac la veille, vous pouvez dormir cinq minutes de plus le lendemain matin. Dans d'autres cas, votre choix peut avoir une incidence directe sur votre capacité à atteindre votre objectif. Ainsi, vous avez décidé de prendre la voiture plutôt que le bus parce que celui-ci est souvent en retard ou bondé et que vous risquez de devoir attendre le suivant. Dans ce dernier cas, vous tenez le type de raisonnement sur la gestion des risques décrit au chapitre 4, *La gestion des risques*.

Les organisations recourent au même type de processus de réflexion pour planifier les étapes qui les aideront à atteindre leurs objectifs, c'est-à-dire l'identification des risques potentiels pesant sur ces objectifs et le management de ces risques pour les ramener à des niveaux acceptables. Les auditeurs internes utilisent également les techniques et les méthodes d'évaluation des risques pour remplir leur mission.

LES PROCESSUS OPÉRATIONNELS

Le chapitre 3, *La gouvernance*, a traité de l'importance du processus de gouvernance dans la fixation des objectifs d'une organisation et les limites dans lesquelles elle doit s'opérer. Ce chapitre examine la façon dont les organisations structurent leurs activités pour mettre en œuvre leurs stratégies et atteindre leurs objectifs

Copyright © 2015 Eyrolles.

(organisationnels). Les activités sont structurées en processus opérationnels ou en projets. Bien qu'il existe des processus communs à toutes les organisations, leur combinaison et leur structure sont uniques à chacune. Au sein d'une même organisation, les processus peuvent différer fortement entre les secteurs d'activité.

Qu'est-ce qu'un processus opérationnel ? C'est simplement l'ensemble des activités reliées entre elles qui ont pour but d'atteindre un objectif. L'encadré 5-2 en présente une classification générique. Il existe trois types d'activités : les processus opérationnels, les processus de supervision et processus support, ainsi que les projets. Même si cet encadré les décrit comme des processus et des activités distincts et séparés, il faut noter qu'ils ne sont pas indépendants les uns des autres. Ainsi, l'activité « Élaborer la stratégie » (processus 2) est un élément de l'orientation stratégique de la gouvernance, illustrée dans l'encadré 3-3, davantage axé sur l'opérationnel. L'élaboration de cette stratégie opérationnelle peut se rapporter à plusieurs des autres activités présentées dans l'encadré 5-2. De plus, les processus de supervision et processus support facilitent et interagissent avec les processus et projets opérationnels.

Pour la plupart des organisations, les processus opérationnels incluent les processus clés grâce auxquels l'organisation atteint ses principaux objectifs. Pour une entreprise de production, il s'agira des processus par lesquels elle fabrique et vend des produits. Pour les prestataires de services, comme un cabinet de conseil ou un établissement financier, ce sera le processus par lequel ils commercialisent et fournissent leurs services. Les entités publiques, comme les pompiers ou les organisations à but non lucratif (les associations, par exemple), ont aussi des processus opérationnels par lesquels elles délivrent des services. Une fois le produit ou le service conçu (processus 1 à 3, dans l'encadré 5-2), les processus opérationnels restants (processus 4 à 6) sont considérés comme essentiellement continus ou répétés de nombreuses fois au cours d'un cycle d'activité. C'est à travers eux que les organisations créent de la valeur et en font bénéficier directement leurs consommateurs.

Certaines organisations procèdent différemment pour organiser les activités créatrices de valeur. La structuration en projets est utilisée lorsque les activités se déroulent sur une période longue, nécessitent un séquençage complexe et sont relativement uniques au sens où une activité spécifique n'est pas effectuée sur une base continue. Les bureaux d'études techniques et les entreprises de BTP, les sociétés minières, pétrolières et gazières, ainsi que les sous-traitants opérant dans le secteur de la défense sont des exemples d'organisations qui structurent souvent leurs activités clés de cette manière. Dans l'encadré 5-2, le processus 13 peut s'expliquer pour deux types de projets différents :

- lorsque l'organisation conçoit et construit un actif, mais aussi quand elle l'exploite, par exemple, une compagnie pétrolière qui fore puis exploite un puits de pétrole ;

Objectifs

Ce qu'une organisation souhaite réaliser. On parle alors des objectifs de l'organisation. Ces objectifs peuvent être liés à la stratégie, aux opérations, au reporting et à la conformité.

Copyright © 2015 Eyrolles.

- lorsque l'organisation conçoit et construit un actif, et qu'elle le transfère à une autre organisation qui l'exploitera (par exemple, un bureau d'études conçoit une usine ou un bâtiment puis le transfère à une autre organisation qui en assurera l'exploitation). Ces exemples concernent des actifs tangibles. La même approche vaut, néanmoins, pour les sociétés de prestation de services. Dans ce cas, l'« actif » peut être une propriété intellectuelle ou un autre actif immatériel.

Le mode « projet » est aussi souvent utilisé par la plupart des organisations pour organiser ainsi des activités non routinières afin de créer des actifs qu'elles utiliseront. Par exemple, une structure de projet servira à sélectionner et à mettre en œuvre un nouveau système comptable, à construire un nouveau site de production, ou encore à mettre en œuvre des initiatives majeures pour respecter les dispositions du *Sarbanes-Oxley Act* de 2002 (États-Unis) en matière de contrôle interne, la LSF de 2003 (France) ou les obligations de communication financière d'autres pays.

Les processus de supervision et processus support sont les activités qui supervisent et appuient les processus de création de valeur de l'organisation. Si ces processus varient d'une organisation à l'autre, ils sont généralement nécessaires dans tous les secteurs, mais ne créent pas directement la valeur intégrée dans les objectifs de l'organisation. Les processus de supervision et processus support incluent ceux servant à gérer les ressources humaines, financières, informationnelles et technologiques de l'organisation, mais aussi physiques (processus 7 à 10). Ils incluent l'embauche, la comptabilité, la gestion de la trésorerie, la paie, les achats, etc. Ces processus englobent également le programme de mise en conformité de l'organisation à la législation et à la réglementation (processus 11). Ils regroupent également les processus de gestion des relations externes (processus 12), par exemple avec les fournisseurs, les clients, les entités publiques et les autorités de régulation et de supervision, ainsi qu'avec les marchés financiers et les partenaires (organisations et alliances). Enfin, même si elles ne sont pas spécifiquement décrites dans cet encadré, les activités incluses dans la gouvernance peuvent également être considérées comme des processus support. Ces activités donnent l'orientation stratégique de l'organisation et permettent de la « surveiller », comme expliqué dans le chapitre 3. Les processus de gouvernance sont, par exemple, la planification stratégique, le programme de mise en conformité et de déontologie de l'organisation, les activités du Conseil et de ses comités, le programme de management des risques de l'entreprise, ainsi que diverses activités de surveillance et d'assurance.

L'encadré 5-2 illustre des processus opérationnels à un niveau d'agrégation élevé (ou synthétique). Chacun de ces 14 types de classification peut être décrit lui-même de manière plus détaillée. L'encadré 5-3 illustre ce point. Par exemple, une organisation de vente au détail peut décrire son « processus général de vente » au

Copyright © 2015 Eyrolles.

niveau le plus synthétique pour les processus 4, 5 et 6. Un type de vente spécifique pourrait être la « vente au détail », faisant appel à des processus détaillés par lesquels le consommateur sélectionne les produits, les paye en espèces ou au moyen d'une reconnaissance de dette et prend possession des produits. Dans la mesure où les ventes au détail peuvent être réalisées en magasin ou sur Internet, il est possible de concevoir des processus plus détaillés pour celles-ci. Le niveau de détail utilisé pour décrire ces processus variera selon le niveau de documentation souhaité. Si l'on souhaite une vue d'ensemble, la description générale présentée en haut de l'encadré 5-3 est suffisante. Si l'on désire un niveau plus détaillé, les exemples présentés au milieu ou en bas de l'encadré 5-3 seront plus appropriés. Dans certains cas, les sous-processus peuvent être présentés à des niveaux encore plus détaillés que ceux proposés à l'encadré 5-3. Par exemple, dans une « vente en magasin » qui consiste en la saisie d'informations dans la caisse enregistreuse, le processus peut faire intervenir un certain nombre de sous-processus, tels que la mise à jour de l'inventaire, l'enregistrement du produit de la vente et l'ouverture du tiroir-caisse. Les présentations générales, comme les présentations détaillées, peuvent être utiles à l'auditeur interne, comme l'explique la section suivante.

Comprendre les processus opérationnels

Stratégie

Manière dont la direction générale prévoit de réaliser les objectifs de l'organisation.

Approche descendante (*top-down*)

Approche qui commence au niveau de l'entité, avec les objectifs de l'organisation, et se poursuit par l'identification des principaux processus critiques pour atteindre chacun de ces objectifs.

Pour que les auditeurs internes créent de la valeur et améliorent les opérations d'une organisation, ils doivent d'abord comprendre le modèle économique de celle-ci. Ce modèle énonce les objectifs de l'organisation et la manière dont ses processus opérationnels sont structurés pour atteindre ces objectifs. Il se définit aussi par la vision, la mission et les valeurs de l'organisation, ainsi que par des ensembles de limites pour cette dernière : les produits ou services qu'elle va proposer, les consommateurs ou marchés qu'elle va cibler et les modes d'approvisionnement et de distribution qu'elle va utiliser. Le modèle économique inclut non seulement les stratégies et l'orientation tactique de la direction concernant le mode de mise en œuvre du modèle, mais également les objectifs annuels qui fixent les étapes spécifiques que l'organisation a l'intention d'appliquer l'année suivante ainsi que la mesure de leur réalisation attendue. Tous ces éléments peuvent faire partie de la documentation interne mise à disposition de l'auditeur interne.

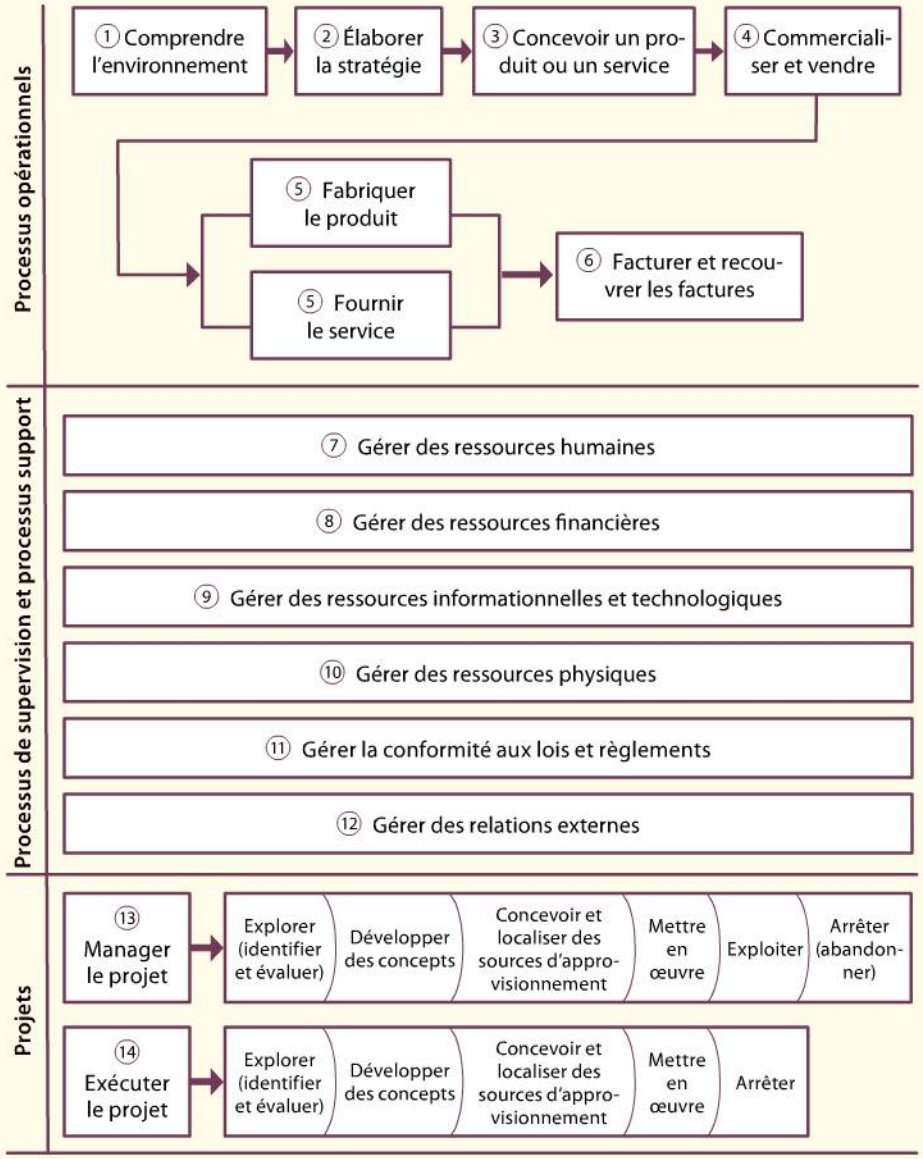
Pour les sociétés cotées, des sources d'information externes peuvent également être disponibles. Par exemple, les déclarations obligatoires, comme le dépôt des rapports 10-k auprès de la *Securities and Exchange Commission* (SEC) ou, en France, les documents de référence de l'AMF (Autorité des marchés financiers) donnent des informations sur les objectifs et les principaux risques. En outre, les rapports des analystes présentent un point de vue extérieur sur les stratégies de l'organisation. Si la vision, la mission, les valeurs et les

Copyright © 2015 Eyrolles.

objectifs d'une organisation sont relativement stables d'une année sur l'autre, la fonction d'audit interne doit tout de même périodiquement actualiser sa connaissance de la stratégie de l'organisation. En général, les auditeurs internes le font chaque année lorsqu'ils analysent les objectifs annuels de l'organisation et de la direction générale.

ENCADRÉ 5-2

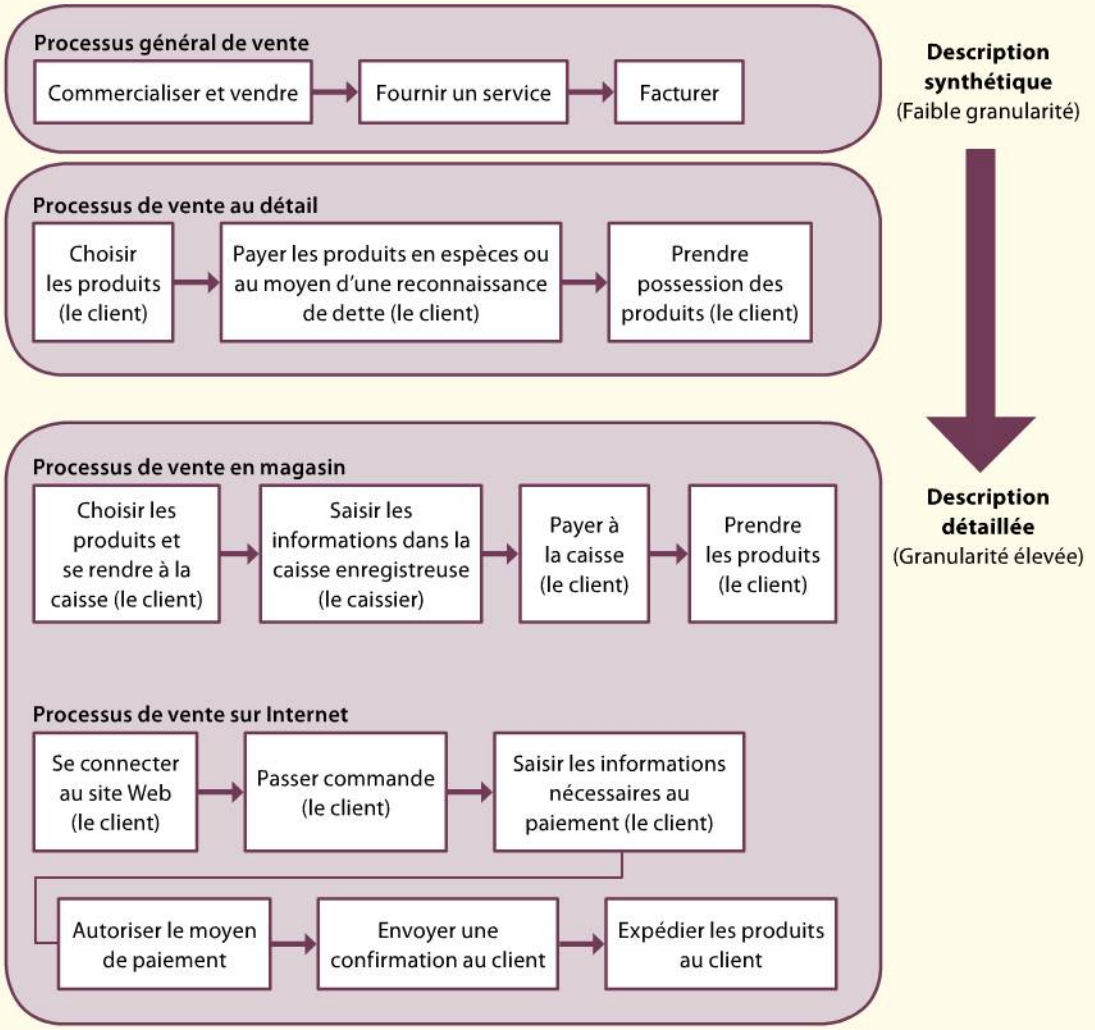
CLASSIFICATION GÉNÉRIQUE DES PRINCIPALES ACTIVITÉS D'UNE ORGANISATION



D'après Protiviti Inc., cabinet de conseil de référence en organisation, gestion des risques technologiques et audit interne (www.protiviti.com). Ce schéma de classification des processus est disponible sur KnowledgeLeader (www.knowledgeleader.com), un site Web sur abonnement qui propose des informations, des outils, des modèles et des ressources pour les professionnels de l'audit interne et de la gestion des risques.

Copyright © 2015 Eyrolles.

GRANULARITÉ DES PROCESSUS



ENCADRÉ 5-3

Deux approches courantes, l'une descendante et l'autre ascendante, permettent de comprendre les processus opérationnels et leur rôle dans le modèle économique. La première, l'approche descendante (*top-down*), commence au niveau de l'entité, avec les objectifs de l'organisation, et se poursuit par l'identification des principaux processus critiques pour atteindre chacun de ces objectifs. Un processus est considéré comme clé par rapport à un objectif spécifique si sa défaillance aura pour conséquence directe d'empêcher l'atteinte de cet objectif. Ainsi, si l'objectif spécifique est d'accroître la valeur aux yeux des actionnaires en augmentant régulièrement le bénéfice d'exploitation, alors (en référence aux processus apparaissant dans l'encadré 5-2) les processus 3, 4 et 5 peuvent être des processus clés, tandis que certains des processus support comme le processus 8 ne le seront pas. Il est important de noter que, si des processus ne sont pas clés pour un objectif spécifique, ils peuvent l'être pour un autre. Dans l'exemple ci-dessus, si la clôture mensuelle des comptes n'est

Copyright © 2015 Eyrolles.

pas un processus clé pour l'objectif de croissance des résultats, elle peut l'être pour l'objectif qui consiste à « fournir des informations financières fiables et en temps utile ». Une fois que les processus clés sont identifiés, ils sont analysés en détail. Le processus est scindé en sous-processus, jusqu'à ce que l'on atteigne le niveau des activités. Cette approche est efficace car elle produit un ensemble gérable de processus critiques. Elle est généralement adoptée par une équipe possédant une vaste vue d'ensemble de l'organisation, mais sans connaissance détaillée de chaque domaine. Cependant, elle peut conduire à négliger des processus qui se révèlent *in fine* critiques.

Approche ascendante (*bottom-up*)

Approche qui commence par une revue de tous les processus au niveau des activités, et se poursuit par l'agrégation des processus identifiés dans l'ensemble de l'organisation.

L'approche ascendante (*bottom-up*) commence par une revue de tous les processus au niveau des activités. Elle nécessite donc que tous les services de l'organisation identifient et documentent les processus opérationnels auxquels ils participent. Cette tâche est exécutée par les collaborateurs responsables des activités en question. Les processus identifiés sont ensuite agrégés dans l'ensemble de l'organisation. Si cette approche fonctionne bien pour des organisations de petite taille comportant un nombre limité de processus, elle est moins efficace pour les organisations grandes et complexes car il devient difficile de déterminer l'importance relative de chaque processus.

Une fois un processus identifié, l'étape suivante, quelle que soit l'approche, consiste à déterminer ses objectifs clés. Il faut répondre aux questions suivantes.

- Pourquoi le processus existe-t-il ?
- Comment le processus soutient-il la stratégie de l'organisation et contribue-t-il à sa réussite ?
- Comment les individus sont-ils censés agir, réagir… ?
- Que réalise le processus qui le rend important pour le management ?[1]

Pour un auditeur interne, ou quelqu'un qui ne participe pas directement au processus, la première source d'information est le propriétaire du processus et la documentation existante sur les règles et les procédures dudit processus. Dans l'idéal, son propriétaire a défini des objectifs formels qui répondent aux quatre questions ci-dessus. Sinon, l'auditeur interne devra, pour obtenir les informations nécessaires, travailler avec les collaborateurs clés impliqués dans ce processus.

Une fois les objectifs du processus compris, il s'agit d'analyser les données d'entrée du processus, les activités spécifiques nécessaires pour parvenir aux objectifs du processus (et aux résultats du processus). Pour comprendre comment ces données d'entrée et activités se combinent pour générer des résultats, il convient de commencer par analyser les documents existants, par exemple :

- les manuels de procédures ;
- les politiques liées au processus ;

Copyright © 2015 Eyrolles.

- la description de poste des collaborateurs concernés ;
- la cartographie des processus qui décrit le flux de processus.

Même si les documents existants constituent un point de départ important, il est généralement nécessaire de discuter des différents aspects du processus avec les collaborateurs qui en ont la responsabilité. Afin de mieux comprendre le processus opérationnel, il est possible de poser les questions suivantes à son propriétaire et aux autres collaborateurs clés.

1. Pourquoi ce processus existe-t-il ?
2. Sur quels objectifs stratégiques de l'organisation le processus peut-il avoir une incidence et comment ?
3. Quelles initiatives, actions, le processus doit-il déclencher pour aider l'organisation à atteindre ses objectifs stratégiques ?
4. Qu'apporte le processus à l'organisation, sans lequel elle aurait du mal à prospérer ?
5. En fin de compte, qu'est-ce qui donne aux collaborateurs participant au processus un sentiment de satisfaction dans leur travail ?
6. Quelles sont les réalisations qui permettent aux collaborateurs participant au processus d'être reconnus par le management ou par les clients internes ?
7. Comment les individus concernés par le processus sont-ils censés agir et que se passe-t-il s'ils ne répondent pas à cette attente ?
8. Existe-t-il des indicateurs clés de performance permettant de mesurer et de suivre les performances ?[2]

Pour comprendre le processus, il faut non seulement identifier les objectifs clés, mais également comprendre comment le management et le propriétaire du processus savent si celui-ci fonctionne comme prévu. Le propriétaire du processus doit avoir défini des indicateurs clés pour suivre les performances du processus. Ces indicateurs doivent être :

- observables (ils peuvent être mesurés objectivement) ;
- pertinents pour l'objectif en question (et non pas utilisés simplement parce qu'ils peuvent être quantifiés) ;
- rapidement disponibles ;
- communiqués aux collaborateurs concernés par le processus.

Les indicateurs clés de performance ou d'autres types d'indicateurs peuvent indiquer les attentes du management, ou ses seuils de tolérance, en ce qui concerne les résultats du processus.

Indicateur clé de performance

Donnée chiffrée ou toute autre forme de mesure permettant de déterminer si un processus ou une tâche donnés respectent les seuils de tolérance fixés.

Copyright © 2015 Eyrolles.

DESCRIPTION ÉCRITE DES PROCESSUS OPÉRATIONNELS

Il est impératif de décrire par écrit le processus opérationnel. Ce sont généralement le propriétaire et les responsables du processus qui s'en chargent. Cependant, il peut arriver qu'ils ne le fassent pas à cause des impératifs quotidiens de leur travail ou parce qu'ils n'en voient pas l'utilité. Si l'absence de description a peu de conséquences immédiates, avec le temps et à mesure que les collaborateurs concernés changent de poste ou quittent l'organisation, les objectifs du processus risquent d'être perdus ou faussés. La description écrite du processus peut se révéler très efficace pour :

- orienter les nouveaux collaborateurs ;
- définir les périmètres de responsabilité ;
- évaluer l'efficience des processus ;
- déterminer des zones prioritaires ;
- identifier les principaux risques et contrôles.

Les auditeurs internes doivent également documenter leur évaluation globale des risques et des contrôles au sein de l'organisation et dans toutes les missions spécifiques d'assurance qu'ils conduiront sur le processus en question.

Deux méthodes sont généralement utilisées : cartographie des processus et description des processus. Les cartographies des processus peuvent être générales ou détaillées activité par activité. Elles constituent une représentation graphique des données d'entrée, des étapes, des flux et des résultats. Elles peuvent s'accompagner d'une note descriptive.

Les cartographies générales cherchent à décrire les données d'entrée, les activités, les étapes, les flux et interactions avec d'autres processus et les résultats. Elles procurent un cadre de référence global permettant de comprendre en détail les activités et les sous-processus. L'objectif de la cartographie générale des processus est la simplicité, car elle se concentre sur l'ensemble et non sur les détails. L'encadré 5-4 donne un exemple de cartographie pour un étudiant qui souhaite arriver à l'heure au cours de 8 h du lendemain.

S'il n'existe pas de norme absolue concernant le format et les symboles à utiliser dans une cartographie, les fonctions d'audit interne et les prestataires de services s'efforcent néanmoins de faire preuve de cohérence.

Commentaire du traducteur

La norme ISO 5807 définit les symboles utilisés pour représenter les processus sous forme de diagrammes de flux.

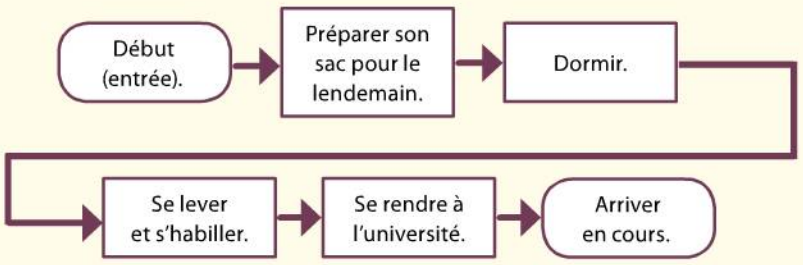
Copyright © 2015 Eyrolles.

L'encadré 5-5 présente les symboles génériques et leur signification. Les cartographies sont généralement structurées de manière à ce que la séquence d'activités se déroule de gauche à droite, comme dans l'encadré 5-4, et/ou de haut en bas.

L'encadré 5-6 présente une cartographie des processus détaillée concernant l'objectif qui consiste à arriver à l'heure au cours de 8 h du lendemain. Le processus général décrit dans l'encadré 5-4 est subdivisé pour montrer les activités ou les sous-processus spécifiques. Une note descriptive accompagne souvent la cartographie afin d'expliquer les activités de manière plus détaillée. L'encadré 5-6 montre comment la note descriptive étaye la cartographie : elle donne de plus amples détails sur l'activité. Elle peut également décrire les contrôles.

ENCADRÉ 5-4

CARTOGRAPHIE GÉNÉRALE DES PROCESSUS : « ARRIVER À L'HEURE AU COURS DE 8 H »



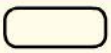
RISQUES OPÉRATIONNELS

Une fois que l'auditeur interne a compris les objectifs d'une organisation et les processus clés qui permettent de les atteindre, il doit évaluer les risques opérationnels susceptibles d'empêcher d'atteindre ces objectifs. La capacité du responsable de l'audit interne et de son équipe à comprendre précisément les risques opérationnels détermine dans quelle mesure la fonction d'audit interne peut remplir sa mission et accroître la valeur de l'organisation. La première étape consiste à élaborer le profil de risque global de l'organisation qui identifie les risques critiques pour chaque objectif stratégique. Pour le nombre croissant d'organisations qui pratiquent le management des risques de l'entreprise (*Entreprise Risk Management* – ERM), le management peut élaborer des profils de risque global. Dans ce cas, chaque fonction d'audit interne peut élaborer son évaluation du risque à partir du profil de risque de l'organisation. S'il n'existe pas de profil de risque global, l'audit interne devra créer ce profil qui lui servira de point de départ pour son plan d'audit annuel.

Copyright © 2015 Eyrolles.

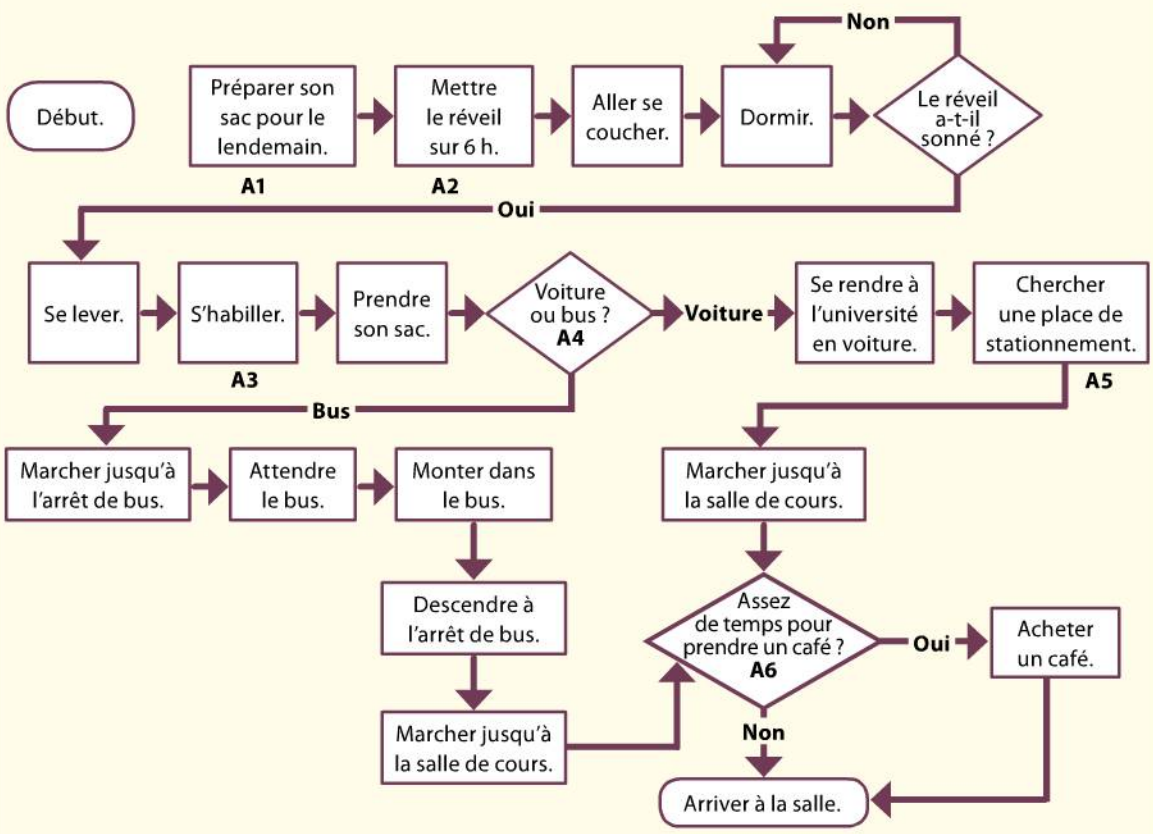
ENCADRÉ 5-5

SYMBOLES COURANTS EN CARTOGRAPHIE DES PROCESSUS

	**Processus ou opération** – Processus, sous-processus ou activité.
	**Décision** – Indique une alternative (par exemple, oui/non ou accepter/rejeter), chaque choix engendrant différents flux d'activités.
	**Ligne de liaison** – Sens dans lequel vont les activités, les flux de travail et les transferts.
	**Terminateur** – Marque de début ou de fin d'un flux.

ENCADRÉ 5-6

CARTOGRAPHIE DÉTAILLÉE DES PROCESSUS : « ARRIVER À L'HEURE AU COURS DE 8 H »



A1 Déterminer quels livres et documents seront nécessaires pour le cours. Placer le téléphone portable et l'ordinateur portable dans le sac.

A2 Mettre la sonnerie du réveil sur 6 h – 5 h 45 si l'on veut prendre un petit déjeuner.

A3 Se doucher, se brosser les dents, se coiffer, repasser sa chemise, si nécessaire.

A4 Évaluer la probabilité de trouver une place de stationnement et la probabilité que le bus soit en retard.

A5 Commencer par le parc C1. Si complet, aller au parc C3. Si complet, aller au parc D3, plus loin.

A6 S'il reste 15 minutes avant le cours au moment de passer devant la cafétéria, s'arrêter et prendre un café. Sinon, aller directement en cours.

Copyright © 2015 Eyrolles.

Il existe plusieurs outils et méthodes pour élaborer un profil de risque. Ce chapitre ne s'intéresse qu'à un petit nombre d'entre eux. Malgré l'apport de ces outils, l'exercice reste, par nature, très subjectif. L'expérience et un jugement sûr sont nécessaires.

Il est fréquent de commencer par une séance de réflexion collective avec la direction générale ou, à défaut, avec l'audit interne. Le groupe peut partir d'un modèle de risque général qui expose les catégories et types de risques qu'une organisation est susceptible de rencontrer. Dans cet exemple (encadré 5-7), les risques potentiels sont subdivisés en quatre catégories qui correspondent aux objectifs de management des risques du COSO et 10 sous-catégories (*cf.* chapitre 4, *La gestion des risques*).

ENCADRÉ 5-7

MODÈLE GÉNÉRIQUE DES RISQUES OPÉRATIONNELS

<table>
<tr><th colspan="2">RISQUES STRATÉGIQUES</th><th colspan="2">RISQUES DE NON-CONFORMITÉ</th><th colspan="2">RISQUES LIÉS AU REPORTING</th></tr>
<tr><th>Externes</th><th>Internes</th><th>Externes</th><th>Internes</th><th>Externes</th><th>Internes</th></tr>
<tr><td rowspan="3">Changement dans les lois et règlements.
Concurrence.
Évolution de la dynamique du marché.
Secteur.
Technologie.</td><td rowspan="3">Réputation.
Orientation stratégique.
Satisfaction des clients.
Gouvernance.</td><td rowspan="3">Contrats.
Réglementation.
Contentieux.
Autorisations.</td><td rowspan="3">Déontologie.
Politiques.
Fraude et autres actes illégaux.</td><td>Reporting financier et comptable.
Fiscalité.</td><td>Budget.
Mesures de la performance.
Contrôle interne et reporting réglementaire.</td></tr>
<tr><td colspan="2">Ressources informationnelles</td></tr>
<tr><td colspan="2">Accès.
Disponibilité des informations.
Intégrité des données.
Infrastructure.
Confidentialité des données.</td></tr>
<tr><th colspan="6">RISQUES OPÉRATIONNELS</th></tr>
<tr><th colspan="2">Liés aux processus</th><th colspan="2">Liés aux individus</th><th colspan="2">Liés aux aspects financiers</th></tr>
<tr><td colspan="2">Capacité de la chaîne d'approvisionnement.
Exécution des processus.
Hygiène et sécurité.
Continuité d'activité.
Durée de cycle.
Catastrophes.
Absence d'innovation.</td><td colspan="2">Offre de main-d'œuvre.
Direction/collaborateurs clés.
Incitations à la performance.
Responsabilisation.
Préparation au changement.
Communication.</td><td colspan="2">Taux d'intérêt.
Taux de change.
Capacité.
Défaillance.
Concentration.
Disponibilité des capitaux.
Gestion de trésorerie.
Prix des matières premières.
Horizon temporel.</td></tr>
</table>

Leur impact (ou gravité) et leur probabilité d'occurrence sont ensuite évalués. L'impact, c'est-à-dire les conséquences défavorables d'un risque survenu, est généralement estimé sous forme de catégories. On utilise habituellement trois catégories (élevé, moyen, faible) ou cinq (recours à un nombre impair pour éviter les résultats médians). L'encadré 5-8 présente un modèle en cinq catégories. Il est utile de délimiter chaque catégorie lorsque l'on collecte des renseignements auprès de plusieurs collaborateurs.

Copyright © 2015 Eyrolles.

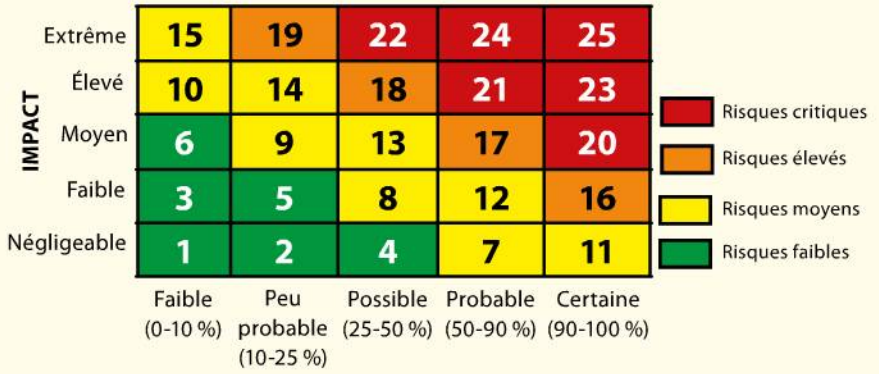
Dans ce modèle, les limites de l'impact sont fixées en termes numéraires et de conséquences pour les objectifs de l'organisation. Cependant, certaines organisations fixent d'autres limites. Ainsi, certaines évaluent l'impact en termes de réputation, d'hygiène et de sécurité, de légalité ou de dommages causés aux actifs. Pour l'hygiène et la sécurité, les catégories peuvent être les suivantes : blessure légère, blessure mineure, blessure majeure, décès et décès multiples, l'échelle allant de « négligeable » à « extrême » (échelle d'impact présentée dans l'encadré 5-8). Le lecteur doit noter que d'autres termes peuvent être employés pour désigner l'impact. On parle parfois d'importance relative, même si les auteurs préfèrent désigner par « importance » une évaluation conjointe de l'impact et de la probabilité. On parle aussi de « sévérité » pour désigner les conséquences défavorables d'un risque survenu.

La probabilité d'occurrence (fréquence) peut être évaluée en termes de « chances/risques » ou de probabilité que le risque survienne. Étant donné la nature subjective de ces estimations, la plupart des managers et des auditeurs internes préfèrent toutefois exprimer la probabilité dans des catégories moins précises. Là encore, on recourt souvent à une échelle comportant trois catégories (élevé, moyen, faible) ou cinq (encadré 5-8). De même que pour l'impact, il est utile de spécifier les limites des catégories, ce qui est généralement effectué en termes de probabilités spécifiques ou de plages de probabilités (voir l'échelle dans l'encadré 5-8).

À l'aide du modèle d'évaluation des risques présenté dans l'encadré 5-8, les différents risques opérationnels qui se dégagent du

ENCADRÉ 5-8

MODÈLE D'ÉVALUATION DES RISQUES



Impact

Extrême : > 100 millions	– Menace sur l'existence de l'organisation	Risques critiques
Élevé : 25-100 millions	– Difficulté à atteindre les objectifs	Risques élevés
Moyen : 5-25 millions	– Difficulté à atteindre certains objectifs	Risques moyens
Faible : 1-5 millions	– Quelques résultats non souhaités	Risques faibles
Négligeable : < 1 million	– Aucun impact notable sur les objectifs	

Copyright © 2015 Eyrolles.

modèle générique (encadré 5-7) peuvent être placés sur la matrice. Cette opération est fréquemment réalisée lors d'une séance de groupe réunissant des membres de la direction générale ou, s'ils ne sont pas disponibles, d'autres membres du management et les membres les plus expérimentés de la fonction d'audit interne. Il est préférable de faire appel à la direction générale et aux managers opérationnels car ce sont ceux qui comprennent le mieux les risques dans leur domaine de responsabilité. Au cours de cette réunion, ils débattent des risques et parviennent à un consensus concernant l'impact, la probabilité d'occurrence et la position des différents risques sur la matrice. La combinaison de l'impact et de la probabilité d'occurrence détermine l'importance des risques. L'encadré 5-8 présente la matrice divisée en 25 cases : les cases 20 à 25 représentent les risques critiques et les cases 16 à 19 les risques importants. Ces risques constituent la plus grande menace qui pèse sur la réalisation des objectifs de l'organisation. Les cases 7 à 15 représentent les risques modérés et les cases 1 à 6 les risques faibles.

ENCADRÉ 5-9

IDENTIFICATION DES RISQUES CRITIQUES

IMPACT	Faible (0-10 %)	Peu probable (10-25 %)	Possible (25-50 %)	Probable (50-90 %)	Certaine (90-100 %)
Extrême	Catastrophes. Gouvernance.	Absence d'innovation de produits.	Disponibilité des informations. Économie. Continuité d'activité.		
Élevé	Changements dans les lois et règlements du secteur. Secteur. Orientation stratégique.	Réputation. Technologie. Concurrence. Satisfaction des clients. Reporting financier et comptable. Accès. Infrastructure. Gestion de trésorerie.	Contentieux. Fraude et autres irrégularités. Budget. Intégrité des données.	Confidentialité des données.	
Moyen	Concentration.	Contrats. Réglementation. Politiques. Contrôle interne et reporting réglementaire. Horizon temporel. Disponibilité des capitaux. Direction/collaborateurs clés. Offre de main-d'œuvre.			
Faible	Hygiène et sécurité. Autorisations.	Fiscalité. Prix des matières premières.	Taux de change. Chaîne d'approvisionnement.		
Négligeable					

PROBABILITÉ

Copyright © 2015 Eyrolles.

MATRICE DES OBJECTIFS ET DES RISQUES CRITIQUES

		RISQUES CRITIQUES (RC)						
Mission : acquérir les connaissances et les compétences nécessaires pour occuper un poste d'auditeur interne junior.		RC1 Être malade.	RC2 Oublier l'échéance.	RC3 Être en retard ou avoir une panne d'oreiller.	RC4 Ne pas avoir les documents nécessaires pour le cours.	RC5 Ne pas avoir assez de temps pour faire tout le travail.	RC6 Être incapable de comprendre les documents.	RC7 Sortir ou faire d'autres activités.
OBJECTIFS	1. Assister à tous les cours.	×		×				
	2. Être à l'heure à tous les cours.	×		×				×
	3. Lire les ouvrages conseillés avant les cours dont ils seront l'objet.		×		×	×		×
	4. Faire tous ses exercices dans les temps.	×	×		×	×	×	×
	5. Obtenir au moins une très bonne évaluation à tous les examens.		×			×	×	×

ENCADRÉ 5-10

Risque

Possibilité qu'un événement survienne et ait un impact défavorable sur la réalisation des objectifs.

L'encadré 5-9 propose un exemple de cartographie du modèle de risque en relation avec la matrice d'évaluation des risques pour une société de services financiers. Quatre risques identifiés comme critiques apparaissent dans les cases 21 et 22. Les risques dans les cases 18 et 19 sont considérés comme étant élevés et, selon le nombre d'objectifs sur lesquels ils ont des conséquences, ils peuvent également nécessiter une attention plus soutenue.

L'étape suivante consiste à trouver un lien formel entre les risques identifiés et les objectifs spécifiques que chaque risque est susceptible d'entraver. Cela permet de s'assurer que tous les principaux risques, et leurs conséquences, ont été identifiés. Pour reprendre notre exemple (arriver à l'heure en cours), supposons que la mission, ce semestre, soit d'acquérir les connaissances et les compétences nécessaires pour occuper un poste d'auditeur interne junior. Plusieurs objectifs stratégiques spécifiques peuvent être fixés pour la réalisation de cette mission :

1. assister à tous les cours ;
2. être à l'heure à tous les cours ;
3. lire les ouvrages conseillés avant les cours dont ils seront l'objet ;
4. faire tous ses exercices dans les temps ;
5. obtenir au moins une très bonne évaluation à tous les examens.

Copyright © 2015 Eyrolles.

Le processus décrit dans les encadrés 5-4 et 5-6, pour arriver à l'heure au cours de 8 h, contribue à l'objectif 2 et, dans une certaine mesure, à l'objectif 1. D'autres processus comme ceux liés à l'étude sont critiques pour les objectifs 3, 4 et 5. Le chapitre 4, *La gestion des risques*, définit le risque comme la « possibilité qu'un événement survienne et ait un impact défavorable sur la réalisation des objectifs ». Cette définition permet d'identifier un certain nombre de risques susceptibles d'empêcher la réalisation des cinq objectifs stratégiques spécifiques pris en exemple ci-devant. Par exemple, tomber malade aura une incidence sur la réalisation des objectifs 1, 2 et 4. L'encadré 5-10 présente sept risques critiques et leur capacité à empêcher la réalisation des cinq objectifs stratégiques.

Le type d'analyse réalisée pour acquérir les connaissances et les compétences nécessaires à un poste d'auditeur interne junior et les objectifs requis peuvent également s'appliquer aux organisations. Comme nous l'avons mentionné dans notre discussion sur les processus opérationnels au début du chapitre, les objectifs sont généralement énoncés dans les déclarations obligatoires, comme les rapports semestriels des sociétés cotées aux États-Unis et les documents de référence de l'AMF, ou dans les documents relatifs à la planification stratégique.

Cartographier les risques liés aux processus opérationnels

Sous l'angle du management des risques de l'entreprise (chapitre 4, *La gestion des risques*), l'étape suivante consiste à élaborer des modalités de traitement appropriées à chaque risque. Il existe quatre modalités de traitement des risques.

- **L'évitement (ou refus).** Décision de cesser ou de céder les activités à l'origine du risque. L'évitement du risque peut aussi bien avoir pour conséquence, par exemple, d'interrompre une ligne de produits, de décider de ne pas procéder à l'expansion prévue sur un nouveau marché géographique que de vendre une activité.
- **La réduction.** Prise de mesures afin de réduire l'impact ou la probabilité d'occurrence du risque, ou les deux à la fois. Il s'agit habituellement d'une multitude de décisions prises quotidiennement, comme la mise en place de contrôles.
- **Le partage (ou transfert).** Réduction de l'impact ou de la probabilité d'occurrence du risque en transférant ou en partageant le risque. Parmi les techniques courantes, citons l'achat de produits d'assurance, les opérations de couverture ou l'externalisation d'une activité.
- **L'acceptation (ou conservation).** Ne rien faire pour modifier l'impact ou la probabilité d'occurrence du risque. L'organisation est disposée à accepter le risque à son niveau actuel plutôt qu'à dépenser des ressources considérables à déployer l'une ou l'autre des solutions.

Évaluation des risques

Identification et analyse (généralement en termes d'impact et de probabilité d'occurrence) des risques susceptibles d'affecter la réalisation des objectifs d'une organisation, de façon à déterminer comment ces risques doivent être gérés.

Quatre stratégies face au risque

– Évitement/refus.
– Réduction.
– Partage/transfert.
– Acceptation/conservation.

Copyright © 2015 Eyrolles.

Afin de sélectionner les bonnes stratégies, il est nécessaire de comprendre comment les risques affectent les processus opérationnels de l'organisation. Les auditeurs internes doivent trouver les liens entre les risques et les processus opérationnels afin de déterminer si le risque est géré à un niveau approprié dans le cadre de la stratégie de traitement du management et d'identifier là où se trouve le risque critique au sein de l'organisation. La Norme 2010, Planification, spécifie que « le responsable de l'audit interne doit établir un plan d'audit fondé sur les risques afin de définir des priorités cohérentes avec les objectifs de l'organisation »[3].

ENCADRÉ 5-11

MATRICE RISQUES/PROCESSUS

P – Lien primaire S – Lien secondaire	Risque 1	Risque 2	Risque 3	Risque 4	Risque 5	Risque 6	Risque 7	…	Risque m
Processus 1		S		P					
Processus 2				S					
Processus 3			S						
Processus 4	P						S		
Processus 5				S					
Processus 6							S		P
Processus 7				S	S	S	P		
Processus 8		P							S
Processus 9	S				P	P			
Processus 10		P							S
Processus 11	S		P		S				
…									
Processus n		S		P			S		

Une méthode efficace permettant de trouver le lien entre les processus et les risques sous-jacents consiste à créer une matrice de risques analogue à la matrice présentée dans l'encadré 5-10, qui reliait les objectifs aux risques critiques. Les risques sont énoncés sur la ligne du haut de la matrice, et les processus sur la colonne de gauche (encadré 5-11). Les risques sont ceux identifiés dans le modèle des risques opérationnels (encadré 5-7). On dénombre généralement de 30 à 70 risques. Le processus d'évaluation des risques présenté dans les encadrés 5-8 et 5-9 peut également servir à réduire la liste des risques. Par exemple, on peut juger utile de limiter les risques, auxquels des processus sont liés, aux seuls risques apparaissant dans les cases 7 à 25 (encadré 5-8).

L'étape suivante consiste à analyser les processus afin de déterminer s'il existe des associations entre les processus et les risques.

Copyright © 2015 Eyrolles.

Pour reprendre l'exemple initial (« être à l'heure au cours de 8 h »), il est possible d'évaluer les liens entre ce processus (encadré 5-6) et les sept risques critiques énoncés à l'encadré 5-10. Une association directe entre ce processus et le risque critique n° 3 (être en retard ou avoir une panne d'oreiller) existe. Il existe également une association avec le risque critique n° 4 (ne pas avoir les documents nécessaires pour le cours) car il faut, pour remplir l'objectif général, avoir rassemblé les documents nécessaires pour suivre les cours et étudier pendant le reste de la journée. Le risque critique n° 5 (ne pas avoir assez de temps pour faire tout le travail) et le risque critique n° 6 (être incapable de comprendre les documents) ne sont à l'évidence pas liés à ce processus. Ils sont liés à d'autres processus comme « gérer le temps », « planifier » et les processus d'étude.

Une fois que l'on a identifié les risques auxquels un processus donné est associé, il convient d'évaluer les associations afin de déterminer si un lien est primaire ou secondaire. Les liens primaires sont ceux par lesquels le processus joue un rôle direct dans la gestion des risques. Les liens secondaires sont ceux par lesquels le processus joue un rôle indirect dans la gestion des risques. Dans notre exemple, le risque critique n° 3 sera considéré comme un lien primaire, tandis que le risque critique n° 4 sera considéré comme un lien secondaire. Lorsque les liens sont envisagés par rapport à un risque particulier, un ou deux (trois au plus) processus peuvent être considérés comme ayant des liens primaires et un nombre indéfini d'autres processus comme ayant un lien secondaire.

Une fois finalisée, la matrice risques/processus peut servir à la fonction d'audit interne pour déterminer quelles missions doivent être incluses dans le plan d'audit annuel. La première étape consiste à inventorier les liens primaires et secondaires de chaque processus. Le nombre et la nature des liens entre les risques et les processus influenceront le type d'audit interne qui sera mené. Par exemple, un processus présentant des liens primaires avec plusieurs risques nécessitera un audit complet de l'intégralité du processus. Si un risque présente des liens primaires avec plusieurs processus, il sera plus judicieux de mener un audit de tous ces processus afin de donner une assurance concernant le risque dans son ensemble. Il est nécessaire d'avoir beaucoup d'expérience pour être à même de procéder à ces jugements. Par ailleurs, on peut établir un cycle d'audit de chaque processus sur la base de l'impact et de la probabilité d'occurrence des risques y afférents. Par exemple, les processus qui entretiennent un lien primaire avec un ou plusieurs risques critiques ou avec plusieurs risques importants et modérés peuvent être audités tous les un ou deux ans. Ceux qui n'entretiennent que des liens secondaires avec des risques critiques et importants peuvent être audités dans un cycle de trois, quatre ou cinq ans. Il convient de relire les résultats des audits antérieurs. Par exemple, si l'audit précédent a identifié des problèmes significatifs, un processus doit être audité avant que son cycle ne se termine, même si celui-ci se déroule sur trois ou quatre ans.

Lien primaire

Lien par lequel le processus joue un rôle direct dans la gestion des risques.

Lien secondaire

Lien par lequel le processus joue un rôle indirect dans la gestion des risques.

Copyright © 2015 Eyrolles.

Pour mettre en relation processus opérationnels et risques, une autre méthode, plus indirecte, consiste à définir des facteurs de risque génériques qui permettront d'évaluer les risques, pour tous les processus (approche reposant sur les facteurs de risque). En général, les modèles de facteurs de risque identifient entre 7 et 15 facteurs qui permettent d'évaluer chaque processus. Ces facteurs ne coïncident pas avec les risques opérationnels figurant sur le modèle générique présenté plus haut (encadré 5-7). Ils comportent un degré d'abstraction plus élevé, qui peut être appliqué à chaque processus. La plupart des modèles se composent de deux catégories génériques : les facteurs de risque externes et les facteurs de risque internes, même si d'autres facteurs de risque peuvent également être pris en compte. Les premiers, externes, font partie intégrante de l'environnement et de la nature du processus lui-même. Il peut s'agir de caractéristiques telles que le niveau d'activité relatif, le volume et la liquidité des actifs utilisés dans le processus, la complexité du processus (nombre d'étapes et de données d'entrée) ou les restrictions juridiques et réglementaires. Les facteurs de risque internes concernent le degré auquel les contrôles intégrés au processus garantissent que celui-ci atteint ses objectifs, les performances des collaborateurs participant aux activités et à la gestion du processus, ainsi que le degré d'évolution du processus et de son environnement. Certains modèles comportent plusieurs autres facteurs, dont, le plus souvent, le temps écoulé depuis le dernier audit, les résultats de l'audit précédent et les préoccupations du management.

Une fois les facteurs de risque identifiés, trois autres décisions doivent être prises avant la mise en œuvre du modèle. Premièrement, il faut fixer l'échelle d'évaluation de chaque facteur. On recourt habituellement à une échelle en trois, cinq ou sept points. Sur une échelle en trois points, 1 est faible, 2 moyen et 3 élevé. On peut également délimiter les trois catégories pour chaque facteur. Par exemple, si l'un des facteurs est « la quantité d'actifs utilisés », la valeur faible (cotation de 1) peut être inférieure ou égale à 500 000, la valeur moyenne (cotation de 2) comprise entre 500 000 et 10 millions et la valeur élevée (cotation de 3) supérieure à 10 millions. Indépendamment de l'échelle retenue (en trois, cinq, sept ou n points), il convient d'utiliser la même pour évaluer tous les facteurs. L'encadré 5-12 présente un exemple de modèle à 10 facteurs, qui recourt à une échelle en trois points. Les 10 facteurs sont divisés en trois types de facteurs de risque (externes, internes et autres). L'encadré 5-12 nomme le facteur de risque dans la première colonne et explique la signification des trois cotations dans la deuxième colonne.

La décision suivante a trait à l'importance relative (poids ou pondération) d'un facteur par rapport à un autre. On peut assigner la même pondération à tous les facteurs de risque si l'on considère que chacun a une importance égale. À cette fin, on attribue en général des chiffres compris entre 0 et 100 afin que la somme des

Copyright © 2015 Eyrolles.

APPROCHE REPOSANT SUR LES FACTEURS DE RISQUE

DESCRIPTION DES FACTEURS DE RISQUE, PONDÉRATIONS ET COTATIONS

Facteurs de risque	Description	Cotation (1-3)	Pondération X	Cotation pondérée
Facteurs externes				
Actifs à risque	1 - Moins de 500 000. 2 - De 500 000 à 5 millions. 3 - Plus de 5 millions.		10	
Visibilité	1 - Unité d'exploitation/clients en direct. 2 - Au niveau des divisions/petit nombre de clients. 3 - Organisation/presse nationale.		10	
Complexité	1 - Processus composé de missions simples et routinières. 2 - Nécessite plusieurs étapes et une interaction entre de nombreux intervenants. 3 - Étapes multiples, imposant une coordination entre de nombreux intervenants dans le cadre du processus et avec d'autres processus.		10	
Taille du processus/ de l'opération	1 - Le processus influe sur moins de 3 % des activités de l'organisation. 2 - Le processus influe sur 3 à 15 % des activités de l'organisation. 3 - Le processus influe sur plus de 15 % des activités de l'organisation.		10	
Obligations juridiques/ réglementaires/ externes	1 - Peu d'obligations ou généralement non réglementées. 2 - Quelques obligations juridiques, réglementaires ou externes. 3 - Obligations nombreuses et/ou complexes.		10	
Facteurs internes				
Stabilité du contrôle interne	1 - Système mature de gestion et de contrôle des risques. 2 - Système stable de gestion et de contrôle des risques avec des changements modérés. 3 - Changements significatifs apportés au système de gestion et de contrôle des risques.		5	
Efficacité du contrôle interne	1 - Pas de problèmes de contrôle interne ou de conformité au cours des deux dernières années. 2 - Cas de fraude, de faiblesses du contrôle interne ou de défauts de conformité, mais aucun d'important au cours des deux dernières années. 3 - Fraude, faiblesses du contrôle interne ou défauts de conformité importants au cours des deux dernières années.		10	
Changements importants dans les opérations, les processus, les collaborateurs ou la technologie de l'organisation	1 - Pas de changement important au cours des 12 derniers mois. 2 - Quelques changements dans les processus ou les collaborateurs clés au cours des 12 derniers mois. 3 - Changement majeur dans l'organisation et dans les processus ou introduction d'un nouveau système d'information au cours des 12 derniers mois.		15	
Autres facteurs				
Préoccupations de la direction générale	1 - Pas de préoccupations exprimées. 2 - Quelques préoccupations exprimées par la direction générale. 3 - Préoccupations notables exprimées par la direction générale ou le Conseil.		10	
Résultats du précédent audit	1 - Pas de problèmes de contrôle interne ou de conformité lors du dernier audit. 2 - Problèmes mineurs de contrôle interne ou de conformité lors du dernier audit. 3 - Faiblesses importantes de contrôle interne ou de conformité lors du dernier audit.		10	
Cotation du risque globale				

Copyright © 2015 Eyrolles.

pondérations soit égale à 100. Par conséquent, s'il existe cinq facteurs de risque considérés comme ayant tous la même importance, on assigne à chacun une pondération de 20. Sur le modèle présenté dans l'encadré 5-12, le facteur « stabilité du contrôle interne » reçoit une pondération de 5, ce qui signifie qu'il est considéré comme deux fois moins important que le facteur « actifs à risque » (pondération de 10) et trois fois moins important que le facteur « changements significatifs » (pondération de 15).

La décision finale porte sur la manière avec laquelle les facteurs de risque sont combinés entre eux. La plupart des approches reposant sur les facteurs de risque recourent à un modèle pondéré, dans lequel on multiplie chaque cotation par la pondération du facteur puis on additionne toutes les cotations pondérées pour obtenir une cotation du risque globale (encadré 5-12). Ainsi, celle-ci peut être comprise entre 100 et 300 et le risque peut être considéré comme un risque faible (cotation inférieure à 150), moyen (de 150 à 239) ou élevé (supérieur ou égal à 240). Après avoir déterminé le processus, on peut définir des intervalles de cotation. Les catégories ainsi créées peuvent ensuite servir à assigner à chaque processus un cycle d'audit d'un, deux, voire trois ans ou plus. Un cycle de deux ans signifie qu'un audit du processus est programmé tous les deux ans.

Une autre solution consiste à hiérarchiser les processus à auditer en les triant en fonction de leur cotation du risque pour sélectionner ceux qui affichent la cotation la plus élevée afin de les inclure dans le plan d'audit interne jusqu'à ce que soient épuisées les heures d'audit disponibles pour la période planifiée. Dans ce cas, il importe de noter la date du dernier audit effectué. À cette fin, on peut notamment ajouter parmi les facteurs de risque le temps écoulé depuis le dernier audit. Par exemple, sur le modèle présenté dans l'encadré 5-12, ce facteur serait intégré aux « autres facteurs » et pourrait recevoir la cotation de 1 « Processus audité au cours des 12 derniers mois », de 2 « Processus audité au cours des 12 à 36 derniers mois » ou de 3 « Processus non audité au cours des 36 derniers mois ».

Certaines fonctions d'audit interne préfèrent ne pas porter de jugement en utilisant des cotations totales, et examinent les cotations facteur par facteur. On peut y parvenir en assignant un indice faible, moyen ou élevé à chaque facteur. La fourchette des cotations varie en fonction du nombre de facteurs dans chaque catégorie (5, 3 et 2 dans notre exemple) et des différences de pondération. Ainsi, sur le modèle présenté dans l'encadré 5-12, la cotation totale des risques externes peut être comprise entre 50 et 150, celle des risques internes entre 30 et 90 et la cotation totale des autres facteurs entre 20 et 60. On peut donc dire que les risques externes sont faibles si leur cotation est inférieure à 90 et qu'ils sont élevés si leur cotation est supérieure ou égale à 125. Les risques internes sont qualifiés de faibles si leur cotation est inférieure à 50 et d'élevés

Copyright © 2015 Eyrolles.

si leur cotation est supérieure ou égale à 75. Les autres facteurs seront qualifiés de faibles si leur cotation est inférieure à 35 et d'élevés si leur cotation est supérieure ou égale à 50. L'encadré 5-13 est une représentation graphique envisageable pour déterminer le cycle d'audit. Comme précédemment, on peut assigner au processus un cycle d'un, deux voire trois ans ou plus.

ENCADRÉ 5-13

APPROCHE REPOSANT SUR LES FACTEURS DE RISQUE

ANALYSE DES RISQUES PAR PROCESSUS OPÉRATIONNEL			
	Externe	Interne	Autre
Processus 1			
Processus 2			
Processus 3			
Processus 4			
Processus 5			
Processus 6			
Processus 7			
Processus 8			
Processus 9			
Processus 10			
Processus 11			
…			
Processus n			
Niveau de risque	**Externe**	**Interne**	**Autre**
Fourchette potentielle des cotations	50 à 150	30 à 90	20 à 60
Faible	≤ 90	≤ 50	≤ 35
Moyen	90-124	50-74	35-49
Élevé	≥ 125	≥ 75	≥ 50

Processus opérationnels et risques dans le cadre de la mission d'assurance

La méthode utilisée jusqu'ici pour identifier les processus opérationnels et les risques de l'organisation s'applique aussi au niveau de la mission. Revenons à l'exemple proposé plus haut dans ce chapitre (encadré 5-10) : la mission consistant à acquérir les connaissances et les compétences nécessaires pour réussir en tant qu'auditeur interne junior, ainsi que les cinq objectifs définis pour y parvenir. Supposons que les parents d'un étudiant souhaitent obtenir l'assurance que celui-ci réalisera sa mission et ses objectifs. Ils demandent à l'un des aînés, récemment diplômé et qui

Copyright © 2015 Eyrolles.

travaille déjà comme auditeur interne, de rendre visite à l'étudiant pour effectuer un audit interne. Au début de l'audit, l'étudiant et son frère recensent ensemble un certain nombre d'activités et de processus que le premier doit mettre en œuvre pour accomplir sa mission :

- étudier pour préparer des examens ;
- lire les documents de cours ;
- faire les exercices et réaliser les projets nécessaires dans le cadre des cours ;
- prendre ses repas ;
- payer les frais de scolarité et autres factures ;
- écouter et prendre des notes pendant les cours ;
- sélectionner les cours appropriés et s'y inscrire ;
- s'entraîner ;
- faire le ménage dans son appartement ;
- arriver à l'heure au cours de 8 h.

Mission d'assurance

Examen objectif d'éléments probants, effectué en vue de fournir à l'organisation une évaluation indépendante des processus de gouvernement d'entreprise, de management des risques et de contrôle.

Cet exemple s'appuie sur le processus 10, qui est à suivre pour arriver à l'heure au cours de 8 h. L'auditeur interne/le frère commence par poser à l'étudiant une série de questions sur la façon dont ce dernier prépare la journée suivante, se lève le matin et va en cours. L'étudiant explique que, bien qu'il n'ait cours que le lundi, le mercredi et le vendredi ce semestre, son premier cours commence à 8 h. Après avoir obtenu des réponses à toutes ses questions, l'auditeur interne/le frère cartographie les processus et demande à l'étudiant si cette cartographie représente bien l'information donnée. L'étudiant propose quelques changements, ce qui aboutit à la cartographie des processus présentée dans l'encadré 5-6.

L'étape suivante consiste à identifier et évaluer les risques spécifiques à chaque activité ou sous-processus. À cette fin, l'auditeur interne/le frère place chaque activité sur une matrice, avec une description de chaque risque jusqu'au bas de la page, ainsi que le montre l'encadré 5-14. Chaque énoncé de risque décrit un événement susceptible d'influer négativement sur la capacité de l'activité ou du sous-processus à réaliser ses objectifs. L'impact potentiel de l'événement est ensuite défini et évalué en fonction de sa gravité. Pour finir, on estime la probabilité d'occurrence de cet événement. Les cinq premières colonnes de l'encadré 5-14 décrivent cette information à l'aide d'une matrice de risques et de contrôles, partiellement remplie, pour les quatre premières activités du processus consistant à se rendre sur le campus et les neuf risques associés.

Copyright © 2015 Eyrolles.

L'évaluation des risques peut également être représentée au moyen d'une cartographie qui hiérarchise les risques associés au processus clé. Les risques apparaissant dans la partie supérieure droite de cette cartographie seraient les plus critiques, et ceux dans la partie inférieure gauche relativement peu préoccupants. L'encadré 5-15 présente une cartographie des risques identifiés dans l'encadré 5-14. En combinant l'impact et la probabilité d'occurrence des événements, cette cartographie permet de déterminer si le risque concerné est critique, modéré ou faible.

Une fois les risques spécifiques identifiés, il faut déterminer comment ils sont gérés et si ce traitement permet de les ramener à un niveau acceptable. Comme indiqué plus haut, il existe quatre solutions : l'évitement (ou refus), la réduction, le partage (ou transfert) ou l'acceptation (ou conservation). Concernant les processus, la solution la plus fréquemment retenue consiste, soit à accepter le risque, soit à tenter de le réduire *via* des contrôles. Ceux-ci seront analysés plus en détail dans le chapitre 6, *Le contrôle interne*, et dans les chapitres suivants. Néanmoins, pour compléter l'analyse des risques dans notre exemple de processus, l'encadré 5-14 ajoute deux colonnes à la matrice de risques : la sixième spécifie la stratégie de traitement des risques et la septième la façon dont on peut obtenir l'assurance que cette stratégie (en particulier le contrôle) a permis une gestion efficace des risques.

Après avoir déterminé les stratégies de traitement, et vérifié leur efficacité, on peut obtenir une vue d'ensemble, en élaborant une cartographie de contrôle du risque, qui représente l'importance du risque. L'impact et la probabilité d'occurrence sont combinés pour aboutir à une importance (faible, modérée ou critique) par rapport à l'efficacité des contrôles. L'encadré 5-16 en donne une illustration en s'appuyant sur les risques spécifiques mentionnés dans l'encadré 5-14 pour le processus 10 (« arriver à l'heure au cours de 8 h »). La cartographie de contrôle du risque indique où se trouve le bon équilibre entre le risque et l'activité de contrôle, là où les activités de contrôle sont plus efficaces vis-à-vis des risques critiques (impact et probabilité élevés) que des risques faibles (impact et probabilité faibles). Dans l'exemple, les risques situés entre les deux lignes parallèles en pointillés (risques 4, 8, 1, 3 et 6) apparaissent bien équilibrés. Dans la partie supérieure gauche de la cartographie (risque 7), la relation contrôle/risque n'est pas équilibrée et la stratégie de traitement ne permet pas une bonne maîtrise des risques. En revanche, dans la partie inférieure droite, il se peut que plusieurs risques (5, 9 et 2) fassent l'objet d'un contrôle excessif. Ils correspondent à des situations dans lesquelles l'efficience pourrait être améliorée, en réduisant les ressources consacrées aux contrôles correspondants.

Copyright © 2015 Eyrolles.

MATRICE DE RISQUES ET DE CONTRÔLES POUR LE PROCESSUS 10 : « ARRIVER À L'HEURE AU COURS DE 8 H »

Activité ou sous-processus au sein du processus principal	Énoncé du risque	Impact potentiel	Quantification de l'impact	Probabilité	Traitement des risques	Technique d'évaluation de l'efficacité
Préparer son sac pour le lendemain	1. Oublier de prendre les exercices faits à la maison.	Perdre des points pour cause de travaux rendus en retard.	Moyen.	Moyenne.	Accepter.	–
	2. Oublier de prendre son téléphone portable.	Ne pas pouvoir recevoir et passer des appels.	Faible.	Élevée.	Réduire : toujours laisser son téléphone portable dans son sac.	Appeler son téléphone pour le localiser.
	3. Oublier d'éteindre et de prendre son ordinateur portable.	Être en retard parce que l'ordinateur portable a tardé à s'éteindre.	Faible.	Moyenne.	Accepter.	–
Régler la sonnerie du réveil à 6 h	4. Oublier de mettre son réveil à sonner.	Dormir trop longtemps et manquer le cours.	Élevé.	Élevée.	Réduire : mettre le réveil à sonner le matin, au lever.	Vérifier et constater que cela a bien été fait.
	5. Subir une panne de courant pendant la nuit.	Dormir trop longtemps et manquer le cours.	Élevé.	Faible.	Réduire : posséder un second réveil, à piles.	Observer.
Aller se coucher	6. Ne pas trouver le sommeil.	Être fatigué le lendemain.	Moyen.	Faible.	Accepter.	–
	7. Se coucher trop tard et manquer de sommeil.	Être fatigué le lendemain.	Moyen.	Moyenne.	Accepter.	–
Dormir/ se lever	8. Arrêter la sonnerie du réveil et se rendormir.	Manquer le cours ou arriver en retard en cours.	Élevé.	Moyenne.	Réduire : placer le réveil à l'autre bout de la chambre.	Vérifier qu'un réveil est placé à l'autre bout de la chambre.
	9. Interrompre plusieurs fois la sonnerie du réveil.	Manquer le cours ou arriver en retard en cours.	Élevé.	Faible.	Réduire : posséder un second réveil.	Observer.

Copyright © 2015 Eyrolles.

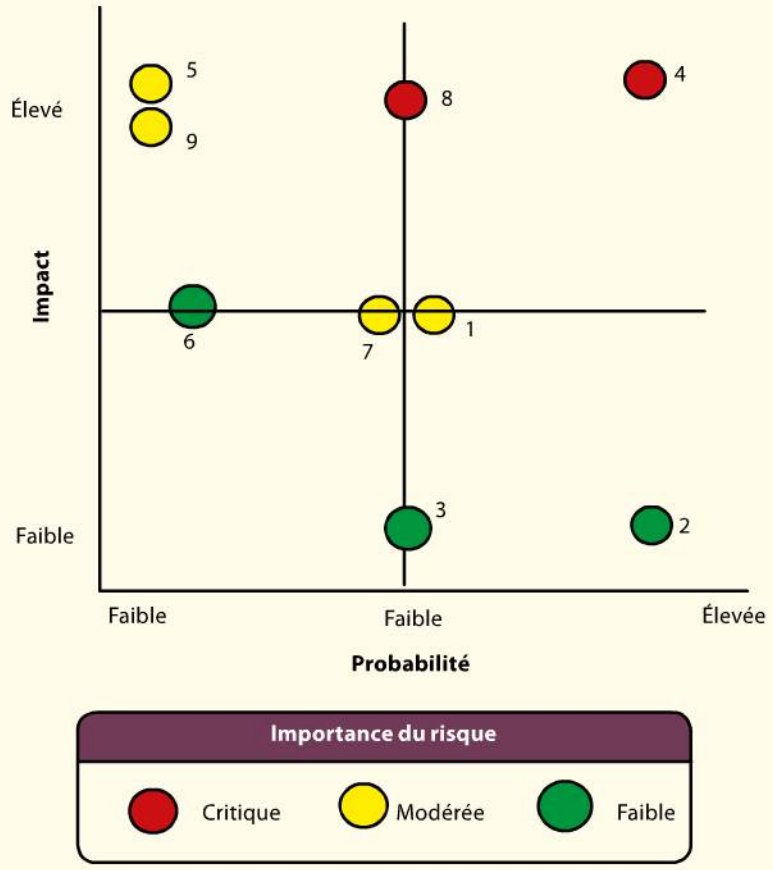
ENCADRÉ 5-14

EXTERNALISATION DE PROCESSUS OPÉRATIONNELS

Avant de conclure cette analyse des processus opérationnels et risques, il est important d'évoquer des situations dans lesquelles le processus n'est pas exécuté par des collaborateurs de l'organisation. Soucieuses de rationaliser leurs opérations et de réduire leurs coûts, de nombreuses organisations externalisent une proportion croissante de leurs processus opérationnels spécifiques. Parce que

ENCADRÉ 5-15

CARTOGRAPHIE PARTIELLE DES RISQUES POUR LE PROCESSUS 10 : « ARRIVER À L'HEURE AU COURS DE 8 H »



ces processus jouent un rôle important pour aider les organisations à atteindre leurs objectifs, il convient également de prendre en compte ces processus externalisés, de les intégrer dans l'évaluation des risques et dans l'univers d'audit interne d'une organisation.

L'externalisation de processus opérationnels (*Business Process Outsourcing*, BPO) consiste à transférer une partie des processus opérationnels d'une organisation à un prestataire extérieur, afin de réduire les coûts tout en améliorant la qualité et l'efficience du service. Étant donné la répétitivité des processus et la signature d'un contrat à long terme, l'externalisation va bien au-delà du recours à des consultants. La fonction paye et les systèmes d'information ont été les premiers processus opérationnels critiques à être externalisés. Cependant, cette tendance s'étend aux ressources humaines, à l'ingénierie, au service client, à la finance et comptabilité, ainsi qu'à la logistique, à mesure que les organisations cherchent à abaisser leurs coûts *via* l'effet de levier et les économies d'échelle obtenus par l'externalisation.

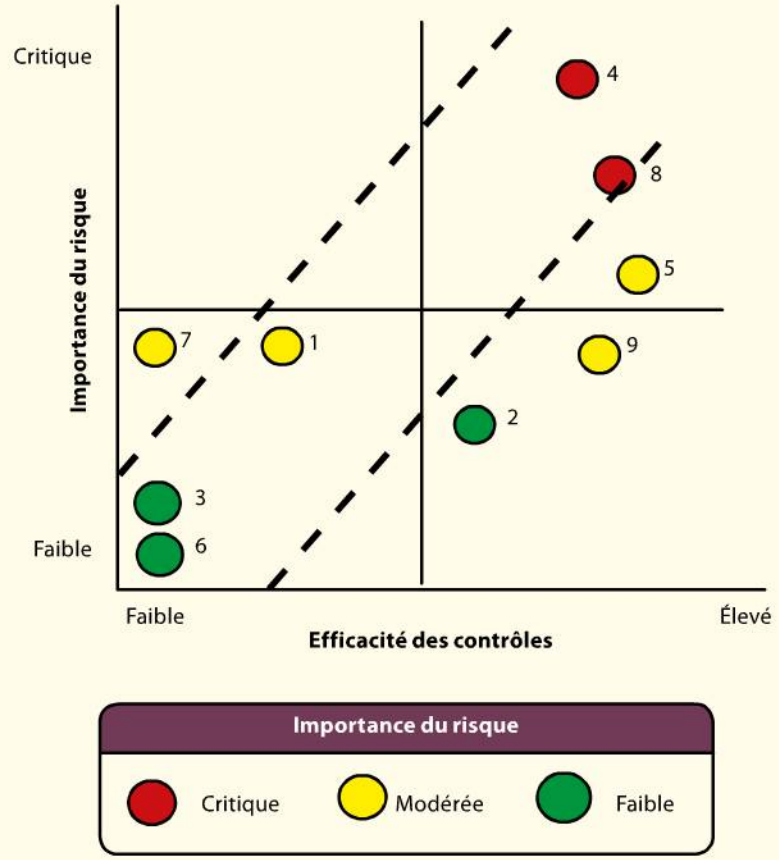
Externalisation de processus opérationnels

Transfert d'une partie des processus opérationnels d'une organisation à un prestataire extérieur, afin de réduire les coûts et d'accroître l'efficacité ou l'efficience de l'exploitation, tout en améliorant la qualité du service.

Copyright © 2015 Eyrolles.

ENCADRÉ 5-16

CARTOGRAPHIE PARTIELLE DES RISQUES POUR LE PROCESSUS 10 : « ARRIVER À L'HEURE AU COURS DE 8 H »



On peut certes externaliser des fonctions, mais il est crucial que le management et l'audit interne veillent à ce qu'un système de contrôle interne adéquat soit en place vis-à-vis du prestataire extérieur. Dans de nombreux cas, le système de contrôle externe peut être meilleur et plus efficient que si les processus restaient internes. Il existe toutefois de nouveaux risques, particulièrement dans la phase de transition pendant laquelle certaines fonctions sont externalisées ou au contraire réinternalisées. La liste qui suit présente quelques-unes des pratiques recommandées aux organisations pour une gestion des risques et un contrôle des processus opérationnels externalisés efficaces.

- Documenter le processus externalisé et indiquer quels contrôles clés ont été externalisés.
- Veiller à ce qu'une surveillance de l'efficacité du processus externalisé soit réalisée.

Copyright © 2015 Eyrolles.

- Obtenir l'assurance que les contrôles internes intégrés dans le processus externalisé fonctionnent de manière effective, soit *via* des audits internes de ces contrôles, soit par un examen externe de ces contrôles (comme un rapport SSAE 16 – *Statement on Standards for Attestation Engagements* – SOC 1 ou SOC 2 – *Service Organization Controls* – aux États-Unis).
- Vérifier régulièrement que l'externalisation du processus en question se justifie toujours.

ENCADRÉ 5-17

APPORTER SON POINT DE VUE SUR L'ANALYSE DES PROCESSUS ET DES RISQUES OPÉRATIONNELS
10 OPPORTUNITÉS POUR L'AUDIT INTERNE

- Identifier les domaines dans lesquels les processus font l'objet d'un contrôle excessif et dans lesquels les activités de contrôle peuvent être limitées pour être plus efficaces.
- Identifier les risques spécifiques dans les processus qui requièrent des contrôles supplémentaires ou pour lesquels les contrôles peuvent être réalisés plus efficacement.
- Identifier les domaines dans lesquels les indicateurs clés de performance peuvent être appliqués ou améliorés afin d'accroître la surveillance des processus opérationnels par le management.
- Aider le management à évaluer régulièrement la stratégie appliquée pour les processus opérationnels externalisés.
- Apporter un point de vue au management sur les contrôles et les opérations liés aux processus externalisés, et évaluer les prestataires dans le cadre de la *due diligence*.
- Faciliter la discussion sur les activités de management des risques de l'entreprise et de cartographie de l'assurance afin d'améliorer la compréhension de l'organisation concernant les risques et processus opérationnels clés, ainsi que leur rôle dans les divers outils utilisés par le management.
- Dans le cadre d'une réduction des effectifs ou d'un réalignement significatifs, expliquer au management en quoi l'impact sur les processus opérationnels majeurs est lié aux risques, aux contrôles et à l'efficacité.
- Évaluer les possibilités d'utiliser la technologie pour améliorer l'efficacité des processus opérationnels et les contrôles y afférents.
- Déterminer les possibilités de réaliser des analyses de données en se familiarisant davantage avec l'ensemble des processus opérationnels majeurs et en identifiant les principaux domaines dans lesquels il serait plus pertinent de les utiliser.
- Procéder à une revue des autres organisations du secteur afin d'identifier les meilleures pratiques pour réaliser les activités de l'organisation.

OPPORTUNITÉS POUR UN POINT DE VUE DE L'AUDIT INTERNE

Grâce à sa capacité à analyser les processus opérationnels et les risques associés, l'audit interne est en mesure d'apporter un point de vue à la direction générale et au management, ce qui lui permet de créer une valeur ajoutée significative pour l'organisation.

Copyright © 2015 Eyrolles.

Ces compétences ont été acquises au cours de travaux d'assurance sur la gestion des risques et le contrôle interne, effectués dans le cadre de missions d'assurance classiques ou spéciales comme des initiatives de refonte des processus opérationnels, des études d'externalisation ou de délocalisation, des revues de *due diligence* dans le cadre de fusions-acquisitions, ou encore des revues de systèmes avant leur mise en œuvre. L'encadré 5-17 présente 10 opportunités pour l'audit interne d'apporter son point de vue concernant les processus opérationnels et les risques associés.

RÉSUMÉ

Les processus opérationnels et les concepts de risques traités dans le présent chapitre forment la base nécessaire pour comprendre comment les organisations structurent leurs activités afin d'atteindre leurs objectifs. Premièrement, il est important de comprendre globalement ces processus, ainsi que la manière selon laquelle ils participent et contribuent à l'atteinte des objectifs. Ensuite, il convient d'identifier et d'évaluer les risques qui peuvent avoir une incidence sur la réalisation des objectifs. Enfin, les processus et sous-processus clés, qui sont conçus pour gérer les risques, conformément aux stratégies souhaitées, peuvent être identifiés comme des sujets potentiels pour des audits internes.

Cependant, ces concepts ne sont pas seulement destinés aux auditeurs internes. Ils peuvent constituer des outils fondamentaux et être utilisés par d'autres collaborateurs de l'organisation, voire au quotidien étayer la prise de décisions. Ces aspects ont été illustrés tout au long de ce chapitre à travers l'exemple de l'étudiant qui a pour objectif de devenir un auditeur interne. Veuillez vous reporter à l'annexe pour un autre exemple d'application de ces principes.

Copyright © 2015 Eyrolles.

ANNEXE

APPLICATION DES CONCEPTS : ÉVALUATION DES RISQUES POUR DES ORGANISATIONS ÉTUDIANTES

Les concepts présentés dans ce chapitre concernent non seulement les auditeurs internes mais également les managers et autres membres à différents niveaux de l'organisation. L'exemple suivant illustre ces concepts en introduisant une méthode que les membres et les responsables d'organisations étudiantes et citoyennes peuvent appliquer sans délai, afin de participer à la gestion des risques liés aux activités et aux événements de leur organisation. Cette méthode a été conçue par l'*Office of the Dean of Students* (bureau du directeur des études aux étudiants) de l'Université du Texas à Austin, mais s'appuie sur des pratiques analogues de gestion des risques dans plusieurs autres universités, organisations et entités publiques.

La méthode considérée inclut un processus en six étapes, que les administrateurs ou comités d'organisations étudiantes sont encouragés à mettre en œuvre pour planifier des événements (comme un concert ou une soirée) ou des activités (visite d'organisation dans une autre ville, tournoi sportif, etc.). Les étapes du processus sont les suivantes :

1. inventorier tous les aspects de l'événement/l'activité dans la partie 1 de la feuille de travail relative à la gestion des risques (encadré 5-A1) ;

2. identifier les risques associés à chaque événement/activité, en envisageant les risques potentiels de façon globale (encadré 5-A2) ;

3. utiliser la matrice (encadré 5-A3) pour déterminer le niveau de risque associé à chaque activité, avant de mettre en œuvre toute stratégie de gestion des risques, et documenter le niveau de risque dans l'encadré 5-A2 ;

4. organiser une séance de réflexion collective pour définir des méthodes de gestion des risques. Trouver des stratégies qui permettent de réduire l'impact et/ou la probabilité d'occurrence d'un risque majeur. Documenter ces stratégies dans l'encadré 5-A2 ;

5. utiliser la matrice (encadré 5-A3) pour réestimer les activités après avoir mis en œuvre les stratégies de gestion des risques, et documenter le nouveau niveau de risque dans l'encadré 5-A2.

6. déterminer si la mise en œuvre des stratégies de gestion des risques aboutit à un niveau de risque résiduel acceptable. Envisager de modifier ou d'éliminer les activités induisant des risques inacceptables. Ne pas oublier de prendre en compte la façon dont l'activité concernée s'articule avec la mission et l'objectif de l'organisation. Documenter les décisions prises dans l'encadré 5-A2.

L'encadré 5-A3 illustre la relation entre impact et probabilité. Il recourt à des échelles et à des définitions légèrement différentes, mais est identique, sur le plan conceptuel, aux autres modèles analysés dans ce chapitre.

Copyright © 2015 Eyrolles.

ANNEXE

Qu'il s'agisse d'une organisation étudiante ou d'une organisation multinationale, la réalisation de sa mission et de ses objectifs suppose de prendre des risques nécessaires. Dans l'environnement concurrentiel d'aujourd'hui, ceux qui gèrent le mieux le risque et qui se concentrent sur des processus opérationnels améliorés seront plus performants que leurs concurrents.

ENCADRÉ 5-A1

FEUILLE DE TRAVAIL RELATIVE À LA GESTION DES RISQUES, PARTIE 1

ÉTAPE 1 : INVENTORIER TOUS LES ASPECTS DE L'ÉVÉNEMENT
Nom de l'événement/l'activité.
De quoi s'agit-il (exemples : conduite, sports/loisirs, collecte de fonds, concerts, événements en extérieur, etc.) ?
Comment se déroule l'événement/l'activité ?
Objectif de l'événement/l'activité.
Quand se déroule l'événement/l'activité ?
Où se déroule l'événement/l'activité ?

Copyright © 2015 Eyrolles.

ENCADRÉ 5-A2

FEUILLE DE TRAVAIL RELATIVE À LA GESTION DES RISQUES, PARTIE 2

Étape 2 : identifier les risques	Étape 3 : déterminer le niveau de chaque risque	Étape 4 : élaborer des stratégies de gestion des risques	Étape 5 : réestimer l'activité en appliquant les stratégies de gestion des risques	Étape 6 : déterminer si la gestion des risques de l'organisation a été efficace
Utiliser les connaissances et l'expérience des dirigeants, des conseillers et des membres de l'organisation pour identifier les risques associés à l'événement ou l'activité.	Utiliser la matrice pour déterminer le niveau de risque associé à chaque activité, avant de mettre en œuvre toute stratégie de gestion des risques.	Utiliser les définitions du risque pour élaborer des stratégies appropriées.	Prendre en compte les mesures de maîtrise et rectifier les risques dans la matrice afin de déterminer s'il est possible de réduire le niveau de risque initial. Analyser le niveau de risque global en fonction de cette information.	Déterminer si les stratégies sélectionnées aboutissent à une gestion des risques appropriée. Si tel n'est pas le cas, revenir sur la réalisation de l'activité ou la modifier en utilisant le processus.
Risques liés aux aspects matériels.				
Risques liés aux aspects psychologiques.				
Risques liés aux aspects financiers.				
Risques liés à la réputation.				
Risques liés à l'environnement.				
Autres risques.				

Copyright © 2015 Eyrolles.

ANNEXE

ENCADRÉ 5-A3

MODÈLE DE RISQUES POUR LES ACTIVITÉS ET LES ORGANISATIONS ÉTUDIANTES

		Probabilité d'occurrence d'un problème				
Catégorie		Peu probable Peu susceptible de survenir.	Rare Peu susceptible de survenir, mais possible.	Occasionnelle Peut parfois survenir.	Probable Très susceptible de survenir au cours du temps.	Fréquente Susceptible de survenir dans l'immédiat ou à court terme.
Impact du risque	**Grave** Peut entraîner la mort.	M	E	E	EE	EE
	Critique Peut entraîner d'importants dégâts matériels/ blessures, de substantielles pertes financières et/ou mauvaises publicités pour l'organisation et/ou l'institution.	F	M	E	E	EE
	Marginal Peut entraîner de légers dégâts matériels/blessures, maladies, pertes financières et/ou mauvaises publicités pour l'organisation et/ou l'institution.	F	F	M	M	E
	Négligeable Le risque représente une menace minime pour la sécurité, la santé et le bien-être des participants.	F	F	F	F	M

EE	**Risque extrêmement élevé**	Les activités entrant dans cette catégorie induisent un niveau de risque inacceptable, notamment un risque de blessure grave ou critique. Les organisations doivent déterminer s'il leur faut éliminer ou modifier les activités dont le risque est encore quantifié comme « EE » après mise en œuvre de toutes les stratégies raisonnables de gestion des risques.
E	**Risque élevé**	Les activités entrant dans cette catégorie induisent un risque potentiellement grave. Il est conseillé de mettre en œuvre des stratégies de gestion offensives afin de réduire ce risque. Les organisations doivent réfléchir à des moyens de faire évoluer ou d'éliminer les risques inacceptables.
M	**Risque modéré**	Les activités entrant dans cette catégorie induisent un certain niveau de risque dont la survenue est peu probable. Les organisations doivent réfléchir à ce qu'elles peuvent faire pour gérer ce risque afin de prévenir ses effets négatifs.
F	**Risque faible**	Les activités entrant dans cette catégorie induisent un risque minime dont la survenue est peu probable. Les organisations peuvent continuer ces activités comme prévu.

Copyright © 2015 Eyrolles.

Questions de révision

1. Qu'est-ce qu'un processus opérationnel ? Que sont les processus opérationnels ?
2. Qu'est-ce qu'un projet et en quoi diffère-t-il d'un processus opérationnel ?
3. Quels sont les processus de supervision et processus support qui sont communs à la plupart des organisations ?
4. Quels sont les éléments composant le modèle économique d'une organisation ?
5. Quelle est la différence entre une approche descendante et une approche ascendante dans la compréhension des processus opérationnels ?
6. Comment une organisation détermine-t-elle les objectifs clés d'un processus opérationnel ?
7. Quelles sont les deux méthodes les plus courantes pour documenter des processus ? Décrivez-les.
8. Que sont les deux variables servant à évaluer les risques ?
9. Une fois l'évaluation des risques terminée, les risques doivent être reliés à deux éléments. Lesquels ?
10. Quelles sont les quatre modalités de traitement des risques qu'une organisation peut mettre en œuvre ?
11. Quelle est la différence entre un lien primaire et un lien secondaire ?
12. Comment l'approche reposant sur les facteurs de risque permet-elle d'identifier des domaines à haut risque dans une organisation ?
13. Quelles sont les deux catégories génériques de facteurs généralement utilisées lorsque l'on applique l'approche reposant sur les facteurs de risque ? Quels autres facteurs sont régulièrement pris en compte ?
14. Dans le cadre d'une mission d'assurance, une fois que les objectifs sont connus, quelles sont les trois premières étapes nécessaires pour identifier les tests à réaliser afin de déterminer si la gestion des risques est efficace ?
15. Quels sont les deux axes habituellement utilisés dans une cartographie de contrôle des risques ? Expliquez à quoi correspondent les deux lignes parallèles en pointillés dans l'encadré 5-16.
16. Quelles sont les pratiques recommandées aux organisations pour une gestion des risques et un contrôle des processus opérationnels externalisés efficaces ?

Copyright © 2015 Eyrolles.

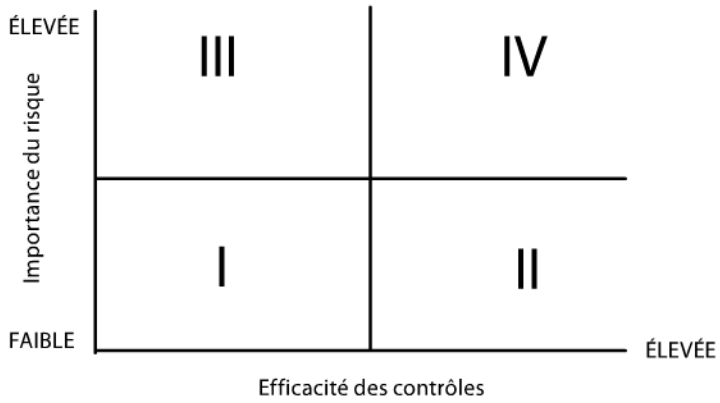
Questions à choix multiples

Sélectionnez la meilleure réponse pour chacune des questions suivantes.

1. Lors de l'évaluation du risque organisationnel dans une organisation de production, lequel des éléments suivants a l'impact durable le plus fort sur l'organisation ?
   a. Le budget publicitaire.
   b. Le calendrier de production.
   c. La politique relative aux stocks.
   d. La qualité des produits.

2. Il est fréquent que les auditeurs internes établissent des cartographies des processus et renvoient certaines parties de ces cartographies à des descriptions détaillées. Cette procédure permet :
   a. De déterminer la capacité des activités à produire des informations fiables.
   b. D'obtenir la compréhension nécessaire pour vérifier le processus.
   c. De documenter le fait que le processus atteint les normes d'audit interne.
   d. De déterminer si le processus répond aux objectifs fixés par le management.

Utilisez le graphique ci-après pour répondre aux questions 3 à 5.



3. Si un risque apparaît en bas à droite de la partie II de la cartographie de contrôle des risques ci-dessus, cela signifie que :
   a. Il existe un bon équilibre entre le risque et le contrôle.
   b. Les contrôles sont peut-être excessifs par rapport au risque.
   c. Les contrôles sont peut-être inadaptés par rapport au risque.
   d. Il n'y a pas suffisamment d'informations pour porter un jugement.

4. Si un risque apparaît au milieu de la partie IV de la cartographie de contrôle des risques ci-dessus, cela signifie que :
   a. Il existe un bon équilibre entre le risque et le contrôle.
   b. Les contrôles sont peut-être excessifs par rapport au risque.

Copyright © 2015 Eyrolles.

c. Les contrôles sont peut-être inadaptés par rapport au risque.
d. Il n'y a pas suffisamment d'informations pour porter un jugement.

5. Parmi les situations suivantes, laquelle inquiète le plus l'auditeur interne ?
   a. Un risque en bas à gauche de la partie I.
   b. Un risque en bas à droite de la partie II.
   c. Un risque en haut à gauche de la partie III.
   d. Un risque en haut à droite de la partie IV.

6. Parmi les éléments suivants : Lesquels sont des processus opérationnels ?
   I. La planification stratégique.
   II. L'examen et l'annulation de prêts non remboursés.
   III. La sauvegarde des actifs.
   IV. Le paiement des cotisations sociales aux organismes concernés.
   a. I et III.
   b. II et IV.
   c. I, II et IV
   d. I, II, III et IV.

7. Parmi les symboles suivants d'une cartographie des processus, lequel est le plus susceptible de contenir une question (un test alternatif) ?
   a. Le rectangle.
   b. Le losange.
   c. La flèche.
   d. L'ovale.

8. Une fois que les risques opérationnels ont été identifiés, ils doivent être évalués en fonction de :
   a. Leur impact et probabilité.
   b. Leur probabilité et risque.
   c. Leur importance relative et sévérité.
   d. Leur importance relative et l'efficacité des contrôles.

9. Dans une matrice risques/processus, un processus qui joue un rôle indirect dans la gestion des risques a :
   a. Un lien primaire.
   b. Un lien secondaire.
   c. Un lien indirect.
   d. Aucun lien.

Copyright © 2015 Eyrolles.

10. Une mise à jour majeure d'un important système d'information constitue très probablement :
    a. Un important facteur de risque externe.
    b. Un important facteur de risque interne.
    c. Un important facteur de risque autre.
    d. Une importante probabilité d'occurrence de problèmes systémiques.

11. Parmi les énoncés suivants, lequel s'applique à l'externalisation de processus opérationnels ?
    a. L'externalisation d'un processus opérationnel stratégique et à risque élevé réduit le risque opérationnel global.
    b. Les processus externalisés ne doivent pas être inclus dans l'univers d'audit interne.
    c. L'auditeur externe est tenu d'examiner tous les processus opérationnels importants qui sont externalisés.
    d. L'audit interne doit tester les contrôles, mis en place par le management, pour s'assurer que le prestataire extérieur respecte les normes de performance contractuelles.

Copyright © 2015 Eyrolles.

Thèmes de discussion

1. En quoi l'organisation des processus opérationnels d'une compagnie d'exploration et de production pétrolière diffère-t-elle de celle d'un groupe de grande distribution ?

2. Citez cinq des processus et risques opérationnels les plus importants pour un grand constructeur automobile tel que Toyota.

3. Si les ressources d'audit interne ne peuvent mener qu'un seul audit d'une division donnée, est-ce qu'un processus à haut risque audité l'an dernier dans cette division doit être audité, au lieu d'un processus moyennement risqué qui a été audité il y a quatre ans ? Développez.

4. Le processus d'achat a pour objectif d'obtenir les bons produits au bon prix et au bon moment. Quels sont les risques importants qui pèsent sur la réalisation de cet objectif ?

5. Réfléchissez au processus de vente et d'émission de tickets de caisse d'un magasin de vêtements que vous fréquentez.
   a. Quels sont les objectifs clés de ce processus ?
   b. Quels sont les principaux risques qui menacent la réalisation de ces objectifs ? Les principaux risques sont ceux qui présentent l'importance relative (c'est-à-dire la combinaison de l'impact et de la probabilité d'occurrence) la plus élevée.
   c. Identifiez et cartographiez les principales activités de ce processus dans l'ordre chronologique.
   d. Sur la base de votre examen des principales activités, quels sont les risques repérés ci-dessus qui ont l'importance sous-jacente la plus grande ?

6. Payswell, petite entreprise de production, existe depuis 10 ans. Sa direction générale envisage d'externaliser la paye.
   a. Citez trois objectifs importants d'un service de paye.
   b. Quels sont les principaux risques qui menacent la réalisation de ces objectifs ?
   c. Quels sont les avantages potentiels de l'externalisation de la paye ?
   d. Quels nouveaux risques pourraient apparaître si ce processus était externalisé ?
   e. Comment le management de Payswell doit-il :
   - Identifier les contrôles clés devant porter sur le processus externalisé ?
   - Déterminer si ces contrôles sont conçus de manière adéquate et fonctionnent de manière effective ?

Copyright © 2015 Eyrolles.

ÉTUDES DE CAS

CAS N° 1

Pizza Inc., une chaîne de pizzas à emporter ou livrées, constate une baisse de son chiffre d'affaires et un recul constant de sa part de marché alors même que ses produits sont appréciés. Sa stratégie est toujours restée la même : accroître sa part de marché en satisfaisant les clients. Le management a demandé à l'audit interne de l'aider à comprendre pourquoi les ventes du magasin, situé dans les quartiers résidentiels, diminuent et en quoi cette baisse pourrait être liée aux activités internes. Votre expérience de l'audit interne et l'observation directe des tâches exécutées dans le magasin en difficulté vous ont permis de recueillir les informations ci-dessous.

- En 20XX, la direction de Pizza Inc. a analysé cet emplacement avant d'y faire construire un magasin, afin de s'assurer que le profil démographique du quartier constituait l'environnement idéal. C'est ainsi que cette chaîne de pizzas s'est implantée à proximité d'une banlieue où résidaient principalement des revenus intermédiaires ou intermédiaires-supérieurs, dans des maisons comportant trois à quatre chambres. Malgré cet emplacement favorable, le magasin que vous êtes en train d'examiner continue d'afficher des marges brutes et d'exploitation inférieures à celles de ses concurrents locaux.

- La formation intégrée au terrain (sur le terrain) est la principale méthode utilisée par les managers pour expliquer aux collaborateurs la politique et les procédures de l'organisation. Cette politique et ces procédures sont détaillées, pour chaque processus clé, dans des documents disponibles, sur demande, auprès du chef d'équipe. Les collaborateurs, majoritairement des hommes (65 % de l'effectif total), âgés de 17 à 23 ans, n'ont que peu, voire aucune expérience professionnelle. L'absentéisme imprévu est élevé. Dans l'objectif de récompenser les personnes qui travaillent régulièrement, conformément au programme de production, les affectations des équipes à temps partiel changent souvent. L'année dernière, l'équipe d'audit interne a noté que le management faisait état d'un taux de rotation (*turnover*) annuel moyen de 18 %.

- Le chef d'équipe est chargé de veiller à ce que toutes les commandes soient exécutées dans les délais promis par la publicité, ce qui constitue depuis longtemps un avantage concurrentiel. Les livreurs sont tenus d'enregistrer sur le ticket de livraison l'heure à laquelle ils arrivent chez le client. Cette heure est comparée à celle figurant sur le ticket de commande afin de calculer le temps total écoulé. L'examen des tickets de livraison des six derniers mois indique que le délai de livraison de référence dans cette organisation, à savoir 25 minutes entre la passation de la commande et l'heure à laquelle le livreur sonne chez le client, est passé à une moyenne de 43,8 minutes. Depuis des mois, selon des rumeurs persistantes, il existe des paris sur la capacité d'un des livreurs à battre à chaque fois son record de lenteur de livraison.

Copyright © 2015 Eyrolles.

- La rapidité de livraison dépend également de la quantité de pizzas prêtes à un moment donné, ainsi que des conditions de circulation dans le quartier. Lors de l'embauche, il est tout d'abord vérifié que les livreurs n'ont pas commis d'infractions graves au Code de la route (comme la conduite en état d'ébriété). Le manager du magasin a affiché au mur une grande carte permettant aux livreurs de repérer leurs trajets. Les kilomètres parcourus étant remboursés au titre des frais d'utilisation d'un véhicule personnel, chaque livreur, à la fin de son temps de travail, remet un rapport kilométrique, qui indique son kilométrage initial et final. Le manager vérifie de manière aléatoire ces chiffres sur le compteur kilométrique du véhicule.

- La politique d'entreprise de Pizza Inc. impose à chaque magasin de se limiter à une zone de livraison d'environ huit kilomètres. Toutefois, une commande n'est jamais refusée. Les commandes par téléphone sont réalisées selon un schéma prévisible, tandis que celles passées sur place sont plus aléatoires et moins fréquentes. Les besoins en personnel, pour répondre à la charge de travail anticipée, sont planifiés une semaine à l'avance. Aux heures de pointe, la charge de travail moyenne est de 29 commandes prises par heure. Les commandes sont notées à la main sur des blocs-notes prénumérotés. Si une erreur est commise, le ticket de commande initial est jeté et un nouveau bon de commande est émis, afin d'éviter toute confusion. Les informations suivantes sont inscrites sur le ticket : la date, l'heure de l'appel (ou de la commande sur place), le nom, l'adresse, le numéro de téléphone, le type de pâte et la garniture souhaités. Des calculettes aident à établir le prix annoncé au client et noté sur le ticket de livraison. Les chefs d'équipe vérifient toutes les commandes pour s'assurer que ces informations sont complètes avant leur traitement.

- Les pizzaïolos doivent utiliser une quantité d'ingrédients précise pour un certain nombre de garnitures standard. Néanmoins, il arrive souvent que des commandes spéciales nécessitent des ingrédients supplémentaires par rapport à la recette standard. Des bols doseurs sont disponibles, mais votre équipe d'audit interne a noté, lors de précédentes missions, que ces collaborateurs, aux heures de pointe, « savent » en général la quantité d'ingrédients à utiliser. À la fin du temps de travail de l'équipe postée, le manager vérifie bacs et réfrigérateurs pour s'assurer que les stocks sont suffisants. Il y a plusieurs mois, le chef de l'équipe du soir a décidé qu'il fallait porter le nombre de réapprovisionnements nécessaires à quatre par semaine, au lieu de trois habituellement. La température des fours est surveillée de près, afin que les pizzas cuisent correctement. Les collaborateurs chargés de la cuisson se basent sur une horloge murale centrale pour minuter la cuisson. Des instructions de cuisson sont affichées pour chaque garniture standard, accompagnées de consignes à suivre si une pizza est trop cuite. En général, celle-ci sera proposée aux collaborateurs.

Copyright © 2015 Eyrolles.

- Tous les collaborateurs doivent faire en sorte que les pizzas cuites soient prédécoupées, emballées, étiquetées à la main pour livraison et confiées au livreur disponible (les livreurs travaillent selon le principe du premier entré, premier sorti).

Après examen des informations reçues de plusieurs sources extérieures, la consultation des documents de communication interne de Pizza Inc. décrivant la stratégie, la mission et la vision de cette organisation, votre équipe d'audit interne a considéré que la mise en relation des risques et des processus opérationnels aiderait le directeur général, le directeur financier et le directeur de l'exploitation à identifier les processus opérationnels critiques et les facteurs clés de réussite.

En votre qualité de chef de mission d'audit interne, vous avez décidé :

A. de repérer et d'inventorier les processus clés mis en œuvre par Pizza Inc. sur ses différents sites ;

B. de définir 10 risques opérationnels pour un site type et d'évaluer l'impact et la probabilité d'occurrence de ces risques ;

C. de relier les processus opérationnels aux risques opérationnels. De déterminer lesquels sont primaires et lesquels sont secondaires. De réaliser une matrice « risques/processus », (encadré 5-11) ;

D. de sélectionner un processus clé (que vous considérez comme étant critique pour la réussite d'un site). De créer une cartographie détaillée des activités ;

E. d'identifier les risques spécifiques associés aux activités composant le processus clé (c'est-à-dire le processus que vous avez sélectionné pour le cartographier). (Compléter la partie « risque » d'une matrice de risques et de contrôles, encadré 5-14) ;

F. de cartographier les risques identifiés, en fonction de leur impact et de leur probabilité d'occurrence. De réaliser une cartographie des risques, (encadré 5-15) ;

G. sur la base des données factuelles présentées ci-dessus, d'identifier les contrôles (actions actuelles du management) qui visent à maîtriser les risques identifiés, puis de les placer sur la matrice de risques et de contrôles dans la colonne présentant les modalités de traitement des risques (encadré 5-14) ;

H. de déterminer les techniques permettant d'évaluer l'efficacité des contrôles existants et de compléter la dernière colonne de la matrice de risques et de contrôles (encadré 5-14) ;

I. de produire des recommandations destinées à permettre la maîtrise des risques existants et à améliorer les performances, en vous fondant sur vos observations et sur votre opinion quant à l'efficacité potentielle des activités actuelles de traitement des risques inhérents au processus critique que vous avez sélectionné.

Copyright © 2015 Eyrolles.

CAS N° 2 Sélectionnez une organisation introduite en bourse depuis moins de cinq ans et procurez-vous le prospectus (généralement disponible sur le site Internet de l'organisation, accessible par celui de l'AMF, ou *via* EDGAR pour les sociétés cotées aux États-Unis, ou auprès d'autres services d'information).

A. Présentez la stratégie et le modèle économique de cette organisation.

B. Identifiez ses objectifs stratégiques.

C. Identifiez ses principaux risques.

D. Élaborez une matrice faisant apparaître les objectifs stratégiques sur l'axe des ordonnées et les risques critiques sur l'axe des abscisses. Pour chaque objectif, indiquez le principal risque correspondant.

E. Expliquez quel risque, à votre avis, l'audit interne doit considérer comme le plus prioritaire.

Copyright © 2015 Eyrolles.


Copyright © 2015 Eyrolles



CHAPITRE 6
LE CONTRÔLE INTERNE

Objectifs pédagogiques

- Comprendre ce que l'on entend par contrôle interne à travers l'analyse comparative de divers référentiels.
- Identifier les objectifs, les composantes et les principes d'un référentiel de contrôle interne efficace.
- Connaître les rôles et responsabilités des différents acteurs d'une organisation en matière de contrôle interne.
- Identifier les différents types de contrôles et leur modalité d'application optimale.
- Comprendre le processus d'évaluation du système de contrôle interne.

> *« Rares sont les activités qui sont plus importantes pour la réussite d'une organisation que son contrôle interne. L'audit interne apporte au management une réelle assurance que les contrôles adéquats sont en place, qu'ils sont mis en œuvre comme prévu, et que toute défaillance est analysée et corrigée rapidement. »*[1]

Chaque organisation se fixe des objectifs, et chaque organisation est exposée à des risques qui menacent la réalisation de ces objectifs. Dans ce chapitre, nous traitons des diverses composantes du système de contrôle interne que les organisations élaborent pour maîtriser et gérer ces risques. La lecture de ce chapitre explicite la signification du contrôle interne et permet d'identifier les différents cadres de référence y afférents. De plus, vous saurez repérer les composantes nécessaires pour que le système de contrôle interne soit conçu de manière adéquate et fonctionne de manière effective. Le contrôle interne relève de la responsabilité de tous les membres d'une organisation. Ce chapitre précise les rôles et responsabilités de chaque acteur au sein de l'organisation, y compris l'évaluation par le management du système de contrôle interne. Nous définissons ici, principalement, les rôles spécifiques de l'audit interne en termes d'évaluation du système de contrôle interne. Différents types d'activités de contrôle servent à maîtriser les multiples risques auxquels doit faire face une organisation. À la fin de ce chapitre, vous saurez les identifier, et utiliser chacun de manière appropriée. Enfin, ce chapitre présente une vue d'ensemble du processus d'évaluation du système de contrôle interne. Ce concept est étudié plus en détail dans les chapitres relatifs à la conduite des missions d'audit interne (chapitres 12 à 15), ainsi que dans les études de cas qui accompagnent le présent manuel.

Copyright © 2015 Eyrolles

ENCADRÉ 6-1

DISPOSITIONS DU CRIPP PERTINENTES RELATIVES AU CHAPITRE 6

Norme 2100 – Nature du travail
Norme 2130 – Contrôle
MPA 2130-1 : Évaluer la pertinence des processus de contrôle
Guide pratique d'audit des technologies de l'information (GTAG) 1 : Les contrôles des systèmes d'information, 2e édition

Cadre de référence (ou référentiel)

Ensemble de principes directeurs qui forment une matrice par rapport à laquelle les organisations peuvent évaluer une multitude de pratiques.

CADRES DE RÉFÉRENCE

Un cadre de référence (ou référentiel) est un ensemble de principes directeurs qui forment une matrice par rapport à laquelle les organisations peuvent évaluer une multitude de pratiques. Ces principes se composent de divers concepts, valeurs, hypothèses et pratiques dont le but est de fournir une référence pour évaluer une structure, un processus ou un environnement, ou encore un groupe de pratiques ou de procédures. Différents cadres de référence, spécifiques à la pratique de l'audit interne, sont utilisés pour évaluer l'adéquation de la conception et le fonctionnement effectif des contrôles.

L'IIA donne les orientations suivantes pour l'utilisation des cadres de référence : « En général, un cadre de référence fournit une structure schématique permettant de comprendre la relation entre un ensemble de connaissances et une ligne directrice. En tant que système cohérent, le cadre de référence permet d'uniformiser l'élaboration, l'interprétation, l'application des concepts et des méthodologies ainsi que les techniques utilisées dans un domaine ou une profession donnée. »[2]

Pour éviter toute confusion, il est important d'être attentif aux éléments qui distinguent les différents cadres de référence évoqués dans ce chapitre. Tous portent sur la maîtrise des risques et différents aspects du contrôle interne. Cependant, les cadres de référence qui se concentrent sur la seule dimension contrôle interne ont un périmètre plus étroit et sont de nature moins stratégique. Néanmoins, même si ce chapitre traite spécifiquement du contrôle interne, il serait incomplet s'il n'identifiait pas les cadres de référence mondialement reconnus relatifs à la gouvernance, à la gestion des risques et au contrôle interne, qui ont été développés ou ont évolué au fil du temps. Le chapitre 3, *La gouvernance,* traite de la hiérarchie entre gouvernance, gestion des risques et contrôle interne, et le chapitre 4, *La gestion des risques*, revient plus en détail sur le cadre de référence relatif au management des risques de l'entreprise élaboré par le *Committee of Sponsoring Organizations of the Treadway Commission* (COSO). L'encadré 6-2 présente ces référentiels.

Copyright © 2015 Eyrolles.

Les référentiels de contrôle interne

Même si tous les cadres de référence évoqués dans l'encadré 6-2 renferment des éléments de contrôle interne, ceux qui sont les plus reconnus au niveau mondial par le management, les comptables, les auditeurs externes et les professionnels de l'audit interne sont : *Le référentiel intégré de contrôle interne*, publié par le COSO en 1992 et actualisé en 2013, *Recommandations sur le contrôle* (souvent appelé Cadre CoCo), publié en 1995 par l'Institut canadien des comptables agréés (ICCA), *Internal Control: Revised Guide for Directors on the Combined Code* (connu sous le nom de rapport Turnbull), publié par le *Financial Reporting Council*, qui est paru pour la première fois en 1999 et a été actualisé en 2005, et,

ENCADRÉ 6-2

CADRES DE RÉFÉRENCE MONDIALEMENT RECONNUS

Référentiels de contrôle interne
La nouvelle pratique du contrôle interne (COSO), *Committee of Sponsoring Organizations of the Treadway Commission*, États-Unis, 1992, actualisé en 2013 sous le nom *Référentiel intégré de contrôle interne*
Recommandations sur le contrôle (CoCo), *The Canadian Institute of Chartered Accountants*, Canada, 1995
Internal Control: Revised Guide for Directors on the Combined Code (rapport Turnbull), *The Institute of Chartered Accountants, England and Wales, 2005*
Cadre de référence – Les dispositifs de gestion des risques et de contrôle interne, Autorité des marchés financiers, 2010
COBIT 5, IT Governance Institute, États-Unis, 2012
Cadres de référence de la gouvernance
Report of the Committee on the Financial Aspects of Corporate Governance (Cadbury), Angleterre, 1992
King Committee on Corporate Governance, Institute of Directors, Afrique du Sud, 2002, mise à jour 2010
Code de gouvernement d'entreprise des sociétés cotées, AFEP MEDEF, France, 1995, révisé en juin 2013
Cadres de référence relatifs au management des risques de l'entreprise
Australian/New Zealand Standard Risk Management (Australian Standard 4360), Joint Technical Committee OB / 7—Risk Management, Australie/Nouvelle-Zélande, 1995
Le management des risques de l'entreprise, Cadre de référence – Techniques d'application (COSO), *Committee of Sponsoring Organizations of the Treadway Commission*, États-Unis, 2004
Management du risque – Principes et lignes directrices (norme ISO 31000), Organisation internationale de normalisation (ISO), Suisse, 2009
Autres cadres qui font référence aux dispositifs de maîtrise des risques
Convergence internationale de la mesure et des normes de fonds propres (Accord de Bâle), Comité de Bâle sur le contrôle bancaire, 1988
Convergence internationale de la mesure et des normes de fonds propres – Dispositif révisé (Bâle II et III), Comité de Bâle sur le contrôle bancaire, 2005 et 2011
Orientations relatives au système de gouvernance [dans le cadre de l'application de la Directive 2009/138/CE du 25 novembre 2009 sur *l'accès aux activités de l'assurance et de la réassurance et leur exercice*], EIOPA, 2013

Copyright © 2015 Eyrolles.

en France, le cadre de référence de l'AMF, publié en 2007 sous l'égide de l'Autorité des marchés financiers et actualisé en 2010. Le COBIT, référentiel de contrôle interne des systèmes d'information (SI), présenté à l'encadré 6-2, est spécifiquement conçu pour donner des orientations sur l'élaboration et l'évaluation de la bonne gouvernance relative aux systèmes d'information. Il complète le COSO, le CoCo et le rapport Turnbull concernant les contrôles relatifs aux SI, mais ne constitue pas en tant que tel un cadre de référence complet de contrôle interne.

COMPARAISON DES RÉFÉRENTIELS DE CONTRÔLE INTERNE RECONNUS

	COSO	CoCo	Turnbull	AMF
Définition du contrôle interne	Processus mis en œuvre par le conseil, le management et les collaborateurs d'une entité afin d'obtenir une assurance raisonnable quant à la réalisation d'objectifs liés aux opérations, au reporting et à la conformité.	Les éléments d'une organisation qui soutiennent les personnes et offrent une assurance raisonnable quant à l'atteinte des objectifs de l'organisation dans les catégories suivantes : efficacité et efficience des opérations, fiabilité du reporting interne et externe, conformité aux lois et règlements, ainsi qu'aux règles internes.	Englobe les règles, processus, tâches, comportements et autres aspects d'une organisation qui offrent l'assurance raisonnable qu'ils en facilitent le fonctionnement efficace et efficient, lui permettent de réagir comme il se doit face aux risques majeurs portant sur l'activité, les opérations, les aspects financiers, la conformité, etc. afin de réaliser les objectifs de l'organisation relatifs à la sauvegarde des actifs, l'identification et la gestion du passif, la qualité du reporting, la conformité aux lois et règlements applicables.	Le contrôle interne est un dispositif de la société, défini et mis en œuvre sous sa responsabilité. Il comprend un ensemble de moyens, de comportements, de procédures et d'actions adaptés aux caractéristiques propres de chaque société qui : a. contribue à la maîtrise de ses activités, à l'efficacité de ses opérations et à l'utilisation efficiente de ses ressources, et b. doit lui permettre de prendre en compte de manière appropriée les risques significatifs, qu'ils soient opérationnels, financiers ou de conformité. Le dispositif vise plus particulièrement à assurer : a. la conformité aux lois et règlements b. l'application des instructions, et des orientations fixées par la Direction générale ou le Directoire, c. le bon fonctionnement des processus internes de la société, notamment ceux concourant à la sauvegarde des actifs, d. la fiabilité des informations financières. Le contrôle interne ne se limite donc pas à un ensemble de procédures ni aux seuls processus comptables et financiers.
Composantes du contrôle interne	Environnement de contrôle, évaluation des risques, activités de contrôle, information et communication, et pilotage.	Finalité, engagement, capacité, pilotage et apprentissage.	Activités de contrôle, processus d'information et de communication, pilotage, intégration dans les opérations de l'organisation, traitement du risque et des changements et reporting.	Organisation, diffusion en interne d'informations pertinentes et fiables, système visant à recenser, analyser les principaux risques, activités de contrôle appropriées, surveillance permanente.

ENCADRÉ 6-3

Il n'existe pas de différences fondamentales entre le COSO, le CoCo, le cadre de référence de l'AMF et le rapport Turnbull. Ils comportent tous des définitions présentant le contrôle interne comme un processus ou un dispositif qui apporte une assurance

Copyright © 2015 Eyrolles.

raisonnable quant à la réalisation des objectifs d'une organisation dans trois catégories : efficacité et efficience des opérations, fiabilité du reporting et conformité. Ces quatre cadres de référence s'accordent également sur la responsabilité du contrôle interne : ils l'attribuent non seulement au Conseil, à la direction générale et au management, mais aussi à chaque personne au sein de l'organisation. Ils rappellent également le rôle de l'audit interne qui contribue, par ses évaluations, à améliorer le contrôle interne. Malgré une désignation différente d'un cadre de référence à l'autre, leurs composantes sont assez similaires et peuvent être examinées d'après les termes figurant dans le COSO : environnement de contrôle, évaluation des risques, activités de contrôle, information et communication, et pilotage. L'encadré 6-3 présente une comparaison des quatre référentiels de contrôle interne, ainsi que la terminologie propre à chacun.

La loi Sarbanes-Oxley, votée aux États-Unis en 2002, fait reposer la responsabilité de la conception, de la gestion et du fonctionnement effectif du contrôle interne uniquement sur la direction générale, plus précisément sur le directeur général et le directeur financier. Conformément à cette législation, la *Securities and Exchange Commission* (SEC) impose au directeur général et au directeur financier des sociétés cotées de se prononcer sur l'adéquation de la conception et le fonctionnement effectif du contrôle interne relatif au reporting financier dans le cadre du dépôt annuel des états financiers auprès de la SEC, ainsi que de signaler, sur une base trimestrielle, tout changement substantiel apporté à ce contrôle le cas échéant. En particulier, la SEC demande des preuves de la conformité : « (…) le management doit fonder son évaluation [ou son opinion] de l'efficacité du contrôle interne relatif au reporting financier sur un référentiel de contrôle interne adapté et reconnu élaboré par un organisme ou un groupement qui a suivi des procédures établies, y compris une vaste diffusion du référentiel pour commentaires du public. »[3] L'encadré 6-4 détaille l'évaluation par la SEC des référentiels de contrôle interne appropriés.

CIRF

Contrôle interne relatif au reporting financier.

Commentaire du traducteur

La France, comme d'autres pays européens, s'est dotée d'un cadre législatif (Loi de Sécurité Financière – LSF – août 2003) comparable à la loi Sarbanes-Oxley, bien que moins contraignant, quant aux dispositifs à mettre en œuvre pour y satisfaire, et moins pénalisant pour les responsables qui y dérogeraient.

Selon l'article L.225-37 du Code de commerce, « dans les sociétés dont les titres financiers sont admis aux négociations sur un marché réglementé, le président du conseil d'administration rend compte, dans un rapport joint au rapport [de gestion] (…), des procédures de contrôle interne et de gestion des risques mises en place par la société, en détaillant notamment celles de ces procédures qui sont relatives à l'élaboration et au traitement de l'information comptable et financière pour les comptes sociaux et, le cas échéant, pour les comptes consolidés ».

Copyright © 2015 Eyrolles.

ENCADRÉ 6-4

LOI SARBANES-OXLEY DE 2002 SUR LA CONFORMITÉ

La *Securities and Exchange Commission* (SEC) des États-Unis mentionne spécifiquement le COSO comme exemple de référentiel permettant aux organisations de jauger leur système de contrôle interne afin d'en vérifier la conformité à la Section 404 de la loi Sarbanes-Oxley, qui régit toutes les entités, étrangères ou américaines, souhaitant accéder au marché des capitaux des États-Unis. La SEC reconnaît également le référentiel CoCo du Canada et le rapport Turnbull de l'Angleterre et du Pays de Galles comme des cadres de référence appropriés.

COSO

Le *Committee of Sponsoring Organizations of the Treadway Commission* est une organisation à but non lucratif du secteur privé dont l'objectif est d'améliorer la qualité du reporting financier par le truchement de l'éthique dans les affaires, l'efficacité du contrôle interne et la gouvernance.

D'après la SEC, « le cadre de référence du COSO satisfait à nos critères et peut servir pour l'évaluation annuelle du contrôle interne par le management et pour les obligations d'information à respecter par ce dernier. Cependant, les règles finales n'imposent pas l'utilisation d'un référentiel particulier, comme celui du COSO, car d'autres normes d'évaluation existent en dehors des États-Unis… »[4]. La SEC, dans la note de bas de page 67 de sa décision finale, cite spécifiquement les *Recommandations sur le contrôle*, et le rapport Turnbull, comme exemples d'autres cadres de référence appropriés. Outre les cadres de référence spécifiquement mentionnés, la SEC reconnaît que « … des référentiels autres que le COSO pourront à l'avenir être élaborés aux États-Unis, qui satisferont à l'intention du texte sans pour autant en amoindrir l'utilité pour les investisseurs. L'utilisation d'indicateurs standard disponibles dans le domaine public améliorera la qualité du rapport relatif au contrôle interne et facilitera la comparabilité des rapports d'organisations différentes. Le règlement final demande au rapport de la direction générale d'identifier le cadre d'évaluation utilisé par le management pour évaluer l'efficacité du contrôle interne de l'organisation relatif au reporting financier. En particulier, un cadre de référence approprié doit : être exempt de préjugés, permettre des mesures qualitatives et quantitatives raisonnablement cohérentes du contrôle interne, être suffisamment complet pour que les facteurs susceptibles de modifier une opinion relative à l'efficacité du contrôle interne d'une organisation ne soient pas omis et permettre une évaluation du contrôle interne relatif au reporting financier » (SEC final ruling 33-8238).[5]

De nombreuses organisations sont à même d'appliquer ces référentiels pour se conformer à la Section 404 de la loi Sarbanes-Oxley, même si elles supportent ce faisant des coûts imprévus substantiels. En revanche, les petites sociétés cotées (telles que définies dans l'encadré 6-5) ont eu du mal à se mettre en conformité à cause des coûts prohibitifs, ainsi que des autres difficultés propres aux petites organisations, notamment :

- obtenir des ressources suffisantes pour mettre en place une séparation des tâches adéquate ;

Copyright © 2015 Eyrolles.

- pallier la capacité du management à avoir de l'emprise sur la réalisation des activités, ce qui peut induire un risque important de contournement des processus dans l'intention de donner l'impression que les objectifs de performance ont été atteints [contournement de contrôles par le management] ;
- trouver des personnes possédant les compétences requises pour siéger efficacement au Conseil et dans ses comités ;
- recruter et fidéliser des collaborateurs possédant une expérience et des compétences suffisantes en matière d'opérations, de reporting, de conformité et dans d'autres disciplines ;
- faire en sorte que le management ne concentre pas toute son attention sur les activités opérationnelles et qu'il accorde suffisamment d'importance au contrôle interne ;
- maîtriser les systèmes d'information et mettre en place des contrôles informatiques généraux et des contrôles applicatifs appropriés avec des ressources techniques limitées.[6]

Commentaire du traducteur

En France, l'AMF a publié en 2010, à l'attention des valeurs moyennes et petites, un guide de mise en œuvre des dispositifs de gestion des risques et de contrôle interne.

Pour aider les organisations, notamment les petites sociétés cotées, à se conformer à la Section 404 de la loi Sarbanes-Oxley, le COSO a publié en 2013 le *Référentiel intégré de contrôle interne – Application au reporting financier externe*, qui vient compléter le référentiel

Publications complémentaires au Référentiel intégré de contrôle interne du COSO

– Contrôle interne relatif au reporting financier – Lignes directrices à l'intention des petites sociétés cotées *(Internal Control over Financial Reporting – Guidance for Smaller Public Companies)*.
– Lignes directrices pour le pilotage des systèmes de contrôle interne *(Guidance on Monitoring Internal Control Systems)*.
– Référentiel intégré de contrôle interne – Application au reporting financier externe *(Internal Control Over External Financial Reporting: A Compendium of Approaches and Examples)*.

ENCADRÉ 6-5

CARACTÉRISTIQUES DES PETITES ENTITÉS

Une grande variété d'entités peuvent être qualifiées de « petites ». Nombre d'entre elles possèdent les caractéristiques suivantes :

- des secteurs d'activités peu nombreux et, pour chacun d'entre eux, un nombre assez restreint de produits ;
- concentration du marketing par canal ou par secteur géographique ;
- rôle moteur du management qui détient des intérêts ou des droits de propriété importants ;
- nombre restreint d'échelons hiérarchiques avec des domaines de compétence étendus ;
- faible degré de complexité des systèmes de traitement des transactions ;
- effectif réduit de collaborateurs aux attributions souvent élargies ;
- capacité limitée à mettre en œuvre des ressources importantes, tant pour les postes opérationnels que pour les fonctions support comme le service juridique, la gestion des ressources humaines, la comptabilité et l'audit interne.

Copyright 2006, *Committee of Sponsoring Organizations of the Treadway Commission* (COSO). Reproduit avec l'aimable autorisation de l'AICPA agissant en qualité d'administrateur agréé pour le COSO.

Copyright © 2015 Eyrolles.

COSO. « La présente publication (…) est consacrée pour l'essentiel aux objectifs liés au reporting financier externe. Les objectifs liés au reporting financier externe couvrent l'établissement de rapports financiers destinés aux tiers, tels que :

- les états financiers destinés à un usage externe ;
- les autres rapports financiers externes établis à partir des livres ou des registres comptables et financiers de l'entité. »[7]

Conçu à l'origine pour aider les organisations de toute taille à se conformer à la Section 404 de la loi Sarbanes-Oxley grâce à un dispositif d'un bon rapport coût/efficacité, cet ouvrage présente en outre l'avantage de donner des orientations aux petites sociétés cotées pour l'application du référentiel COSO lorsqu'elles évaluent l'efficacité du contrôle interne relatif au reporting financier.

En outre, le référentiel COSO actualisé offre de plus amples informations sur l'utilisation du pilotage pour étayer les conclusions quant à l'efficacité du contrôle, et notamment celle du contrôle interne relatif au reporting financier, particulièrement important pour les petites sociétés cotées qui s'efforcent de se conformer à la Section 404 de la loi Sarbanes-Oxley. De même que pour les autres composantes du contrôle interne, le référentiel actualisé développe deux principes liés au pilotage (voir l'encadré 6-10 (*cf.* p. 6-24) pour une présentation des 17 principes) :

- l'organisation sélectionne, développe et réalise des évaluations continues et/ou ponctuelles pour s'assurer que les composantes du contrôle interne sont mises en place et fonctionnent (principe 16) ;[8]
- l'organisation évalue et communique les déficiences de contrôle interne en temps voulu aux responsables des mesures correctives, y compris, le cas échéant, à la direction générale et au Conseil (principe 17).[9]

La composante « Pilotage » du référentiel COSO actualisé est analysée plus en détail ultérieurement dans ce chapitre.

En raison de l'attention accrue portée par le public au contrôle interne, de nombreuses organisations ont élargi leur vision du contrôle interne à d'autres dimensions. Au-delà de la sphère financière, le COSO, le CoCo, le cadre de référence de l'AMF et le rapport Turnbull sont également utilisés pour évaluer l'ensemble du système de contrôle interne.

L'IIA reconnaît la contribution qu'apportent ces cadres de référence à la conception des contrôles, qui doivent désormais s'aligner sur les objectifs de l'organisation : « Le contrôle a longtemps *exclusivement* relevé de l'audit interne. Avec l'apparition de référentiels plus vastes, comme celui du COSO – le *Référentiel intégré de contrôle interne* – et les critères de contrôle de l'Institut canadien

Copyright © 2015 Eyrolles.

des comptables agréés (CoCo), l'auditeur interne ne s'est plus cantonné aux contrôles financiers et à la conformité pour s'intéresser aux contrôles du management et aux processus de gouvernance qui remédient aux risques organisationnels. Ces cadres de référence élargissent le spectre des contrôles traités par les auditeurs internes et alignent plus étroitement leurs activités de contrôle sur les objectifs et les principaux processus de création de valeur d'une organisation. »[10]

Comme déjà indiqué dans le présent chapitre, ces référentiels comportent des définitions analogues du contrôle interne qui décrivent un processus apportant une assurance raisonnable quant à la réalisation des objectifs d'une organisation dans trois catégories : opérations, reporting et conformité. Ces catégories sont désignées différemment d'un cadre de référence à l'autre, mais leurs composantes sont pour l'essentiel les mêmes. En conséquence, la suite de ce chapitre utilise le référentiel du COSO pour étudier plus en détail ces diverses composantes. En effet, ce référentiel rend compte des concepts présents dans les quatre référentiels.

Référentiels COSO, CoCo, Turnbull et cadre de référence de l'AMF

Référentiels utilisés par un nombre croissant d'organisations dans le but d'évaluer l'intégralité du système de contrôle interne, et pas uniquement le contrôle interne relatif au reporting financier.

DÉFINITION DU CONTRÔLE INTERNE

Le COSO définit le contrôle interne en ces termes :

> *« …un processus mis en œuvre par le Conseil, le management et les collaborateurs d'une entité, destiné à fournir une assurance raisonnable quant à la réalisation d'objectifs liés aux opérations, au reporting et à la conformité. Cette définition met l'accent sur les aspects suivants du contrôle interne :*

- *il est axé sur la réalisation d'objectifs relevant d'une ou plusieurs catégories qui se recoupent – objectifs liés aux opérations, au reporting et à la conformité ;*
- *il s'agit d'un processus qui repose sur la mise en œuvre de tâches et d'activités continues. Il constitue un moyen et non une fin en soi ;*
- *il est mis en œuvre par des personnes : il ne repose pas simplement sur un ensemble de règles et de manuels de procédures, de documents et de systèmes ; il est assuré par des personnes œuvrant à tous les niveaux de l'organisation ;*
- *il permet à la Direction générale et au conseil d'obtenir une assurance raisonnable, et non une assurance absolue ;*
- *il est adaptable à la structure de toute entité. Il offre une certaine souplesse d'application pour l'ensemble de l'entité ou une filiale, une division, une unité opérationnelle ou un processus métier en particulier. »*[11]

Contrôle interne (définition du COSO)

Processus mis en œuvre par le Conseil, le management et les collaborateurs de l'entité afin d'obtenir une assurance raisonnable quant à la réalisation d'objectifs liés aux opérations, au reporting et à la conformité.

Même si cette définition du contrôle interne peut sembler très générale, elle en envisage les différentes catégories individuellement ou

Copyright © 2015 Eyrolles.

ensemble. Lorsqu'on les considère ensemble, on parle de système de contrôle interne. D'après le COSO : « Cette définition est délibérément large pour deux raisons. Premièrement, elle rend compte des concepts fondamentaux sur lesquels reposent la conception, la mise en place et le pilotage du contrôle interne, ainsi que l'évaluation de son efficacité par les organisations. Elle fournit ainsi une base essentielle pour l'application du contrôle interne dans différents types d'organisations, secteurs d'activités ou zones géographiques. Deuxièmement, cette définition permet de gérer des sous-domaines de contrôle interne. »[12] Le COSO précise également : « En effet, ceux qui le souhaitent peuvent par exemple se focaliser sur le contrôle interne relatif au reporting ou à la conformité aux lois et règlements. De même, il est possible de se concentrer sur les contrôles visant des unités ou des activités spécifiques. »[13] Une organisation peut aussi choisir de se focaliser sur son système global de contrôle interne. L'encadré 6-7 présente les composantes du contrôle interne en mettant en évidence les relations qu'elles entretiennent les unes avec les autres.

Il convient de noter que si le COSO définit la réalisation des objectifs liés à la conformité au sens strict comme le « respect des lois et règlements applicables »[14], le Cadre de référence international des pratiques professionnelles de l'audit interne de l'IIA la définit plus généralement comme « l'adhésion aux règles, plans, procédures, lois, règlements, contrats ou autres exigences »[15]. Le COSO considère que la conformité et les autres obligations liées à la gouvernance font partie de la réalisation des objectifs liés aux opérations et non des objectifs liés à la conformité. La classification est beaucoup moins importante que la réalisation réelle des objectifs, quelle que soit la manière dont une organisation choisit de les classer. Cette distinction constitue toutefois un aspect important lorsque l'audit interne planifie une mission d'assurance et en détermine le périmètre. Pour une analyse détaillée de la mission d'assurance (planification, définition du périmètre et communications), voir le chapitre 12, *Introduction au processus d'audit*, le chapitre 13, *Le déroulement de la mission d'assurance*, et le chapitre 14, *La communication des résultats d'une mission d'assurance et les procédures de suivi.*

LES OBJECTIFS, LES COMPOSANTES ET LES PRINCIPES DU CONTRÔLE INTERNE

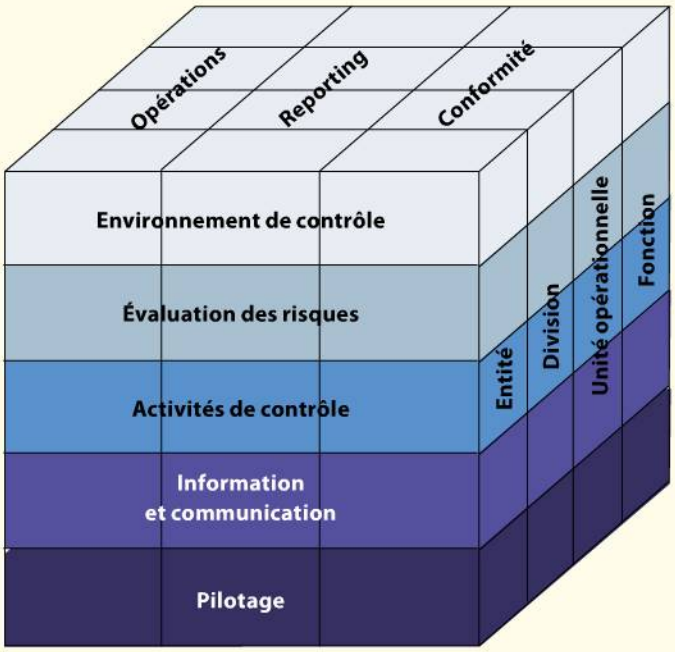
D'après le COSO : « Il existe un lien direct entre les *objectifs* que l'entité cherche à atteindre, les *composantes* [et principes] du contrôle interne nécessaires à leur réalisation, et la *structure de l'entité* (ses unités opérationnelles, ses entités juridiques, etc.). Ce lien est représenté dans le cube ci-après. »[16]

Le COSO énonce également dix-sept principes qui correspondent aux concepts fondamentaux associés aux cinq composantes intégrées du

Copyright © 2015 Eyrolles.

ENCADRÉ 6-6

LE CUBE DU COSO



Copyright 2013, *Committee of Sponsoring Organizations of the Treadway Commission* (COSO). Reproduit avec l'aimable autorisation de l'AICPA agissant en qualité d'administrateur agréé pour le COSO.

contrôle interne. Ces principes sont présentés dans l'encadré 6-10 et sont détaillés plus loin dans ce chapitre.

Objectifs

Le référentiel [COSO] établit trois catégories d'objectifs, ce qui permet aux organisations de prendre en compte différents aspects du contrôle interne :

- objectifs liés aux opérations – ils concernent l'efficacité et l'efficience des opérations. Il s'agit notamment des objectifs de performance opérationnelle et financière, ainsi que la sauvegarde des actifs ;
- objectifs liés au reporting – ils concernent le reporting interne et externe, financier et extra-financier. Ils peuvent englober la fiabilité, les délais, la transparence ou d'autres aspects demandés par les régulateurs, les organismes de normalisation ou les instructions internes ;
- objectifs liés à la conformité – ils concernent le respect des lois et règlements applicables.[17]

Les composantes du contrôle interne

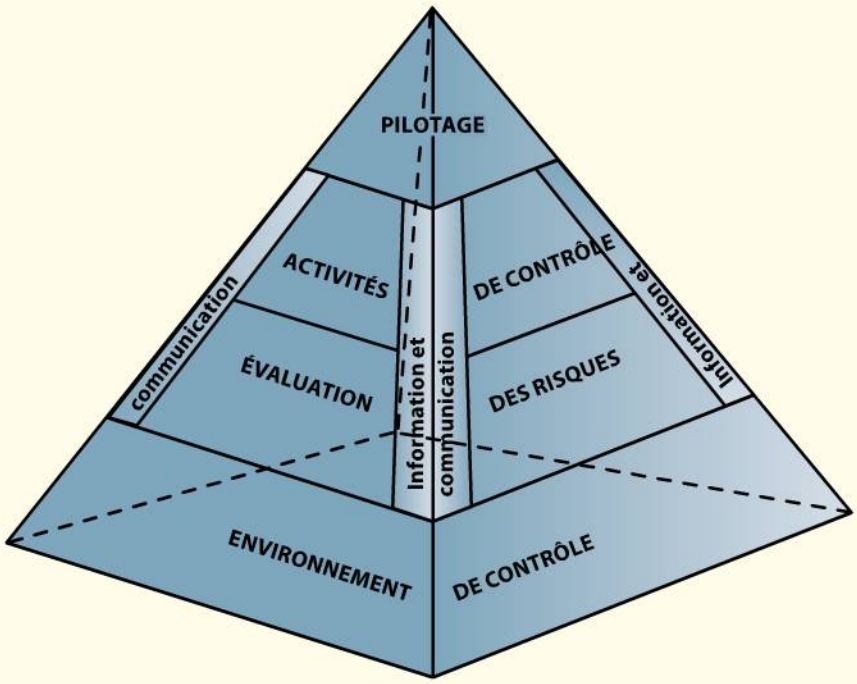
– Environnement de contrôle.
– Évaluation des risques.
– Activités de contrôle.
– Information et communication.
– Pilotage.

Copyright © 2015 Eyrolles.

Selon le COSO : « Un système de contrôle interne devrait fournir à une organisation un niveau d'assurance raisonnable quant à la réalisation des objectifs liés au reporting externe et à la conformité aux lois et règlements. La réalisation de ces objectifs, qui sont principalement fondés sur des lois, règlements et normes établis par les législateurs, les régulateurs et les organismes de normalisation, dépend de la façon dont sont conduites les activités relevant du périmètre de responsabilité de l'entité. En règle générale, le management et/ou le conseil auront plus de latitude pour définir les objectifs liés au reporting interne qui ne sont pas directement régis par les tiers. Néanmoins, l'organisation peut choisir d'aligner ses objectifs liés au reporting interne et externe afin que le reporting interne étaye mieux le reporting externe de l'entité. »[18]

ENCADRÉ 6-7

COMPOSANTES DU CONTRÔLE INTERNE



L'*environnement de contrôle* constitue le « milieu » dans lequel les personnes accomplissent leurs tâches et assument leurs responsabilités en matière de contrôle. Il sert de base pour les autres éléments du contrôle interne. Dans cet environnement, les dirigeants *évaluent les risques* susceptibles de mettre en cause la réalisation d'objectifs spécifiques. Les *activités de contrôle* sont mises en place pour permettre à la direction de s'assurer que ses directives visant à traiter ces risques ont été exécutées. Entre-temps, les *informations* pertinentes sont recueillies et *communiquées* à l'ensemble de l'organisation. Le processus complet fait l'objet d'un *pilotage* et de modifications le cas échéant.

Copyright 1992, *Committee of Sponsoring Organizations of the Treadway Commission* (COSO). Reproduit avec l'aimable autorisation de l'AICPA agissant en qualité d'administrateur des droits d'auteur pour le COSO.

Copyright © 2015 Eyrolles.

Composantes

Le COSO indique : « Pour atteindre ses objectifs, l'organisation peut s'appuyer sur cinq composantes du contrôle interne :

- environnement de contrôle ;
- évaluation des risques ;
- activités de contrôle ;
- information et communication ;
- pilotage.

Ces composantes du contrôle interne s'appliquent à l'échelle de l'entité, à ses filiales, ses divisions ou unités opérationnelles, ses fonctions ou à toute autre subdivision. »[19] Les composantes telles que définies par le COSO sont détaillées ci-dessous.

Environnement de contrôle

L'environnement de contrôle d'une organisation imprègne tous les services de l'organisation et influence la manière dont les personnes abordent le contrôle interne. Cette composante fondamentale du contrôle interne crée le contexte dans lequel existent les autres composantes du contrôle interne.

Pour le COSO : « L'environnement de contrôle est l'ensemble des normes, des processus et des structures qui constituent le socle de la mise en œuvre du contrôle interne dans toute l'organisation. Le conseil et la direction générale font preuve d'exemplarité en ce qui concerne l'importance du contrôle interne, et notamment les normes de conduite attendues. Le management répercute et précise ces attentes aux différents niveaux de l'organisation. L'environnement de contrôle englobe l'intégrité et les valeurs éthiques de l'organisation, les éléments permettant au conseil d'exercer ses responsabilités en matière de surveillance, la structure organisationnelle ainsi que l'attribution des pouvoirs et des responsabilités, le processus de recrutement, de formation et de fidélisation de personnes compétentes, et la robustesse des indicateurs, des mesures d'incitation et des gratifications favorisant le devoir de rendre compte de la performance. L'environnement de contrôle a un impact déterminant sur l'ensemble du système de contrôle interne. »[20]

L'histoire et la culture de l'organisation influent directement sur l'environnement de contrôle. Les objectifs de l'organisation sont atteints, en partie, grâce à l'environnement de contrôle qui, s'il est mis en œuvre efficacement, conduit à une culture d'entreprise qui valorise l'intégrité et met l'accent sur la sensibilisation au contrôle. Un tel environnement de contrôle se traduit généralement par l'exemplarité au plus haut niveau et par des règles et procédures appropriées, qui s'accompagnent souvent d'un code de conduite.

Facteurs clés de réussite

Succès qui conditionnent la réalisation des objectifs.

Copyright © 2015 Eyrolles.

Ces éléments favorisent l'adhésion aux valeurs de l'organisation et le travail en équipe pour la réalisation des objectifs.

Évaluation des risques

Toutes les organisations sont confrontées à des risques, c'est-à-dire à des menaces qui pèsent sur la réalisation de leurs objectifs. Tous les risques, externes et internes, doivent être évalués. D'après le COSO : « Toute entité est confrontée à une diversité de risques, provenant de sources externes et internes. Un risque est défini comme la possibilité qu'un événement survienne et ait un impact défavorable sur la réalisation des objectifs. L'évaluation des risques implique un processus dynamique et itératif d'identification et d'analyse des risques susceptibles d'affecter la réalisation des objectifs. Ces risques sont envisagés au regard des seuils de tolérance au risque. Pour déterminer la manière dont les risques seront gérés, il convient donc de commencer par les évaluer. Pour pouvoir procéder à cette évaluation, il est nécessaire d'avoir préalablement défini des objectifs cohérents aux différents niveaux de l'entité. Le management spécifie des objectifs liés aux opérations, au reporting et à la conformité avec suffisamment de clarté pour pouvoir identifier et analyser les risques susceptibles d'affecter la réalisation de ces objectifs. Le management tient également compte de la pertinence des objectifs pour l'entité. L'évaluation des risques nécessite par ailleurs que le management tienne compte de l'impact d'éventuelles évolutions dans l'environnement externe et dans son propre modèle économique, susceptibles de rendre le contrôle interne inefficace. »[21]

L'identification et l'analyse des risques, qui sont toutes deux importantes pour une évaluation efficace des risques, sont traitées de manière plus approfondie plus loin dans ce chapitre.

L'établissement d'objectifs clairs constitue la condition préalable à une identification des risques, à leur évaluation et à un traitement des risques efficaces. Il faut d'abord définir des objectifs dans l'optique de déterminer une stratégie, avant que le management puisse identifier les risques susceptibles d'empêcher la réalisation des objectifs et prendre les mesures nécessaires pour gérer ces risques. Comme l'explique le chapitre 4, *La gestion des risques*, la fixation des objectifs, l'identification des événements, l'évaluation des risques et le traitement des risques constituent des éléments clés du management des risques. En conséquence, la fixation des objectifs est une condition préalable du contrôle interne et facilite son efficience et sa pertinence.

Les processus permettant de fixer les objectifs peuvent être très structurés comme tout à fait informels. L'énoncé de la stratégie d'une organisation détermine souvent les objectifs à l'échelle de l'entité. Avec l'évaluation des forces, des faiblesses, des risques et des opportunités, les objectifs établissent un contexte permettant

Copyright © 2015 Eyrolles.

de définir la stratégie d'une organisation. Le plan stratégique qui en découle est, la plupart du temps, général.

Des objectifs plus spécifiques que les objectifs à l'échelle de l'entité sont définis à partir du plan stratégique général. Les objectifs à l'échelle de l'entité sont ensuite rattachés aux objectifs plus spécifiques qui ont été définis pour les différentes activités de l'organisation. Les objectifs spécifiques à chaque activité doivent s'aligner sur les objectifs à l'échelle de l'entité.

Il est important pour l'organisation de fixer les objectifs à l'échelle de l'entité et au niveau des processus afin qu'elle soit en mesure d'identifier les *facteurs clés de réussite* (les succès qui conditionnent la réalisation des objectifs). Ces facteurs clés de réussite sont présents à tous les niveaux d'une organisation et facilitent l'instauration de critères mesurables permettant d'évaluer les performances.

Activités de contrôle

Les activités de contrôle sont les mesures prises par la direction générale, le Conseil et d'autres parties afin de maîtriser le risque et d'accroître la probabilité que les objectifs et buts fixés seront atteints. Les managers planifient, organisent et dirigent la mise en œuvre de mesures suffisantes pour donner une assurance raisonnable que les objectifs et les buts seront atteints. Tout comme les facteurs clés de réussite décrits plus hauts, les activités de contrôle sont présentes à tous les niveaux de l'organisation. Et, comme les objectifs qu'elles sont censées permettre d'atteindre, les activités de contrôle peuvent être classées selon les trois catégories suivantes : opérations, reporting et conformité. Cependant, les activités de contrôle sont souvent conçues pour maîtriser des risques multiples qui peuvent menacer les objectifs dans plus d'une catégorie. N'oublions pas que la catégorie à laquelle appartient un contrôle importe moins que la capacité de ce dernier à maîtriser le ou les risques auxquels elle correspond.

Séparation des tâches

Répartition de certaines tâches incompatibles entre différentes personnes pour réduire le risque d'erreur ou d'action inappropriée d'une personne.

Chaque organisation dispose de son propre ensemble d'objectifs et de stratégies de mise en œuvre. Étant donné que chacune est gérée par des personnes différentes qui recourent à leur propre jugement dans des environnements opérationnels d'une complexité variable, il n'y a pas deux organisations présentant le même ensemble d'activités de contrôle, même si elles peuvent avoir instauré des stratégies très similaires. Les activités de contrôle jouent par conséquent un rôle vital dans la gestion d'une organisation, car elles veillent à ce que les différents risques propres à l'organisation soient maîtrisés, ce qui permet à l'organisation de réaliser ses objectifs.

Comme le COSO l'indique : « Les activités de contrôle sont réalisées à tous les niveaux de l'[organisation] et à divers stades des processus métier. Elles peuvent également être mises en œuvre par l'intermédiaire des systèmes d'information. Il peut s'agir de contrôles préventifs ou détectifs, incluant diverses activités manuelles et

Copyright © 2015 Eyrolles.

automatisées, comme des autorisations et des approbations, des vérifications, des rapprochements et des revues de performance opérationnelle. »[22]

En ce qui concerne les revues de performance opérationnelle, le COSO précise : « Les contrôles de supervision évaluent si les autres activités de contrôle des transactions ([à savoir] vérifications spécifiques, rapprochements, autorisations et approbations, contrôles des données permanentes et contrôles physiques) sont exhaustives, exactes et conformes aux règles et aux procédures. Le management fait généralement appel à son jugement pour sélectionner et développer les contrôles de supervision des transactions à haut risque. Par exemple, un superviseur peut examiner si les rapprochements effectués par un comptable sont conformes à la règle. Il peut s'agir d'un examen superficiel [activité de pilotage] (par exemple, vérifier si le tableur de rapprochement est renseigné), ou d'un examen plus approfondi [activité de contrôle] (par exemple, vérifier si des éléments de rapprochement ont été suivis et corrigés ou convenablement justifiés). »[23]

Plus loin, le COSO indique : « Pour déterminer si une activité relève du pilotage ou des activités de contrôle, les organisations doivent en examiner les caractéristiques sous-jacentes, en particulier si elle implique un certain niveau de revue à des fins de surveillance. Le classement des revues parmi les activités de contrôle ou parmi les activités de pilotage peut être une affaire de jugement. Par exemple, la finalité d'une activité de contrôle d'exhaustivité réalisée mensuellement serait de détecter et de corriger les erreurs, tandis qu'une activité de pilotage rechercherait les causes des erreurs et confierait au management le soin de corriger le processus afin de prévenir les erreurs futures. Plus simplement, une activité de contrôle répond à un risque spécifique, tandis qu'une activité de pilotage consiste à évaluer si les contrôles en place au sein de chacune des cinq composantes du contrôle interne fonctionnent comme prévu. »[24]

Néanmoins, il existe un concept fondamental commun à tous les contrôles, ce que le COSO définit comme *la séparation des tâches*. Celui-ci consiste à répartir ou discriminer les tâches liées à l'autorisation des transactions, au traitement de ces transactions et à l'accès physique aux actifs liés à ces transactions sous-jacentes.

Commentaire du traducteur

Par exemple, les tâches liées à l'autorisation d'achat d'une marchandise, celles liées à l'exécution de l'achat et enfin celles liées à la réception et au stockage de la marchandise doivent être séparées.

Lorsqu'il n'est pas possible de séparer des tâches, le management sélectionne et développe des activités de contrôle alternatives.

Copyright © 2015 Eyrolles.

La finalité première de la séparation des tâches (répartition de certaines tâches incompatibles) entre différentes personnes est la réduction du risque d'erreur ou d'action inappropriée de la part d'une personne.

Outre la séparation des tâches, de nombreuses activités de contrôle communément admises sont en place dans un système de contrôle interne bien conçu. Par exemple :

- les évaluations de la performance et les activités de suivi ;
- les autorisations (validations) ;
- les contrôles d'accès aux SI ;
- la documentation (rigoureuse et détaillée) ;
- les contrôles relatifs à l'accès physique ;
- les contrôles applicatifs des SI (entrées, traitements, sorties) ;
- les vérifications et rapprochements indépendants.

Information et communication

Une information de qualité doit être communiquée de façon appropriée. C'est en raison de l'interdépendance de ces deux notions que le COSO les regroupe. Des informations pertinentes, exactes et opportunes doivent être disponibles pour les personnes qui en ont besoin, à tous les niveaux d'une organisation, pour la faire fonctionner efficacement. L'information doit être au service des utilisateurs concernés, de sorte que ces derniers puissent assumer leurs responsabilités liées aux opérations, au reporting et à la conformité. En outre, la communication doit également être élargie à d'autres aspects importants, tels que les attentes et les responsabilités des personnes et des groupes. La communication avec les tiers est également importante et peut apporter des informations essentielles au fonctionnement des contrôles. Ces tiers sont, notamment, les clients, les fournisseurs, les prestataires de services, les régulateurs, les auditeurs externes et les actionnaires.

Il est particulièrement important de veiller à ce que l'information reste alignée sur les besoins de l'organisation pendant les périodes de changement. Il convient également de veiller à ce que cette information soit communiquée en temps opportun à toutes les parties intéressées.

Les organisations ont à leur disposition de nombreux moyens de communication. Les moyens matériels incluent les manuels, les notes d'information et les panneaux d'affichage situés dans les lieux où les personnes se réunissent. La communication peut également revêtir la forme de réunions en face à face ou se faire de manière électronique, *via* les courriels, les sites intranet, la vidéoconférence ou les panneaux d'affichage électroniques. La culture

Les actes en disent plus long que les paroles

Outre les moyens de communication matériels, électroniques et verbaux, les actions du management reflètent fortement les valeurs de l'organisation.

Copyright © 2015 Eyrolles.

de l'organisation, ainsi que le contenu de l'information à partager, déterminent la forme de communication optimale. Étant donné que les personnes accueillent, et traitent, l'information différemment, la plupart des organisations utilisent plusieurs outils pour que toutes les personnes traitent et comprennent l'information qui leur est apportée. Les actions du management reflètent fortement les valeurs de l'organisation, car les actes en disent plus long que les paroles.

À l'évidence, la culture d'une organisation joue un rôle important dans la manière dont cette dernière communique ses priorités. Généralement, les organisations qui ont mis en place une culture de l'intégrité et de la transparence ont plus de facilité à communiquer que les autres.

Pilotage

Pour rester fiables, les systèmes de contrôle interne doivent être pilotés. Comme l'indique le COSO, le pilotage consiste en des « évaluations continues, qui sont intégrées au cœur des processus métier à tous les niveaux de l'entité, [et qui] permettent de disposer d'informations en temps voulu. Les évaluations ponctuelles, réalisées périodiquement, varient généralement, en termes de périmètre et de fréquence, en fonction de l'évaluation des risques, de l'efficacité des évaluations continues et d'autres considérations d'ordre managérial. Les constats sont établis selon les critères définis par les régulateurs, les organismes de normalisation, le management et le conseil. Le cas échéant, les déficiences sont communiquées au management et au conseil. »[25] S'il ne fait pas partie des opérations quotidiennes de l'organisation, le pilotage s'effectue en même temps que ces opérations et en continu. Plus les procédures de supervision et de vérification sont solides et complètes, plus le management peut être assuré de l'efficacité avec laquelle ces procédures assureront la cohérence et la fiabilité des opérations en cours. Si les activités de pilotage sont efficaces, et les évaluations du risque précises et fiables, il est possible de réduire la fréquence des évaluations ponctuelles.

Le pilotage est plus efficace lorsque l'on met en œuvre une approche à plusieurs niveaux. Le premier niveau englobe les activités quotidiennes exécutées par la direction d'un secteur donné, comme décrit plus haut. Le deuxième niveau est constitué d'une évaluation ponctuelle distincte des évaluations non indépendantes de premier niveau (démarche d'auto-évaluation des contrôles par le management). Cette évaluation vise à donner l'assurance que toutes les déficiences existantes ont été identifiées et réglées en temps opportun. Le troisième niveau est une évaluation indépendante effectuée par un service ou une fonction extérieure, souvent l'audit interne, dans le but de valider les résultats (exactitude et fiabilité) de l'auto-évaluation, réalisée par le management, de l'efficacité des

Copyright © 2015 Eyrolles.

contrôles dans le secteur concerné. Si, comme indiqué ci-dessus, l'audit interne donne une assurance précieuse, dans la plupart des organisations, d'autres catégories de parties prenantes fournissent également une certaine forme d'assurance (les services chargés de l'environnement et de la sécurité, les acteurs de l'assurance qualité, les services de contrôle des transactions, etc.) soit directement au Conseil, soit par des communications aux membres de la direction générale chargés de donner une assurance au Conseil. Grâce à cette approche multiniveaux, l'organisation sait que le système de contrôle interne reste efficace et les déficiences du contrôle interne sont identifiées et éliminées en temps opportun. Cette stratégie est souvent désignée comme un modèle de « lignes de maîtrise multiples ». Le modèle des trois lignes de maîtrise est un exemple classique. Ce modèle est illustré et expliqué plus en détail dans le chapitre 3, *La gouvernance*.

Il est important de noter que les activités de pilotage se produisent dans chacune des cinq composantes du contrôle interne (environnement de contrôle, évaluation des risques, activités de contrôle, information/communication et pilotage), et non simplement comme un élément isolé. L'inclusion des activités de pilotage dans les processus exécutés lors des opérations quotidiennes de l'organisation permet au pilotage de s'effectuer sur une base régulière, et de saisir les problèmes avant qu'ils ne deviennent ingérables. Les évaluations ponctuelles ne présentent pas cet avantage parce qu'elles sont réalisées à une phase ultérieure du processus et parce qu'elles sont moins fréquentes. Ces évaluations procurent un aperçu supplémentaire du système de contrôle interne, repèrent les problèmes qui ont pu échapper au pilotage continu, et évaluent l'efficacité du pilotage continu intégré aux activités quotidiennes du secteur en question. Malgré les avantages divers de ces deux méthodes de pilotage, elles sont toutes deux nécessaires si l'on veut que le processus de pilotage soit solide. L'encadré 6-8 donne des exemples de différents types de pilotage.

Comme indiqué plus haut, la direction générale est la première responsable de l'efficacité du système de contrôle interne de l'organisation, y compris du pilotage. Lorsque certains contrôles relèvent de niveaux hiérarchiques supérieurs, la supervision traditionnelle devient plus délicate. Les activités de pilotage effectuées par les subordonnés sont nettement moins efficaces que celles réalisées par les supérieurs. Lorsque la direction générale exécute les contrôles, il peut être judicieux que d'autres membres de la direction générale pilotent ces contrôles. Lorsqu'il y a un risque de contournement des contrôles par la direction générale, il peut être nécessaire que ce soit le Conseil qui effectue le pilotage.

In fine, c'est le Conseil qui est chargé de vérifier que la direction générale a mis en place un système de contrôle interne efficace. Pour remplir cette mission, le Conseil doit bien comprendre les

Copyright © 2015 Eyrolles.

risques qui pèsent sur l'organisation, ainsi que la manière dont la direction générale maîtrise ces risques à un niveau acceptable.

Déficience (définition du COSO)

Une déficience peut correspondre à une insuffisance observée, potentielle ou réelle, ou représenter une opportunité de renforcer le système de contrôle interne, afin d'accroître la probabilité d'atteindre les objectifs de l'entité.

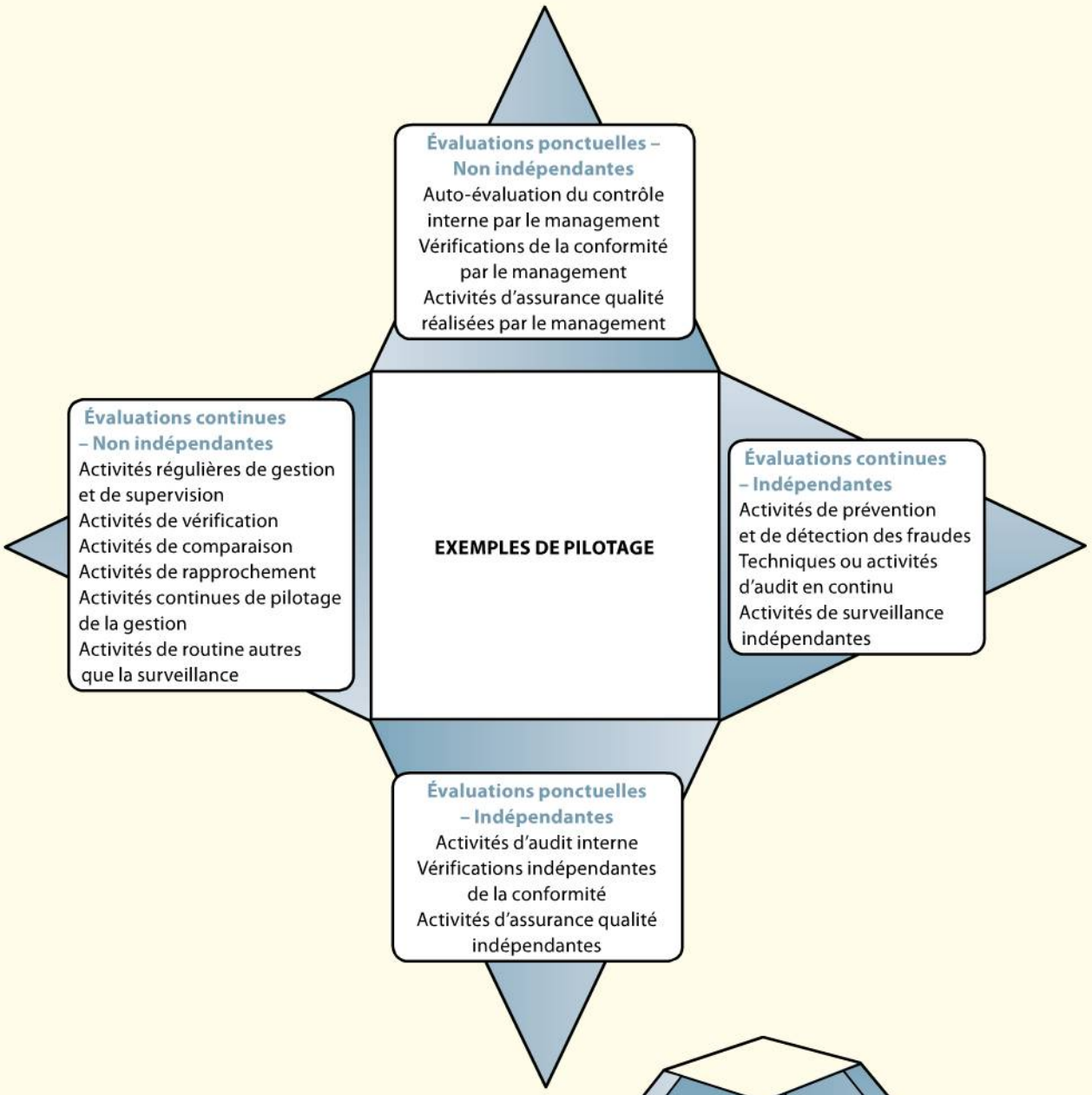
Les déficiences du contrôle interne d'une organisation peuvent être identifiées par le pilotage continu ou par des évaluations ponctuelles. Le COSO définit globalement une déficience comme « une insuffisance dans une composante ou un principe, qui réduit la probabilité que l'entité atteigne ses objectifs ». Plus précisément :

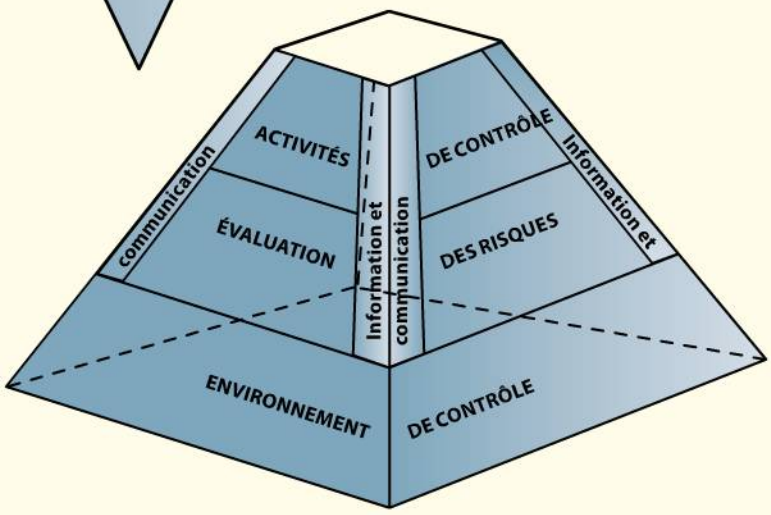
> *« Il existe de nombreuses sources potentielles pour identifier les déficiences du contrôle interne, parmi lesquelles les activités de pilotage, les autres composantes et les tiers qui fournissent des informations sur la mise en place et le fonctionnement des composantes et des principes.*
>
> *Une déficience du contrôle interne ou une combinaison de déficiences est qualifiée de « déficience majeure » lorsqu'elle réduit fortement la probabilité que l'entité atteigne ses objectifs. Une déficience majeure est un sous-ensemble des déficiences du contrôle interne. Ainsi, une déficience majeure est également une déficience du contrôle interne, par définition.*
>
> *Lorsqu'il détermine si les principes et les composantes sont mis en place et fonctionnent, et si ces dernières fonctionnent conjointement, et* in fine*, lorsqu'il conclut à l'efficacité du système de contrôle interne de l'entité, le management fait appel à son jugement pour évaluer la sévérité d'une déficience du contrôle interne, ou d'une combinaison de déficiences. En outre, l'espace laissé au jugement peut varier selon la catégorie d'objectifs.*
>
> *Les régulateurs, les organismes de normalisation et autres tiers concernés peuvent définir des critères pour déterminer la sévérité, évaluer et communiquer les déficiences du contrôle interne. Le Référentiel reconnaît et s'inscrit dans le cadre du mandat et de la responsabilité des tiers tels que prescrits par les lois, règlements et normes externes.*
>
> *Lorsque l'entité applique une loi, un règlement ou une norme externe, le management devrait utiliser uniquement les critères pertinents qui y sont inclus pour classer la sévérité des déficiences du contrôle interne, plutôt que de s'appuyer sur la classification du Référentiel. Toute déficience du contrôle interne qui se traduirait par une inefficacité du système de contrôle interne en regard de ces critères empêcherait le management de conclure que l'entité satisfait aux exigences d'un contrôle interne efficace conformément au Référentiel (par exemple, une non-conformité majeure concernant les objectifs liés aux opérations ou à la conformité, ou bien une faiblesse significative concernant les objectifs liés à la conformité ou au reporting externe). »*[26]

Les déficiences identifiées grâce au pilotage continu et aux évaluations ponctuelles doivent être communiquées rapidement aux parties concernées au sein de l'organisation. Selon son impact sur l'efficacité potentielle du système de contrôle interne, une déficience

Copyright © 2015 Eyrolles.

EXEMPLES D'ACTIVITÉS DE PILOTAGE





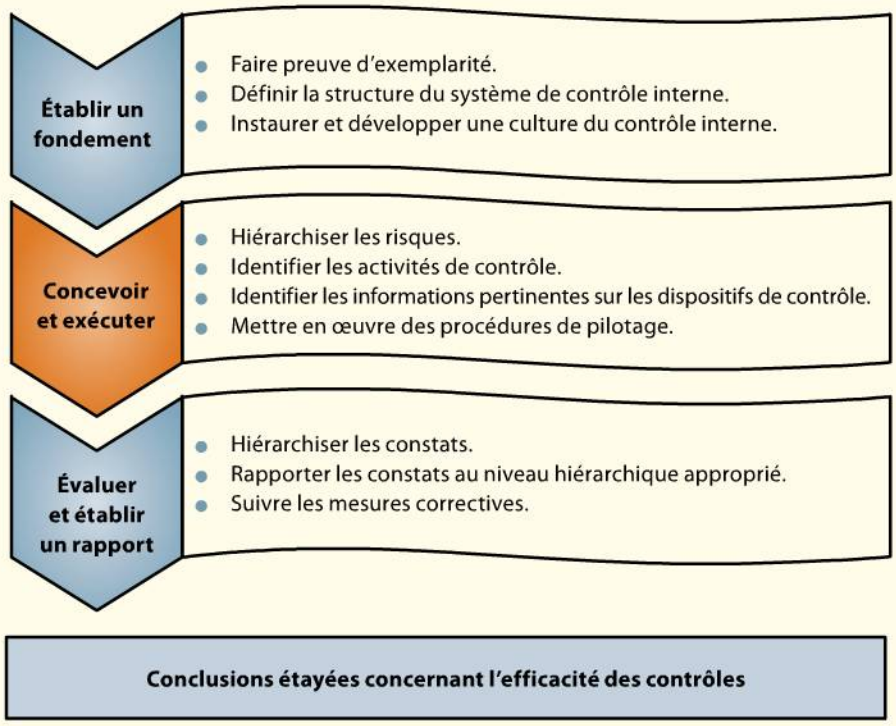
Copyright © 2015 Eyrolles.

devrait être signalée au management, à la direction générale et/ou au Conseil. Lors de l'évaluation du système de contrôle interne, il convient de tenir compte des déficiences signalées. Cette évaluation sera traitée en détail plus loin dans ce chapitre. Les communications formelles relatives aux missions d'assurance effectuées par l'audit interne sont détaillées dans le chapitre 14, *La communication des résultats d'une mission d'assurance et les procédures de suivi*.

Comme nous l'avons évoqué plus haut, certaines organisations sous-utilisent le pilotage, en particulier en ce qui concerne les obligations de reporting financier. Lorsqu'il est conçu dans ce but, le pilotage peut se révéler un outil efficace pour valider les critères de qualité du contrôle interne. Les organisations du monde entier qui doivent justifier aux tiers de l'efficacité de leurs systèmes de contrôle interne peuvent concevoir le type, le moment et le degré de pilotage qui est effectué pour étayer les critères selon lesquels le contrôle interne a fonctionné de manière effective à un moment donné et pendant une période particulière. L'encadré 6-9 décrit la représentation par le COSO du processus de pilotage visant à étayer les conclusions relatives à l'efficacité des contrôles.

ENCADRÉ 6-9

LE PROCESSUS DE PILOTAGE



Copyright 1992, *Committee of Sponsoring Organizations of the Treadway Commission* (COSO). Reproduit avec l'aimable autorisation de l'AICPA agissant en qualité d'administrateur des droits d'auteur pour le COSO.

Copyright © 2015 Eyrolles.

Principes fondamentaux

Le COSO énonce dix-sept principes qui correspondent aux concepts fondamentaux associés aux cinq composantes intégrées du contrôle interne : « Tous ces principes étant directement dérivés des différentes composantes, une entité peut mettre en œuvre un contrôle interne efficace en les appliquant tous. L'ensemble des principes s'applique aux objectifs liés aux opérations, au reporting et à la conformité. »[27] Les principes associés aux cinq composantes du contrôle interne sont énoncés dans l'encadré 6-10.

RÔLES ET RESPONSABILITÉS EN MATIÈRE DE CONTRÔLE INTERNE

Le contrôle interne relève de la responsabilité de tous les membres d'une organisation :

Management

Le directeur général assume la responsabilité ultime du système de contrôle interne. C'est lui qui fait preuve d'exemplarité en termes d'éthique et d'intégrité de l'organisation et qui transmet les valeurs à respecter aux cadres supérieurs, intermédiaires et à tous les membres d'une organisation. Le directeur général est plus ou moins visible et exerce une influence plus ou moins directe en fonction de la taille de l'organisation. Dans les organisations de petite taille, il a une incidence très directe sur le système de contrôle interne. Dans les organisations de grande taille, il exerce surtout une influence sur les cadres supérieurs qui, à leur tour, influent sur les subordonnés. De cette manière, les cadres supérieurs et intermédiaires agissent comme des « directeurs généraux » pour les domaines dont ils sont responsables.

Conseil

Le Conseil supervise la direction générale, donne des orientations sur le contrôle interne et, *in fine*, est chargé de vérifier la mise en place du système de contrôle interne. Le COSO définit des membres efficaces du Conseil comme « objectifs et compétents et [faisant] preuve de curiosité ». Ils doivent « posséder une connaissance solide concernant les activités et l'environnement de l'[organisation] et consacrer le temps nécessaire à leurs responsabilités ».[28] L'efficacité des membres du Conseil est indispensable à un système de contrôle interne efficace, car la direction générale a la capacité de contourner les contrôles et de faire disparaître les preuves en cas de comportement contraire à l'éthique ou de fraudes. Ce comportement a plus de chances d'être découvert ou empêché si le Conseil

Le directeur général

Il fait preuve d'exemplarité et instaure un environnement de contrôle favorable.

L'exemplarité au plus haut niveau

Les cadres supérieurs d'une organisation font preuve d'exemplarité de par leur intégrité et leur sensibilisation au contrôle dans l'ensemble d'une organisation.

Copyright © 2015 Eyrolles.

ENCADRÉ 6-10

17 PRINCIPES POUR UN CONTRÔLE INTERNE EFFICACE

Environnement de contrôle

- L'organisation démontre son engagement en faveur de l'intégrité et des valeurs éthiques.
- Le Conseil fait preuve d'indépendance vis-à-vis de la direction générale. Il surveille la mise en place et le bon fonctionnement du système de contrôle interne.
- La direction générale, agissant sous la surveillance du Conseil, définit les structures, les rattachements, ainsi que les pouvoirs et les responsabilités appropriés pour atteindre les objectifs.
- L'organisation démontre son engagement à attirer, former et fidéliser des personnes compétentes conformément aux objectifs.
- L'organisation instaure pour chacun un devoir de rendre compte de ses responsabilités en matière de contrôle interne afin d'atteindre les objectifs.

Évaluation des risques

- L'organisation définit des objectifs de façon suffisamment claire pour permettre l'identification et l'évaluation des risques susceptibles d'affecter leur réalisation.
- L'organisation identifie les risques susceptibles d'affecter la réalisation de ses objectifs dans l'ensemble de son périmètre et procède à leur analyse de façon à déterminer comment ils doivent être gérés.
- L'organisation intègre le risque de fraude dans son évaluation des risques susceptibles d'affecter la réalisation des objectifs.
- L'organisation identifie et évalue les changements qui pourraient avoir un impact significatif sur le système de contrôle interne.

Activités de contrôle

- L'organisation sélectionne et développe des activités de contrôle qui visent à maîtriser et à ramener à un niveau acceptable les risques susceptibles d'affecter la réalisation des objectifs.
- L'organisation sélectionne et développe des contrôles généraux informatiques pour faciliter la réalisation des objectifs.
- L'organisation déploie les activités de contrôle par le biais de règles qui précisent les objectifs, et de procédures qui permettent de mettre en œuvre ces règles.

Information et communication

- L'organisation obtient, produit et utilise des informations pertinentes et de qualité pour faciliter le fonctionnement du contrôle interne.
- L'organisation communique en interne l'information nécessaire au bon fonctionnement du contrôle interne, notamment les informations relatives aux objectifs et aux responsabilités du contrôle interne.
- L'organisation communique aux tiers les éléments qui peuvent affecter le fonctionnement du contrôle interne.

Pilotage

- L'organisation sélectionne, développe et réalise des évaluations continues et/ou ponctuelles pour s'assurer que les composantes du contrôle interne sont mises en place et fonctionnent.
- L'organisation évalue et communique les déficiences de contrôle interne en temps voulu aux responsables des mesures correctives, y compris, le cas échéant, à la direction générale et au Conseil.

est activement engagé. Comme expliqué précédemment, le Conseil est l'ultime responsable de la mise en place par la direction générale d'un système de contrôle interne efficace.

Copyright © 2015 Eyrolles.

Les rôles et responsabilités du Conseil tels que décrits par le COSO déterminent la gouvernance d'une organisation. Pour une illustration de ce processus, voir l'encadré 3-3 du chapitre 3, *La gouvernance*. Le chapitre 3 décrit la gouvernance comme le processus piloté par le Conseil qui consiste à autoriser, diriger et surveiller les activités de la direction générale en vue de réaliser les objectifs de l'organisation.

Auditeurs internes

Si le management, avec à sa tête le directeur général, est l'ultime responsable de la conception adéquate et du fonctionnement efficace du système de contrôle interne, les auditeurs internes n'en jouent pas moins un rôle de premier plan. En effet, ils vérifient que le management a bien assumé ses responsabilités. Le management effectue des évaluations continues du système de contrôle interne. Par son évaluation indépendante, l'audit interne apporte une assurance raisonnable sur l'adéquation de la conception et le fonctionnement effectif du système de contrôle interne, ce qui accroît la probabilité que les objectifs et buts de l'organisation seront atteints. Le référentiel du COSO définit le rôle de l'auditeur interne de manière analogue, bien que plus générale : « Les auditeurs internes [...] fournissent au management une assurance et des avis en matière de contrôle interne. [...] [La fonction] d'audit interne comprend l'évaluation de la pertinence et de l'efficacité des contrôles, en réponse aux risques, dans le cadre des processus de surveillance, des opérations et des systèmes d'information de l'organisation. »[29] De plus, « en règle générale, le domaine d'intervention des auditeurs internes devrait inclure la gouvernance, la gestion des risques et le contrôle interne, ainsi que la fourniture d'une assistance à l'organisation dans la mise en place d'un contrôle efficace. Cette assistance revêt la forme d'une évaluation de l'efficacité et de l'efficience du système de contrôle et de propositions visant à l'améliorer continuellement. L'audit interne communique ses constats et interagit directement avec le management, le comité d'audit et/ou le conseil. »[30] En raison de sa position au sein de l'entité et des pouvoirs dont il est investi, l'audit interne contribue de façon très importante au pilotage. La relation entre le management et l'audit interne dans l'évaluation du système de contrôle interne et de remontée de l'information à cet égard est analysée en détail plus loin dans ce chapitre ainsi que dans le chapitre 9, *La gestion de l'audit interne.*

Collaborateurs

Le COSO indique clairement que le contrôle interne relève de la responsabilité de tous les membres d'une organisation : « Le contrôle interne relève de la responsabilité de tous les membres

Copyright © 2015 Eyrolles.

de l'entité et figure par conséquent, de façon explicite ou implicite, dans la description de poste de chaque collaborateur. Les collaborateurs opérationnels constituent la première ligne de défense en matière de mise en œuvre du contrôle interne. »[31] En principe, tous les collaborateurs produisent des informations utilisées par le système de contrôle interne ou accomplissent des tâches nécessaires pour assurer le contrôle. Le COSO précise aussi clairement que toutes les personnes associées partagent la responsabilité de communiquer au management ou à d'autres instances pertinentes les problèmes liés aux opérations, au non-respect du code de conduite, ou toute violation des normes de l'organisation ou acte illégal.

Le COSO souligne par ailleurs que des personnes extérieures à l'organisation contribuent à la réalisation de ses objectifs. Bien qu'ils ne soient pas responsables du système de contrôle interne de l'organisation, les auditeurs externes y contribuent en apportant un point de vue indépendant et objectif, par l'examen des états financiers et de l'efficacité du contrôle interne relatif au reporting financier. D'autres tiers, tels que le législateur, les autorités de régulation et de supervision, les clients et autres relations d'affaires, les analystes financiers, les agences de notation et la presse, sont également susceptibles de fournir des informations pertinentes sur le contrôle interne.

Dans de nombreux cas, des prestataires extérieurs se chargent de certains éléments du système de contrôle interne. Cependant, la propriété ou le devoir de rendre compte des éléments externalisés relève alors toujours du management qui exerce l'ultime responsabilité sur les tests et la certification des contrôles clés externalisés. Parmi les exemples figurent le traitement des données, la paye et même l'audit interne. L'externalisation des processus opérationnels est expliquée plus en détail dans le chapitre 5, *Les processus et les risques*.

LIMITES DU CONTRÔLE INTERNE

Assurance raisonnable

Niveau d'assurance étayé par des procédures et des jugements d'audit généralement acceptés.

Le contrôle interne vise à maîtriser les risques qui menacent la réalisation des objectifs d'une organisation ou à permettre à une organisation de saisir des opportunités. Même si la direction générale, le Conseil, les auditeurs internes, le management et les collaborateurs travaillent ensemble à l'efficacité du contrôle interne, aucun système de contrôle interne ne peut garantir que les objectifs seront atteints. Cela tient aux limites inhérentes au contrôle interne. En particulier, selon le COSO : « Il est admis […] que, si le contrôle interne fournit une assurance raisonnable que les objectifs de l'entité seront atteints, il comporte des limites. Le contrôle interne ne peut éviter des jugements erronés ou de mauvaises décisions, ou bien encore des événements externes qui peuvent empêcher l'atteinte des objectifs opérationnels. En d'autres termes, un

Copyright © 2015 Eyrolles.

système de contrôle interne, même efficace, peut s'avérer défaillant. Ces limites peuvent résulter des facteurs suivants :

- la pertinence des objectifs fixés comme préalable au contrôle interne ;
- le fait que des décisions peuvent être prises en se fondant sur un jugement erroné ou biaisé ;
- des dysfonctionnements provoqués par des défaillances humaines telles que de simples erreurs ;
- la capacité du management à contourner les dispositifs de contrôle interne ;
- la capacité du management, des collaborateurs et/ou des tiers à contourner les contrôles par le biais d'une collusion ;
- les événements externes échappant au contrôle de l'organisation. »[32]

Si un système de contrôle interne bien conçu peut apporter une assurance raisonnable au management concernant la réalisation des objectifs de l'organisation, aucun système de contrôle interne ne peut apporter d'assurance absolue pour les raisons indiquées ci-dessus. Cela se vérifie quelle que soit la catégorie dans laquelle se classent les objectifs (opérations, reporting financier ou conformité). Comme nous l'avons déjà expliqué, la fixation d'objectifs est une condition préalable à la conception d'un système de contrôle interne efficace. Les objectifs constituent les cibles mesurables en vue desquelles une organisation mène ses opérations. Pour comprendre les concepts de limites inhérentes et d'assurance raisonnable, il faut également comprendre les liens et les interdépendances des objectifs et des risques qui affectent directement ou indirectement la capacité d'une organisation à atteindre ses objectifs. Ce n'est qu'alors qu'une organisation pourra concevoir et mettre en place un système efficace de contrôle interne.

Risque inhérent, risque maîtrisable et risque résiduel

La capacité d'une organisation à atteindre les objectifs qu'elle s'est fixés dépend de facteurs de risque internes et externes. La combinaison de ces facteurs de risque internes et externes à leur état d'origine, en l'absence de contrôle, est ce que l'on appelle le risque inhérent. Autrement dit, le risque inhérent correspond au risque brut s'il n'existe aucun dispositif de contrôle interne. Les limites inhérentes dépendent de la reconnaissance de l'existence du risque inhérent et du fait que certains événements ou situations sortent simplement du cadre de contrôle du management (facteurs de risque externes).

L'identification des facteurs internes et externes qui contribuent au risque à l'échelle d'une entité et au niveau d'une activité (processus et transaction) est essentielle pour l'évaluation du risque réel.

Copyright © 2015 Eyrolles.

Limites inhérentes au contrôle interne

Limitations qui concernent les limites inhérentes au jugement humain, les contraintes en matière de ressources, la nécessité d'étudier le ratio coût/bénéfice des contrôles, le fait que des dysfonctionnements soient plausibles, et l'éventualité d'un contournement des contrôles par le management ou d'une collusion.

Comme l'explique le chapitre 5, *Les processus et les risques*, une fois que les principaux risques ont été identifiés, le management peut évaluer leur importance et, si possible, relier les facteurs de risque aux objectifs et opérations y afférentes.

Il est nécessaire de procéder à une analyse des risques, en termes d'impact et de probabilité, une fois que ceux-ci ont été identifiés à la fois à l'échelle de l'entité et de chaque activité. Cette analyse dépend de nombreux facteurs propres à une organisation, mais porte généralement sur les aspects suivants :

- évaluation de l'importance du risque (sévérité ou impact) ;
- évaluation de la probabilité (ou fréquence) d'occurrence du risque ;
- prise en compte de la façon de gérer le risque, c'est-à-dire évaluation des mesures à prendre.

Les résultats de l'analyse des risques permettent au management de réfléchir à la meilleure manière de réagir face aux risques qui menacent la réalisation des objectifs de l'organisation. Les risques qui ne sont pas significatifs, c'est-à-dire ceux qui ont une faible probabilité d'occurrence et un faible impact, recevront une attention limitée. Les risques qui sont significatifs recevront une plus grande attention. Les risques de type intermédiaire nécessitent généralement une analyse plus approfondie, compte tenu de la part de jugement pour maîtriser ces risques de manière efficiente.

Risque inhérent

Combinaison de facteurs de risque internes et externes à leur état d'origine, en l'absence de contrôle, ou risque brut s'il n'existe aucun dispositif de contrôle interne.

Les contrôles sont les modalités de traitement des risques que prend le management pour réduire l'impact et/ou la probabilité de menaces à la réalisation des objectifs. Le management doit tenir compte de l'appétence pour le risque et des différents seuils de tolérance au risque définis par l'organisation lorsqu'il décide des mesures à prendre. L'ouvrage du COSO intitulé *Enterprise Risk Management – Integrated Framework* (« Le management des risques de l'entreprise, Cadre de référence – Techniques d'application ») définit l'appétence pour le risque comme le « niveau de risque qu'une organisation est prête à accepter dans le cadre de sa mission (ou de sa vision) », et la tolérance au risque comme « le niveau [d'intensité et] de variation acceptable dans l'atteinte d'un objectif ».[33] La tolérance au risque doit être conforme à l'appétence pour le risque.

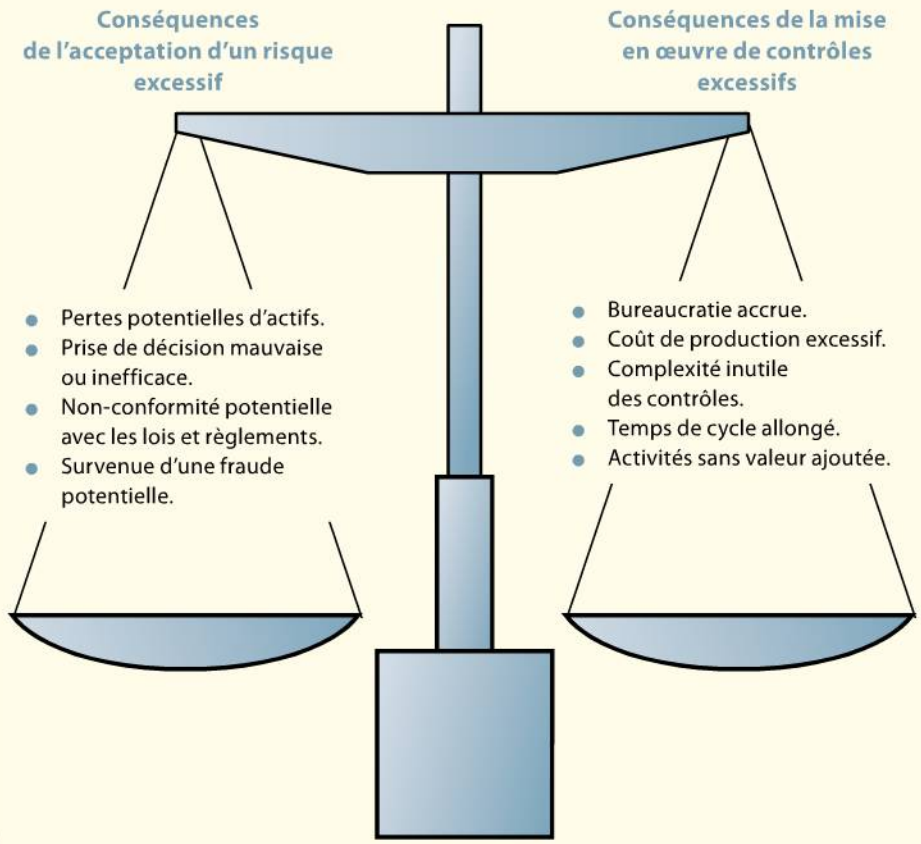
De plus, la tolérance au risque tient compte du niveau de risque que le management accepte consciemment après avoir évalué les coûts et les avantages de la mise en œuvre des contrôles. Il importe de reconnaître l'existence d'une relation directe entre le niveau de maîtrise du risque et le coût associé à la mise en œuvre des activités de contrôle conçues pour arriver à cette réduction des risques. Par conséquent, une organisation doit faire en sorte de n'avoir ni un risque excessif ni des contrôles excessifs. L'encadré 6-11 énumère

Copyright © 2015 Eyrolles.

certaines conséquences possibles de ces deux situations. Du fait des arbitrages à faire, l'organisation acceptera un niveau de risque plus ou moins élevé, en fonction de la nature du risque, de la réglementation en vigueur et de la philosophie du management.

ENCADRÉ 6-11

ÉQUILIBRAGE DES RISQUES ET DES CONTRÔLES



Cela étant, le management doit tenir compte de nombreux facteurs lorsqu'il détermine les mesures spécifiques qu'il devrait mettre en place pour maintenir le risque inhérent à un niveau suffisamment faible dans le cadre de la tolérance au risque que s'est fixée l'organisation. Pour commencer, le management doit s'intéresser au risque maîtrisable.

Le *risque maîtrisable* correspond à la part du risque inhérent sur laquelle le management peut exercer une influence directe et qu'il peut réduire *via* les activités quotidiennes. Une fois que le management a mis en place des activités de contrôle d'un bon rapport coût/efficacité pour parer au risque maîtrisable, alors, et seulement alors, il peut déterminer si l'organisation agit conformément à l'appétence pour le risque définie par la direction générale et le Conseil. La part du risque inhérent qui subsiste après traitement de l'ensemble des risques maîtrisables constitue le *risque résiduel*.

Appétence pour le risque

Niveau de risque global qu'une organisation est prête à accepter en vue de la réalisation de ses objectifs. L'appétence pour le risque tient compte du niveau de risque que le management accepte consciemment après avoir évalué les coûts et les avantages de la mise en œuvre des contrôles.

Tolérance au risque

Niveaux acceptables d'intensité et de variation du risque au regard de la réalisation des objectifs, lesquels doivent être conformes à l'appétence pour le risque de l'organisation.

Copyright © 2015 Eyrolles.

Si le risque résiduel est inférieur à l'appétence pour le risque que l'organisation s'est fixée, alors le système de contrôle interne fonctionne à un niveau acceptable et dans les limites de l'appétence pour le risque définie pour une organisation.

Si, en revanche, le risque résiduel est supérieur à l'appétence pour le risque que l'organisation s'est fixée, il est nécessaire de réévaluer le système de contrôle interne pour déterminer si des activités de contrôle supplémentaires présentant un bon rapport coût/efficacité peuvent être mises en œuvre, afin de réduire encore le risque résiduel et de le ramener à un niveau correspondant à l'appétence pour le risque du management. Sinon, cette dernière doit envisager d'autres possibilités, comme le partage ou le transfert d'une part du risque résiduel à un tiers indépendant prêt à le supporter, *via* l'assurance ou l'externalisation. Si le risque résiduel ne peut pas être transféré ou partagé efficacement, le management peut accepter ce niveau de risque supérieur (et ajuster son appétence pour le risque en conséquence) ou l'organisation doit décider si elle veut poursuivre l'activité qui est à l'origine du risque. Pour un examen approfondi de la gestion des risques et de ses techniques, voir le chapitre 4, *La gestion des risques*.

Un système de contrôle interne conçu de manière adéquate et qui fonctionne de manière effective peut, par définition, gérer les risques dans les limites de l'appétence pour le risque que s'est fixées l'organisation. Il devrait maîtriser le risque inhérent lié aux trois catégories d'objectifs définies par le COSO (opérations, reporting et conformité) dans le cadre de l'appétence pour le risque définie par le management.

LES DIFFÉRENTES APPROCHES DU CONTRÔLE INTERNE

Étant donné que, dans une organisation, chacun exerce une responsabilité liée au contrôle interne, celui-ci fera bien sûr l'objet d'approches différentes. Des perceptions divergentes du contrôle interne ne sont pas à rejeter. Le contrôle interne porte principalement sur les objectifs de l'organisation et il est légitime que différents groupes s'intéressent à des objectifs différents. De même, en raison de leurs perspectives différentes, différents groupes percevront les avantages et les coûts du contrôle interne de manière très différente, ce qui apporte une aide précieuse à l'organisation lorsqu'elle évalue l'adéquation de la conception et le fonctionnement effectif du contrôle interne.

Management

La direction générale étant chargée de fixer les objectifs de l'organisation, elle considère naturellement le contrôle interne dans cette

Risque maîtrisable

Part du risque inhérent que le management peut réduire *via* des opérations et des activités de gestion quotidiennes.

Risque résiduel

Part du risque inhérent qui subsiste après prise en compte des modalités de traitement des risques mises en œuvre par le management (on parle parfois de risque net).

Copyright © 2015 Eyrolles.

perspective. Le management doit envisager le contrôle interne en termes de coûts et de bénéfices attendus et allouer les ressources nécessaires pour atteindre ces objectifs.

Du point de vue du management, le contrôle interne englobe un certain nombre d'activités conçues pour maîtriser les risques ou bénéficier d'opportunités qui ont une incidence sur la réalisation des objectifs d'une organisation. La participation du management au système de contrôle interne lui permet de réagir rapidement lorsque les conditions l'exigent. Elle lui permet aussi de se conformer aux lois et règlements au niveau national, local et sectoriel.

Auditeurs internes

Tout comme la direction générale, les auditeurs internes considèrent le contrôle interne sous l'angle de son rôle dans la réalisation des objectifs de l'organisation. Alors que le management est responsable du système de contrôle interne, les auditeurs internes sont chargés de vérifier, en toute indépendance, que les dispositifs de contrôle de l'organisation sont conçus de manière adéquate et fonctionnent de manière effective. Cette validation indépendante, qui tient compte de tous les systèmes, processus, opérations, fonctions et activités d'une entité, augmente la probabilité que les objectifs de l'organisation soient atteints. En outre, les auditeurs internes sont bien placés pour exprimer leur avis sur les coûts et les avantages des différentes activités de contrôle et peuvent indiquer au management les contrôles dont la suppression est, selon eux, envisageable en raison de leur caractère redondant ou parce que les avantages qu'ils procurent sont inférieurs au coût que représente leur mise en œuvre.

Auditeurs externes (commissaires aux comptes)

La responsabilité première des auditeurs externes d'une organisation est d'attester de la sincérité des comptes, et dans certains pays, de l'efficacité du contrôle interne relatif au reporting financier. Pour cette raison, ils se concentrent sur l'incidence du contrôle interne sur le reporting financier. Si, lorsqu'ils s'acquittent de leur responsabilité, les auditeurs externes tiennent compte des objectifs et de la stratégie de l'organisation, ils ne considèrent pas le contrôle interne dans une perspective aussi large que ne le font la direction et les auditeurs internes.

Autres parties externes

Les parties externes qui s'intéressent au contrôle interne d'une organisation sont le législateur, les autorités de régulation et de

Copyright © 2015 Eyrolles.

supervision, les investisseurs et les créanciers. Étant donné qu'ils s'intéressent à des aspects différents, ils auront une perception différente du contrôle interne. Par conséquent, le législateur et les autorités de régulation et de supervision ont élaboré diverses définitions du contrôle interne qui sont conformes à leurs responsabilités. Ces définitions concernent généralement les types d'activités suivies et peuvent englober la réalisation des objectifs de l'organisation, ses obligations en matière de reporting, l'utilisation des ressources conformément aux lois et règlements et la lutte contre le gaspillage, les pertes et les utilisations abusives. Les investisseurs et les créanciers, en revanche, ont surtout besoin des informations financières que valident les auditeurs externes.

TYPOLOGIE DES CONTRÔLES

Le référentiel COSO explique que les activités de contrôle existent à tous les niveaux d'une organisation et peuvent généralement être classées en deux catégories : les activités de contrôle dans l'ensemble de l'entité et les activités de contrôle des processus métier. Dans cette deuxième catégorie, le référentiel intégré de contrôle interne du COSO regroupe également des contrôles des transactions ou des contrôles applicatifs, qui représentent « les activités de contrôle les plus fondamentales au sein d'une [organisation], car [elles] s'appliquent aux modalités de traitement des risques déployées au sein des processus métier pour que les objectifs du management soient atteints. »[34]

Une organisation met en œuvre de nombreux types d'activités de contrôle pour augmenter la probabilité que ses objectifs seront atteints. Il importe de noter que certains contrôles peuvent être désignés différemment d'une organisation à l'autre (voire d'une personne à l'autre au sein d'une organisation). Le type de contrôle est plus important que le terme utilisé pour le décrire. Il peut toutefois en découler une certaine confusion, car beaucoup de contrôles relèvent simultanément de plusieurs catégories. Ce point est traité en détail plus loin dans ce chapitre.

Selon leur application spécifique, ces contrôles peuvent être classés de diverses manières et dans plusieurs catégories à la fois. Les sections suivantes présentent les différents types de contrôles et leur finalité.

Contrôles à l'échelle de l'entité, des processus et des transactions

Tous les contrôles visent à maîtriser le risque, soit au niveau de l'organisation soit au niveau opérationnel dans une organisation. Comme indiqué plus haut, le référentiel COSO utilise les

Contrôle à l'échelle de l'entité

Contrôle au niveau de toute une entité et qui, par conséquent, n'est ni lié ni associé à un processus en particulier.

Copyright © 2015 Eyrolles.

expressions « dans l'ensemble de l'entité » et « [au niveau] des processus métier » pour décrire ces contrôles. Bien qu'il ne soit pas rare que, dans le secteur de l'audit interne, des organisations recourent à une terminologie différente, telle qu'« au niveau de l'organisation » ou « au niveau de l'entité », pour des questions de simplicité et de cohérence, on emploiera ci-après les termes les plus récemment adoptés par le COSO, à savoir « à l'échelle de l'entité ». Ce chapitre décrit également les contrôles au niveau des processus et les contrôles au niveau des transactions, qui constituent ensemble les activités de contrôle des processus métier, telles que définies par le référentiel COSO. La finalité et le fonctionnement effectif des contrôles sont toutefois plus importants que les termes utilisés pour désigner ces contrôles. Pour une illustration des contrôles, qui sont décrits ci-après, voir l'entonnoir de l'encadré 4-3.

Les contrôles à l'échelle de l'entité sont très généraux et ont souvent trait à l'environnement ou à la culture au sein de l'organisation. Ils sont destinés à maîtriser directement les risques qui existent au niveau de l'organisation, notamment les risques survenant aussi bien en interne qu'en externe. Ils peuvent maîtriser indirectement les risques au niveau des processus et des transactions. Ces contrôles « ont un effet généralisé sur la réalisation de nombreux objectifs ». Aux États-Unis, l'*Auditing Standard No. 5* du *Public Company Accounting Oversight Board* (PCAOB) énumère les exemples suivants de contrôles à l'échelle de l'entité :

- contrôles dans l'environnement de contrôle ;
- contrôles sur la possibilité de contournement des risques par le management ;
- processus d'évaluation des risques de l'organisation ;
- traitement et contrôles centralisés, y compris environnements de services partagés ;
- contrôles destinés à piloter les résultats d'opérations ;
- contrôles visant à piloter d'autres contrôles, tels que les activités de l'audit interne, du comité d'audit et des programmes d'auto-évaluation ;
- contrôles sur le processus du reporting financier en fin d'exercice ;
- politiques portant sur d'importantes pratiques de contrôle et de gestion des risques de l'organisation.[35]

Les contrôles à l'échelle de l'entité peuvent être classés en deux catégories : les contrôles relevant de la gouvernance et les contrôles relevant de la surveillance exercée par le management. Les premiers sont définis par le Conseil et la direction générale afin d'instituer la culture de contrôle de l'organisation et de donner des orientations qui soutiennent les objectifs stratégiques. Les seconds sont définis par le management de chaque unité opérationnelle et

Copyright © 2015 Eyrolles.

dans le cadre de la ligne hiérarchique afin de réduire les risques au niveau de l'unité opérationnelle et d'accroître la probabilité que celle-ci atteigne ses objectifs.

Contrôle au niveau des processus

Activité opérée au sein d'un processus spécifique dans le but d'atteindre les objectifs au niveau du processus.

Les contrôles au niveau des processus sont plus détaillés que les contrôles à l'échelle de l'entité. Ils sont définis par les propriétaires de chaque processus qui cherchent à réduire le risque qui menace la réalisation des objectifs des processus. Bien que cohérents, ces contrôles peuvent différer au niveau de leur exécution d'un processus à l'autre. Voici des exemples de contrôles au niveau des processus :

- rapprochements des comptes significatifs ;
- vérifications physiques des actifs (comme inventaire physique des stocks) ;
- supervision des collaborateurs chargés des processus et évaluations des performances ;
- évaluation des risques au niveau des processus ;
- pilotage/surveillance de certaines transactions.

Contrôle au niveau des transactions

Activité qui réduit le risque associé à une catégorie de tâches ou de transactions opérationnelles au sein d'une organisation.

Les contrôles au niveau des transactions sont encore plus détaillés que les contrôles au niveau des processus et réduisent le risque associé à un groupe d'activités (tâches) ou de transactions opérationnelles au sein d'une organisation. Ils doivent permettre le traitement exact et rapide des différentes activités, tâches ou transactions opérationnelles, ainsi que des ensembles connexes d'activités, de tâches ou de transactions opérationnelles. Exemples de contrôles au niveau des transactions :

- autorisations ;
- documentation (documents de référence, par exemple) ;
- séparation des tâches ;
- contrôle applicatif des SI (entrées, traitements, sorties).

S'ils sont conçus de manière adéquate et fonctionnent de manière effective, les contrôles à l'échelle de l'entité ainsi qu'au niveau des processus et des transactions fonctionnent de manière coordonnée et protègent l'organisation contre les risques qui menacent la réalisation de ses objectifs.

Copyright © 2015 Eyrolles.

Contrôles clés et secondaires

Contrôle clé (ou contrôle primaire)

Activité destinée à réduire les risques associés à un objectif critique de l'organisation.

On peut également classer les contrôles suivant leur importance, c'est-à-dire en contrôles clés ou secondaires.

Un contrôle clé (souvent appelé contrôle « primaire ») est une activité destinée à réduire les principaux risques associés aux objectifs

de l'organisation. L'absence de contrôles clés conçus de manière adéquate et fonctionnant de manière effective peut empêcher l'organisation d'atteindre ses objectifs critiques, voire compromettre sa pérennité.

Un contrôle secondaire vise :

- soit à maîtriser les risques associés aux objectifs de l'organisation qui ne sont pas critiques ;
- soit à réduire en partie le niveau de risque lorsqu'un contrôle clé ne fonctionne pas de manière effective. Les contrôles secondaires maîtrisent le niveau de risque résiduel lorsque les contrôles clés ne fonctionnent pas de manière effective, mais ils ne suffisent pas, à eux seuls, à ramener un risque donné à un niveau acceptable. Ils constituent généralement un sous-ensemble de contrôles compensatoires.

Contrôle secondaire

Activité destinée soit à réduire les risques associés aux objectifs de l'organisation qui ne sont pas critiques pour la survie ou pour la réussite de l'organisation, soit à appuyer un contrôle clé.

Contrôles compensatoires

Ces contrôles sont destinés à relayer des contrôles clés inefficaces, ou qui ne permettent pas de maîtriser pleinement un risque ou un ensemble de risques, pour le ramener à un niveau acceptable, à savoir dans les limites de l'appétence pour le risque définie par la direction générale et le Conseil. Par exemple, une supervision étroite dans les cas où la séparation des tâches est impossible peut constituer un contrôle compensatoire. Ces contrôles peuvent également appuyer ou dupliquer des contrôles multiples et peuvent porter sur plusieurs processus et risques.

Contrôle compensatoire

Activité qui, si les contrôles clés ne fonctionnent pas de manière effective, peut contribuer à réduire le risque considéré. Un contrôle compensatoire ne peut pas, en tant que tel, ramener le risque à un niveau acceptable.

Comme indiqué plus haut, les contrôles secondaires et les contrôles compensatoires sont nécessaires lorsqu'il n'est pas possible de créer ou de concevoir un contrôle clé efficace pour maîtriser pleinement un risque ou un groupe de risques et le ramener dans les limites de l'appétence pour le risque définie par le management. Des limitations économiques ou une complexité opérationnelle, ou les deux, peuvent en être à l'origine. Quelle qu'en soit la raison, il faut des contrôles secondaires et compensatoires dans le cas où il n'existe aucun contrôle clé efficace. Les contrôles compensatoires fonctionnent souvent en concurrence avec des contrôles clés connexes ou qui les recoupent, tout en servant de contrôles secondaires pour un contrôle clé en particulier.

Contrôles préventifs et détectifs

Les nombreux types de contrôles sont souvent distingués selon leur finalité. Voici une courte liste de ces types de contrôles et leur définition.

Copyright © 2015 Eyrolles.

Un *contrôle préventif* est destiné à empêcher la survenue d'un événement non voulu. Étant donné la nature dynamique et la complexité des opérations quotidiennes de l'organisation, il est plus difficile de concevoir un contrôle préventif économique et efficient. C'est pourquoi la plupart des organisations combinent contrôles préventifs et contrôles détectifs pour établir un système de contrôle interne qui soit à la fois efficace et efficient. Parmi les exemples de contrôles préventifs, on peut citer les contrôles relatifs à l'accès physique et logique, comme les portes fermées à clé et les identifiants utilisateurs assortis de mots de passe spécifiques.

À l'inverse, un *contrôle détectif* est destiné à mettre en évidence un événement indésirable déjà survenu. Pour être jugé efficace, ce contrôle doit être mis en œuvre rapidement (avant que l'événement indésirable ait un effet négatif inacceptable sur l'organisation). Parmi les exemples de contrôles détectifs, on peut citer les caméras de sécurité qui permettent de repérer les accès physiques non autorisés ou l'examen des journaux informatiques qui dressent la liste des tentatives d'intrusion.

Contrôles des systèmes d'information

En raison de la dépendance actuelle vis-à-vis des systèmes d'information, il convient de mettre en œuvre des contrôles pour maîtriser les risques associés aux systèmes automatisés qui sont nécessaires à l'activité principale d'une organisation.

Deux types de contrôles des systèmes d'information, parfois désignés sous le terme générique « contrôles SI », peuvent servir à maîtriser ces risques :

- **les contrôles informatiques généraux :** les contrôles informatiques généraux « s'appliquent à la quasi-totalité des opérations et contribuent à assurer leur fonctionnement correct » ;
- **les contrôles applicatifs :** les contrôles applicatifs « comprennent des procédures programmées à l'intérieur même des logiciels d'application ainsi que des procédures manuelles associées assurant le contrôle du traitement des différentes transactions »[36] ;
- l'ensemble de ces contrôles permet « de garantir l'exhaustivité, l'exactitude et la validité des informations, financières ou autres, stockées dans le système »[37].

On considère les contrôles informatiques généraux comme des contrôles à l'échelle de l'entité, car ils s'appliquent à l'ensemble de l'organisation et de ses nombreuses applications informatiques. Les contrôles applicatifs, en revanche, sont plus souvent considérés comme des contrôles au niveau des processus ou des transactions. Le chapitre 7, *Les risques et les contrôles des systèmes*

Copyright © 2015 Eyrolles.

d'information, traite plus en détail ces deux types de contrôles et en donne des exemples.

Classification des contrôles dans plusieurs catégories

Comme évoqué plus haut dans ce chapitre, certains contrôles peuvent entrer dans plusieurs catégories à la fois. Ainsi, un contrôle peut être à la fois un contrôle à l'échelle de l'entité et un contrôle clé. Le même contrôle peut aussi être un contrôle détectif. En revanche, il ne peut pas être à la fois un contrôle secondaire ou un contrôle au niveau des transactions et un contrôle clé ou un contrôle à l'échelle de l'entité. Si ces nuances peuvent être source de confusion au début, on comprend mieux, au fur et à mesure que l'on se familiarise avec les contrôles, comment les différentes catégories peuvent être englobées dans un même contrôle.

ÉVALUATION DU SYSTÈME DE CONTRÔLE INTERNE – PRÉSENTATION

Comme indiqué plus haut, l'adéquation de la conception et le fonctionnement effectif du système de contrôle interne relèvent en dernier ressort du management (directeur général). Le management est donc responsable de l'instauration, à l'échelle de l'entité et au niveau des activités, de contrôles conçus de manière adéquate et fonctionnant de manière effective, destinés à maîtriser les risques associés à la réalisation des objectifs de l'organisation, dans chacune des trois catégories définies par le COSO : opérations, reporting et conformité.

Les auditeurs internes jouent un rôle important dans la vérification de l'exercice des responsabilités du management. C'est ce dernier qui procède à l'évaluation préliminaire du contrôle interne, à l'aide d'un processus formalisé développé à cette fin. L'audit interne valide ensuite de manière indépendante les résultats obtenus par le management. De plus, un rapport est généralement soumis au comité d'audit, soit par la direction générale soit par le responsable de l'audit interne. Il présente les résultats de l'évaluation du management en ce qui concerne l'adéquation de la conception et le fonctionnement effectif du système de contrôle interne de l'organisation.

Comme indiqué dans le *Cadre de référence international des pratiques professionnelles de l'audit interne* de l'IIA et plus particulièrement selon la Modalité Pratique d'Application 2130-1, Évaluer la pertinence des processus de contrôle, l'audit interne doit évaluer les contrôles d'une organisation (certains éléments ou la totalité du système de contrôle interne) :

Copyright © 2015 Eyrolles.

« Lors de l'évaluation de l'efficacité des processus de contrôle d'une organisation, le responsable de l'audit interne tient compte :

- du caractère significatif des anomalies ou des faiblesses mises en évidence ;
- des corrections ou améliorations apportées après les constatations ;
- du fait que les constatations et leurs conséquences potentielles induisent à conclure à un état entraînant un niveau de risque inacceptable. »

De surcroît, aux États-Unis, la loi Sarbanes-Oxley fait obligation au management des organisations enregistrées auprès de la SEC de publier un rapport sur la fiabilité de leur contrôle interne relatif au reporting financier. Comme déjà indiqué, cette loi fait reposer la responsabilité de la conception, de la gestion et du fonctionnement effectif de ce contrôle uniquement sur la direction générale, plus précisément sur le directeur général et le directeur financier. Conformément à cette législation, la SEC impose au directeur général et au directeur financier des sociétés cotées de se prononcer sur la fiabilité du reporting financier (c'est-à-dire sur l'adéquation de la conception et le fonctionnement effectif du contrôle interne relatif au reporting financier) dans le cadre du dépôt annuel des états financiers auprès de la SEC, ainsi que de signaler, sur une base trimestrielle, tout changement substantiel apporté à ce contrôle le cas échéant. De nombreux autres pays ont mis en place des obligations analogues.

Dans l'optique de garantir la fiabilité du reporting financier, « le management fixe des critères de qualité concernant la comptabilisation, l'évaluation, la présentation et la publication des comptes, transactions et événements inclus dans les états financiers de l'entité »[38]. Il existe cinq critères de qualité génériques concernant les états financiers.

- *Existence ou survenue* – Les actifs, les passifs et les droits de propriété existent à une date donnée et les transactions enregistrées correspondent à des événements qui sont réellement survenus au cours d'une période donnée.
- *Exhaustivité* – L'intégralité des transactions, événements ou circonstances qui sont survenus au cours d'une période donnée et qui auraient dû être comptabilisés au cours de cette même période ont effectivement été enregistrés.
- *Droits et obligations* – Les actifs correspondent aux droits de l'entité à une date donnée tandis que les passifs reflètent ses obligations.
- *Valorisation ou allocation* – Les éléments de l'actif, du passif, des produits et des charges sont comptabilisés pour le bon montant conformément aux principes comptables appropriés et

Copyright © 2015 Eyrolles.

pertinents. Les transactions sont mathématiquement exactes et correctement enregistrées dans les livres ou les registres de l'entité.

- *Informations présentées et publiées* – Les informations figurant dans les états financiers sont correctement présentées, libellées et classées.[39]

Les activités de contrôle menées dans l'ensemble de l'entité et sur les processus métier, qui ont pour but d'apporter une assurance raisonnable que les objectifs liés au reporting externe sont atteints et d'étayer les critères de qualité retenus par le management, présentent plusieurs éléments en commun. Pour être conçus de manière adéquate et pour fonctionner de manière effective, ces contrôles devraient correspondre aux concepts de lancement d'une tâche, d'autorisation, d'enregistrement, de traitement et de reporting. Comme indiqué plus haut dans ce chapitre, on parle communément du contrôle interne relatif au reporting financier.

Le *Public Company Accounting Oversight Board* (PCAOB) a été créé dans l'optique d'élaborer des règles auxquelles doivent se conformer les auditeurs externes et – indirectement – le management, afin de respecter les exigences de reporting. Pour cela, le PCAOB a publié le 12 juin 2007 la norme d'audit n° 5 (*Auditing Standard* No. 5), « *An Audit of Internal Control Over Financial Reporting That is Integrated with an Audit of Financial Statements* ». Pour plus de détails, veuillez vous reporter directement à cette norme.

OPPORTUNITÉS POUR UN POINT DE VUE DE L'AUDIT INTERNE

PCAOB

Public Company Accounting Oversight Board

Étant donné que les auditeurs internes réalisent des missions d'audit dans tous les services de l'organisation, ils ont une opportunité unique d'apporter un point de vue sur l'efficacité du système de contrôle interne de l'organisation. L'encadré 6-12 expose dix cas où l'audit interne a la possibilité d'apporter son point de vue.

RÉSUMÉ

Ce chapitre analyse les contrôles que les organisations élaborent pour maîtriser les risques susceptibles de menacer la réalisation de leurs objectifs. Après avoir défini le contrôle interne, il explique en quoi consiste un référentiel puis comment des concepts tels que le contrôle interne et le management des risques de l'entreprise sont plus efficaces lorsqu'ils sont mis en œuvre sur la base de référentiels bien conçus et largement acceptés. Par ailleurs, les différents référentiels qui traitent du contrôle interne ont été présentés. Ensuite, le chapitre identifie et définit les composantes d'un

Copyright © 2015 Eyrolles.

ENCADRÉ 6-12

APPORTER SON POINT DE VUE SUR L'EFFICACITÉ DU CONTRÔLE INTERNE 10 OPPORTUNITÉS POUR L'AUDIT INTERNE

- Aider l'organisation à élaborer un cadre de référence global pour évaluer l'adéquation de la conception et le fonctionnement effectif du contrôle interne.
- Aider le management à établir une structure logique pour analyser, documenter et évaluer la conception et la mise en œuvre du contrôle interne par l'organisation.
- Aider l'organisation à développer un processus d'identification, d'évaluation et de résolution des déficiences du contrôle interne.
- Fournir une assurance indépendante sur l'adéquation de la conception et le fonctionnement effectif du contrôle interne.
- Agir avec fermeté lorsque des changements ou des déficiences potentiellement significatives du contrôle interne sont identifiées.
- Accompagner l'analyse *a posteriori* lors de la survenue de déficiences du contrôle interne.
- Informer le management des dysfonctionnements potentiels du contrôle interne, qui entraînent un risque accru pour l'organisation.
- Aider le management à développer un comportement éthique (exemplarité) et une tolérance moindre face à l'inefficacité du contrôle interne.
- Se tenir au courant et informer le management des nouveaux règlements, lois et problématiques liés à l'efficacité du contrôle interne.
- Organiser des sessions de sensibilisation au contrôle interne dans l'ensemble de l'organisation.

système de contrôle interne conçu de manière adéquate et fonctionnant de manière effective. Au sein d'une organisation, chacun assume une part de responsabilité dans le contrôle interne, et ce chapitre présente les rôles et les responsabilités propres à chaque groupe d'intervenants à l'intérieur de l'organisation, notamment le processus d'évaluation, par le management, du système de contrôle interne global. En outre, il analyse également les rôles et les responsabilités propres à l'audit interne vis-à-vis de ce système. Il décrit les divers types de contrôles qui servent à maîtriser les nombreux risques auxquels une organisation est confrontée. Il explique également en détail la mise en œuvre appropriée de chacun de ces contrôles. Enfin, ce chapitre présente le processus d'évaluation du système de contrôle interne, qui sera décrit plus loin dans le présent manuel.

Copyright © 2015 Eyrolles.

Questions de révision



1. Qu'est-ce qu'un cadre de référence ? Quels sont les trois référentiels de contrôle interne les plus reconnus au niveau mondial par le management, les comptables, les auditeurs externes et les professionnels de l'audit interne ?

2. Que doivent faire le directeur général et le directeur financier d'une société cotée afin de se conformer à la loi Sarbanes-Oxley ?

3. Comment le COSO définit-il le contrôle interne ?

4. Que sont les objectifs ? Quelles sont les trois catégories d'objectifs établies par le référentiel COSO ?

5. Quelles sont les cinq composantes du contrôle interne détaillées dans le référentiel COSO ?

6. Que comprend l'environnement de contrôle ?

7. Qu'est-ce qu'implique l'évaluation des risques ?

8. Que sont les activités de contrôle ? Quels types d'activités de contrôle existent dans un système de contrôle interne bien conçu ?

9. Qu'est-ce qu'une information de qualité ? Pourquoi faut-il communiquer des informations de qualité ?

10. Quand le pilotage est-il le plus efficace ? Qui effectue le pilotage ? Qu'est-ce qui distingue les évaluations ponctuelles des activités de pilotage continues ?

11. Quels sont les 17 principes du contrôle interne définis par le COSO ?

12. Quelles sont les responsabilités des catégories de personnes suivantes au regard du contrôle interne ?
    a. Le management (y compris la direction générale).
    b. Le Conseil.
    c. Les auditeurs internes.
    d. Les autres membres de l'organisation.
    e. L'auditeur externe (commissaire aux comptes).

13. Que signifie « limites du contrôle interne » ? Donnez des exemples de limites inhérentes au contrôle interne.

14. Qu'est-ce que le risque inhérent ? Qu'est-ce que le risque maîtrisable ? Qu'est-ce que le risque résiduel ?

Copyright © 2015 Eyrolles.



Questions de révision

15. En quoi le point de vue des auditeurs internes sur le contrôle interne diffère-t-il de celui du management ?

16. En quoi les contrôles à l'échelle de l'entité diffèrent-ils des contrôles au niveau des processus et au niveau des transactions ?

17. Qu'est-ce qu'un contrôle clé ? Qu'est-ce qu'un contrôle secondaire ? Qu'est-ce qu'un contrôle compensatoire ?

18. Quelle est la différence entre un contrôle préventif et un contrôle détectif ?

19. Quelles sont les deux grandes catégories de contrôles des systèmes d'information ?

20. Comment le système de contrôle interne est-il évalué ?

Copyright © 2015 Eyrolles.

Questions à choix multiples

Sélectionnez la meilleure réponse pour chacune des questions suivantes.

1. Parmi les objectifs suivants, lequel décrit le mieux celui d'un auditeur interne qui examine les processus de gouvernance, de gestion des risques et de contrôle en place dans une organisation ?
   a. Aider à déterminer la nature, le calendrier et l'étendue des tests nécessaires à la réalisation des objectifs d'une mission.
   b. Veiller à ce que les faiblesses du système de contrôle interne soient corrigées.
   c. Apporter l'assurance raisonnable que ces processus permettront la réalisation efficiente et économique des objectifs de l'organisation.
   d. Déterminer si ces processus débouchent sur une comptabilité correcte et sur des états financiers sincères.

2. Qu'est-ce que le risque résiduel ?
   a. L'impact du risque.
   b. Le risque contrôlé.
   c. Le risque non géré.
   d. Le risque sous-jacent dans l'environnement.

3. L'obligation d'effectuer des achats auprès de fournisseurs figurant sur une liste de prestataires agréés est un exemple de :
   a. Contrôle préventif.
   b. Contrôle détectif.
   c. Contrôle compensatoire.
   d. Contrôle du pilotage.

4. Un système de contrôle interne efficace est susceptible de déceler une fraude commise par :
   a. Un groupe de collaborateurs agissant en collusion.
   b. Un seul collaborateur.
   c. Un groupe de managers agissant en collusion.
   d. Un seul manager.

5. Le contrôle le plus susceptible de déterminer que les chèques de paie ne sont établis que pour les montants autorisés consiste à :
   a. Effectuer une vérification périodique auprès des collaborateurs chargés de la paie.
   b. Exiger que les chèques non distribués soient retournés au caissier.
   c. Exiger que les cartes de pointage des collaborateurs soient validées par la hiérarchie.
   d. Assister périodiquement à la distribution des chèques de paie.

Copyright © 2015 Eyrolles.

6. Un auditeur interne prévoit d'auditer l'adéquation des contrôles sur les placements dans de nouveaux instruments financiers. Parmi les activités suivantes, laquelle n'est pas nécessaire dans le cadre d'une telle mission ?
   a. Déterminer s'il existe une politique décrivant les risques que le trésorier peut prendre et les types d'instruments dans lesquels ce dernier peut investir.
   b. Déterminer l'étendue de la surveillance exercée par le management sur les placements dans des instruments sophistiqués.
   c. Déterminer si le trésorier dégage sur les placements des rendements supérieurs ou inférieurs à ceux obtenus par ses homologues travaillant dans des organisations comparables.
   d. Déterminer la nature des activités de pilotage liées au portefeuille d'investissements.

7. Au sein d'une multinationale, pour que le contrôle interne soit approprié dans une succursale dotée d'un service chargé des virements :
   a. La personne qui lance les virements ne doit pas être la même que celle qui procède au rapprochement des relevés bancaires.
   b. Le manager de la succursale doit recevoir tous les virements.
   c. Les taux de change doivent être calculés séparément par deux collaborateurs différents.
   d. La direction générale autorise l'embauche de collaborateurs dans ce service.

8. Qui est l'ultime responsable du pilotage du contrôle interne ?
   a. L'auditeur externe (commissaire aux comptes).
   b. L'audit interne.
   c. La direction générale.
   d. Le Conseil.

9. Une assurance raisonnable, dans le domaine du contrôle interne signifie que :
   a. Les objectifs du contrôle interne varient selon la méthode de traitement des données utilisée.
   b. Un système de contrôle interne bien conçu permettra de prévenir ou de détecter toute erreur ou fraude.
   c. Les limites inhérentes au contrôle interne empêchent un système de contrôle interne de fournir une assurance absolue quant à la réalisation des objectifs.
   d. Le management et les collaborateurs ne peuvent contourner les contrôles par le biais d'une collusion.

Copyright © 2015 Eyrolles.

Questions à choix multiples

10. Parmi les exemples suivants, lequel décrit le mieux une activité de contrôle constituant une vérification indépendante ?
    a. Le rapprochement des comptes bancaires par quelqu'un qui ne gère pas la trésorerie ou qui n'enregistre pas les transactions en espèces.
    b. L'utilisation de badges d'identification et de codes de sécurité pour restreindre l'accès au site de production.
    c. L'existence de documents comptables et de pièces justificatives qui retracent l'historique des ventes et des encaissements.
    d. La séparation de la gestion physique et de la gestion comptable des stocks.

11. La composante « Évaluation des risques » du contrôle interne implique :
    a. L'évaluation du risque résiduel par l'auditeur externe.
    b. L'évaluation des déficiences du contrôle interne par la fonction audit interne.
    c. L'identification et l'analyse, par l'organisation, des risques qui menacent la réalisation de ses objectifs.
    d. Le pilotage de l'information financière par l'organisation pour repérer les potentielles anomalies significatives.

Copyright © 2015 Eyrolles.

Thèmes de discussion

1. Un rapport d'audit contient les observations suivantes :
   a. l'emplacement du service technique ne permet pas de rendre des services adéquats à d'autres unités ;
   b. les antécédents des collaborateurs recrutés à des postes sensibles ne sont pas vérifiés ;
   c. les managers n'ont pas accès aux rapports qui présentent les performances globales par rapport à celles d'autres organisations de référence ;
   d. le management n'a pas pris des mesures correctives pour remédier aux observations de missions antérieures portant sur les contrôles des stocks.

   Parmi ces observations, quelles sont les deux qui sont les plus susceptibles d'indiquer des faiblesses de contrôles relatifs à la protection des actifs ? Pourquoi ?

2. Conformément aux normes relatives à l'évacuation des déchets, une usine met en œuvre un système de contrôles destiné à empêcher le rejet d'eaux usées ne satisfaisant pas à ces normes. L'un des contrôles consiste à analyser l'eau, avant le rejet, pour rechercher des éléments spécifiés sur l'autorisation. Ce contrôle est-il approprié ? Pourquoi ?

3. Une organisation entend empêcher que des volumes de stocks supérieurs à ses besoins ne soient commandés. Dans cette organisation, une personne souhaite concevoir un contrôle imposant l'examen, par un superviseur du service utilisateur, de toutes les demandes d'achat, avant la présentation de ces demandes au service des achats. Une autre personne veut instaurer une politique exigeant la validation de l'avis de réception et du bordereau de marchandises avant le stockage des nouveaux produits reçus. Lequel/Lesquels de ces contrôles permet/permettent d'atteindre l'objectif spécifié ? Expliquez pourquoi.

4. Selon le COSO : « Les auditeurs internes jouent un rôle important dans l'évaluation des systèmes de contrôle interne, qu'ils contribuent à maintenir à un niveau d'efficacité satisfaisant. Par ailleurs, en raison de leur position au sein de l'organisation et de l'autorité dont ils sont investis, les auditeurs internes jouent souvent un rôle important dans la surveillance du fonctionnement du système de contrôle interne. ». Répondez aux questions suivantes en fonction de cette citation.
   a. La fonction d'audit interne d'une organisation fait-elle partie de son système de contrôle interne ? Si vous répondez par l'affirmative, expliquez comment l'audit interne peut évaluer l'adéquation de la conception et le fonctionnement effectif du contrôle interne tout en restant indépendant du système de contrôle interne de l'organisation. Si vous répondez par la négative, expliquez le rôle de l'audit interne dans le système de contrôle interne de l'organisation.
   b. Si le pilotage est, par définition, un élément du contrôle interne dont la direction générale est responsable, faut-il que l'audit interne réalise des activités de pilotage ? Développez votre réponse.

Copyright © 2015 Eyrolles.

ÉTUDE DE CAS

[40] Les contrôles maîtrisent les risques qui menacent la réalisation des objectifs et apportent ainsi l'assurance raisonnable que ceux-ci seront atteints. Les risques englobent à la fois les risques de survenue d'événements négatifs et de non-survenue d'événements positifs. Certains contrôles sont visibles et peuvent par conséquent être photographiés.

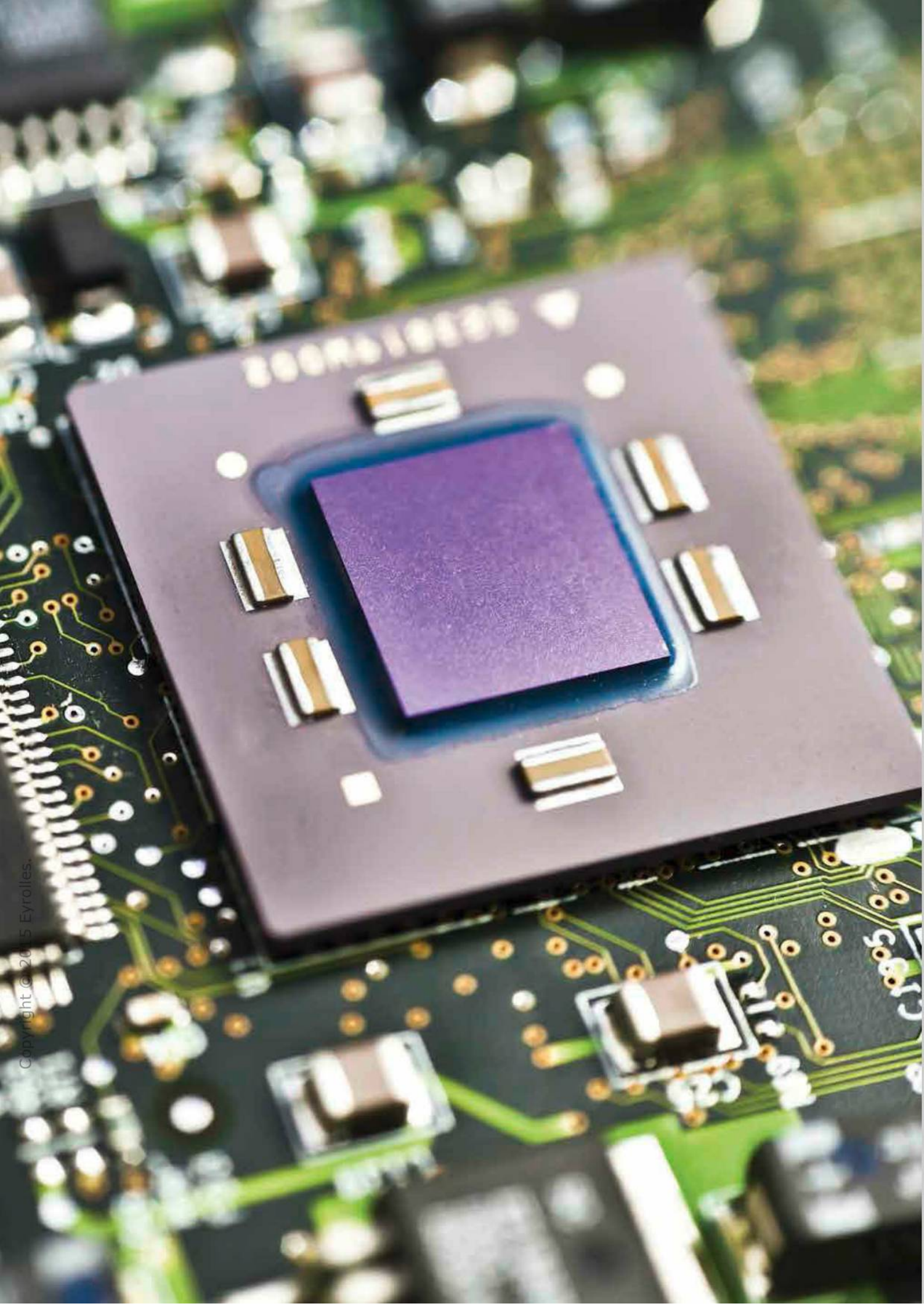
A. Choisissez un ou deux étudiants avec le(s)quel(s) vous souhaitez travailler dans le cadre de cette mission. Chaque équipe aura besoin d'un appareil photo.

B. En équipe, photographiez cinq contrôles différents observés sur le campus et/ou aux alentours. Faites appel à votre imagination et à votre ingéniosité. Chaque équipe doit travailler de manière indépendante pour produire un ensemble unique de clichés. Au moins deux des contrôles photographiés doivent avoir pour finalité de maîtriser le risque de non-survenue d'un événement positif (c'est-à-dire de permettre la survenue d'un événement positif).

C. Pour chaque contrôle photographié :
   - indiquez clairement s'il est conçu pour maîtriser le risque de survenue d'un événement négatif ou de non-survenue d'un événement positif ;
   - ensuite, décrivez brièvement et séparément :
   a. un objectif dont ce contrôle doit permettre la réalisation ;
   b. un risque que ce contrôle doit maîtriser (N.B. : le risque que vous décrivez ne doit pas être simplement l'inverse de l'objectif concerné) ;
   c. comment ce contrôle est censé opérer (c'est-à-dire comment il fonctionne) ;
   d. comment vous testeriez ce contrôle pour déterminer son fonctionnement effectif.

Éléments à produire :
A. les cinq photographies ;
B. les descriptions des cinq contrôles que ces photographies illustrent, comme spécifié en c.

Copyright © 2015 Eyrolles.



Copyright ©2015 Eyrolles.



CHAPITRE 7
LES RISQUES ET LES CONTRÔLES DES SYSTÈMES D'INFORMATION

Objectifs pédagogiques

- Comprendre comment les systèmes d'information (SI) sont liés aux objectifs, aux stratégies et aux opérations d'une organisation.
- Décrire les principales composantes des systèmes d'information.
- Expliquer la nature des opportunités et des risques SI.
- Comprendre les concepts fondamentaux de la gouvernance, de la gestion des risques et des contrôles relatifs aux SI.
- Comprendre l'impact des SI pour les auditeurs internes.
- Connaître les sources de lignes directrices relatives à l'audit des SI.
- Comprendre les conséquences de l'introduction de nouvelles technologies pour l'environnement économique.
- Comprendre comment l'audit interne peut donner des orientations dans le cadre de projets SI.

Les systèmes d'information évoluent rapidement. Ils impliquent ainsi de nouveaux défis que les organisations doivent relever, même si elles décident de ne pas opérer des changements similaires sur les systèmes d'information déployés en interne. Par exemple, du fait de l'utilisation accrue des réseaux sociaux comme Twitter et Facebook, des informations négatives sur une organisation peuvent être publiées en ligne, même si celle-ci n'est pas du tout active sur Internet et les réseaux sociaux. Certaines organisations ont donc créé des groupes qui ont pour but de gérer les répercussions, sur leurs activités, de la manière dont elles sont perçues par les personnes qui utilisent les réseaux sociaux. Les organisations doivent se montrer prudentes dans l'appréhension de ce nouvel outil, car les effets des publications négatives sont instantanés et ne peuvent être annulés. Les spécialistes des réseaux sociaux font notamment observer que ce domaine en rapide expansion présente de nombreux risques et opportunités pour les organisations.

Grâce à l'utilisation des réseaux sociaux, les organisations sont davantage susceptibles d'atteindre leurs objectifs. En effet, utilisés efficacement, les réseaux sociaux offrent les possibilités suivantes aux organisations :

- augmenter le chiffre d'affaires ;
- fidéliser et améliorer la satisfaction de la clientèle ;

- recruter et fidéliser les meilleurs talents ;
- améliorer le développement de produits et l'innovation ;
- améliorer l'image de marque et la perception de la clientèle.[1]

Parallèlement, sans une surveillance appropriée, l'utilisation des réseaux sociaux peut engendrer d'autres risques, parmi lesquels :

- une gouvernance absente ou inefficace autour de l'utilisation des réseaux sociaux ;
- un manque de conformité aux exigences réglementaires ;
- une incapacité à définir ou à suivre des indicateurs relatifs aux réseaux sociaux ;
- une incapacité à établir une politique efficace concernant l'utilisation des réseaux sociaux.[2]

Politique « Apportez vos outils personnels » (*Bring Your Own Device*, BYOD)

Politique par laquelle une organisation autorise ses collaborateurs à accéder à leur messagerie électronique professionnelle, à leur agenda et à d'autres données *via* leur ordinateur personnel, leur smartphone, leur tablette ou d'autres appareils.

L'exemple des réseaux sociaux n'en est qu'un parmi d'autres, qui illustre la manière dont la technologie doit être revue et évaluée en permanence pour en identifier à la fois les avantages et les risques. L'adoption d'une nouvelle technologie par la société peut avoir un impact à long terme sur chaque organisation, y compris celles qui refusent d'intégrer la technologie en question. L'audit interne a la possibilité d'être impliqué dès les premières phases du processus, lorsque les questions émergentes se posent. Il peut alors apporter son point de vue concernant l'optimisation des opportunités et la maîtrise des risques.

Les organisations étudient depuis longtemps la meilleure façon de permettre à leurs collaborateurs d'accéder, à distance et de manière sécurisée, à leur messagerie électronique professionnelle, à leur agenda et à d'autres informations. La « consumérisation » des systèmes d'information a ainsi engendré la multiplication de politiques « Apportez vos outils personnels » (*Bring Your Own Device*, BYOD). Ainsi, les collaborateurs choisissent de plus en plus d'accéder à leur messagerie électronique et à d'autres données *via* leur ordinateur personnel, leur smartphone, leur tablette ou d'autres appareils informatiques. La croissance rapide de l'utilisation des smartphones et autres appareils a augmenté le risque lié aux informations de l'organisation pour les biens personnels non sécurisés.

Si de nombreuses organisations ont établi des règles et procédures relatives à l'utilisation d'appareils personnels, beaucoup d'autres n'en ont pas fait autant. Même celles qui ont établi de telles règles considèrent qu'il est très difficile pour la fonction SI de piloter et de contrôler le transfert des données de l'organisation vers les appareils portables. Dans la mesure où il est compliqué de donner l'assurance que les données personnelles et celles de l'organisation sont protégées sur ces appareils, la sécurité de l'information et la confidentialité des données personnelles se révèlent de plus en plus cruciales.

Copyright © 2015 Eyrolles.

Quelle que soit la vitesse à laquelle les organisations adoptent une nouvelle technologie après son apparition, toutes investissent massivement dans les SI. Plusieurs raisons les poussent à réaliser de tels investissements, et toutes découlent directement de la volonté de parvenir à leurs objectifs. Par exemple, les SI permettent la mise en œuvre des stratégies, améliorent les performances des processus opérationnels et facilitent la prise de décisions. En fait, les SI sont désormais si imbriqués avec les objectifs, les stratégies et les opérations des organisations que ces dernières doivent les intégrer dès les premières phases de l'élaboration de toute nouvelle initiative, de manière à ce que les SI et les activités aillent dans le même sens.

Prenons quelques exemples.

- Une organisation de distribution cherche à développer son chiffre d'affaires grâce à la vente directe sur son site Web. Envisager une stratégie de vente en ligne ne serait pas possible si la technologie du commerce électronique et d'Internet n'existait pas.
- Une organisation souhaite vendre à l'étranger mais son système d'information n'est pas en mesure de gérer les achats clients effectués en devises. Grâce aux fonctions multidevises intégrées dans la plupart des applications d'achat, une organisation peut rapidement s'adapter au traitement des devises.
- Une organisation industrielle cherche à rationaliser son processus d'achats afin d'en comprimer les coûts. L'Échange de données informatisées (EDI), grâce auquel les transactions se font directement de l'ordinateur de l'organisation à ceux des fournisseurs, constitue une solution technologique que le management doit envisager.
- Une grande chaîne de boutiques de fleuristes veut évaluer plus précisément les performances opérationnelles quotidiennes de ses points de vente, qui sont géographiquement dispersés. Un entrepôt de données (*data warehouse*), dans lequel seraient stockées les informations historiques pertinentes, faciliterait le calcul des performances quotidiennes de chaque magasin, l'analyse des tendances des performances par gamme de produits et l'analyse des scénarios d'anticipation de performance.

L'impact de plus en plus étendu des SI sur les stratégies et les opérations quotidiennes des organisations a des répercussions importantes sur la profession d'audit interne. La place croissante des SI a fait évoluer les compétences que les auditeurs internes doivent posséder et la manière dont ils mènent leurs activités d'assurance et de conseil. Dans le monde des affaires d'aujourd'hui, une fonction d'audit interne sera pratiquement dans l'incapacité d'apporter des services à valeur ajoutée à son organisation si elle ne connaît pas parfaitement les risques et les contrôles relatifs aux SI et si elle n'est pas capable d'appliquer efficacement des techniques d'audit informatisées.

Auditeur des systèmes d'information (SI)

Auditeur interne qui travaille essentiellement dans le domaine des systèmes d'information informatisés et qui possède une bonne connaissance des risques, des contrôles et de l'audit des SI.

Copyright © 2015 Eyrolles.

ENCADRÉ 7-1

DISPOSITIONS DU CRIPP PERTINENTES RELATIVES AU CHAPITRE 7

Norme 1210 – Compétence
Norme 1220 – Conscience professionnelle
Norme 2110 – Gouvernement d'entreprise
Norme 2110.A2
Norme 2120 – Management des risques
Norme 2130 – Contrôle

Modalité Pratique d'Application 1210-1 : Compétence
Modalité Pratique d'Application 1210.A1-1 : Recours à des prestataires externes
Modalité Pratique d'Application 1220-1 : Conscience professionnelle
Modalité Pratique d'Application 2120-1 : Évaluer la pertinence des processus de management des risques
Modalité Pratique d'Application 2130-1 : Évaluer la pertinence des processus de contrôle
Modalité Pratique d'Application 2130.A1-1 : Fiabilité et intégrité de l'information
Modalité Pratique d'Application 2130.A1-2 : L'évaluation du dispositif mis en place par l'organisation pour protéger la vie privée

Guides pratiques

GTAG 1 : Les contrôles et le risque des systèmes d'information, 2e édition
GTAG 2 : Contrôles de la gestion du changement et des patchs : un facteur clé de la réussite pour toute organisation, 2e édition
GTAG 3 : Audit continu : répercussions sur l'assurance, le pilotage et l'évaluation des risques
GTAG 4 : Management de l'audit des systèmes d'information
GTAG 7 : L'infogérance, 2e édition
GTAG 8 : Audit des contrôles applicatifs
GTAG 9 : Gestion des identités et des accès
GTAG 10 : Gestion de la continuité d'activité
GTAG 11 : Élaboration d'un plan d'audit des SI
GTAG 12 : Audit des projets SI
GTAG 13 : *Fraud Prevention and Detection in an Automated World*
GTAG 14 : *Auditing User-developed Applications*
GTAG 15 : *Information Security Governance*
GTAG 16 : *Data Analysis Technologies*
GTAG 17 : *Auditing IT Governance*
GTAG 18 : *Cloud Computing* – à paraître
GTAG 19 : *Social Media* – à paraître

***The GAIT Methodology* (La méthodologie du GAIT)**

GAIT for IT General Control Deficiency Assessment
GAIT for Business and IT Risk (GAIT-R)
Études de cas – Utiliser le GAIT-R pour se conformer aux normes PCI

Un auditeur interne qui travaille essentiellement dans le domaine des systèmes d'information informatisés doit posséder une bonne connaissance des risques, des contrôles et de l'audit des SI. On désigne souvent ces auditeurs sous le vocable d'auditeurs des

Copyright © 2015 Eyrolles.

systèmes d'information ou d'auditeurs des SI. Même si tous les auditeurs internes n'ont pas besoin de disposer d'un savoir aussi pointu que celui d'un auditeur spécialiste des SI, chaque auditeur interne doit avoir au minimum une bonne maîtrise de certains concepts fondamentaux. Par exemple, tous les auditeurs internes doivent connaître les composantes génériques des systèmes d'information de leur organisation, les risques SI qui menacent la réalisation des objectifs de leur organisation, ainsi que les processus de gouvernance, de gestion des risques et de contrôle relatifs à ces SI.

Ce chapitre commence par présenter certaines des principales composantes des systèmes d'information. Il décrit ensuite les opportunités et les risques SI, puis s'intéresse à la gouvernance, à la gestion des risques et aux contrôles relatifs aux SI. Il traite enfin des impacts des SI pour les auditeurs internes et conclut en identifiant les sources de lignes directrices relatives à l'audit des SI à suivre par les auditeurs internes dans ce domaine.

PRINCIPALES COMPOSANTES DES SYSTÈMES D'INFORMATION

Les systèmes d'information varient considérablement d'une organisation à l'autre, et le présent manuel n'a pas pour objet de passer en revue toutes les configurations de systèmes qui existent actuellement. Cependant, ces systèmes ont des points communs que les auditeurs internes ont besoin de connaître et de comprendre. Ces composantes communes sont le matériel informatique, les réseaux, les logiciels, les bases de données, l'information et les ressources humaines. L'encadré 7-2 représente une configuration d'un système d'information simple, qui servira de contexte dans lequel s'inscriront les exemples des composantes décrites plus loin.

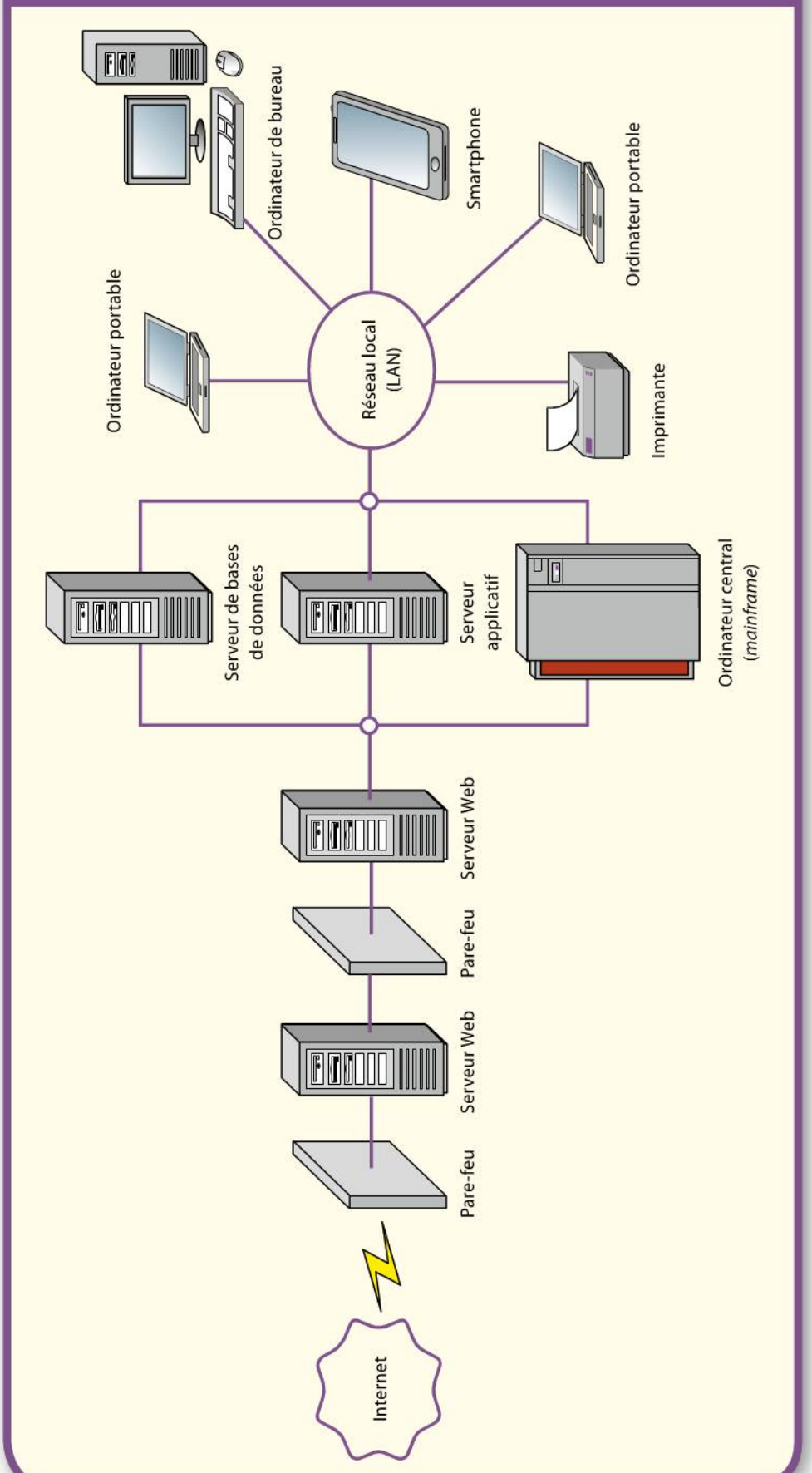
Matériel informatique. Le matériel informatique englobe les éléments physiques d'un système d'information. Le matériel comprend, par exemple, les unités centrales (CPU), les serveurs, les postes de travail et les terminaux, les puces, les périphériques d'entrée/sortie comme les scanners et les imprimantes, les dispositifs de stockage tels que les disques durs et les appareils de communication comme les modems et les routeurs sans fil.

> **Exemple :** le matériel informatique décrit à l'encadré 7-2 comprend un smartphone, un ordinateur de bureau, deux ordinateurs portables, une imprimante, un ordinateur central (*mainframe*), quatre serveurs et deux pare-feux. D'autres appareils dont l'organisation n'a pas connaissance sont également susceptibles d'accéder aux données et de modifier les bases de données protégées par le pare-feu. C'est pourquoi les règles de sécurité de l'information sont cruciales pour l'organisation.

Copyright © 2015 Eyrolles.

ENCADRÉ 7-2

CONFIGURATION D'UN SYSTÈME D'INFORMATION SIMPLE



Copyright © 2015 Eyrolles.

Réseaux. Un réseau informatique relie deux ordinateurs ou appareils, ou plus, de manière à ce qu'ils puissent échanger des informations et/ou des charges de travail. Il existe plusieurs sortes de réseaux :

- un réseau client-serveur relie un ou plusieurs ordinateurs clients à un serveur, et le traitement des données est partagé entre le(s) client(s) et le serveur de manière à optimiser l'efficience du processus ;
- un réseau local (*local area network*, LAN) couvre une zone relativement restreinte, comme un immeuble ou un pâté de maisons ;
- un réseau étendu (*wide area network*, WAN) est un système regroupant plusieurs LAN connectés ensemble afin de couvrir une zone régionale, nationale ou mondiale ;
- un intranet est le réseau privé d'une organisation, qui n'est accessible qu'aux collaborateurs de cette organisation ;
- un extranet est accessible à des tiers sélectionnés tels que les fournisseurs et/ou les clients autorisés ;
- un réseau à valeur ajoutée (RVA) est un réseau de tiers, qui connecte une organisation avec ses partenaires ;
- Internet (*inter*connected *net*works) est le système public très vaste et complexe de réseaux informatiques qui permet aux usagers de communiquer sur toute la planète ;
- deux appareils peuvent échanger des informations entre eux sans être reliés à d'autres réseaux.

Exemple : l'encadré 7-2 présente l'interconnexion entre le LAN, l'intranet de l'organisation et Internet.

Logiciels. Il existe plusieurs types de logiciels : les systèmes d'exploitation, les utilitaires, les logiciels de gestion de bases de données (SGBD), les logiciels d'application et les pare-feux. Le système d'exploitation commande les entrées, les traitements et les sorties dans l'ordinateur et gère l'interconnectivité des différentes composantes du matériel informatique. Les logiciels utilitaires complètent le système d'exploitation avec des fonctions telles que le chiffrage, l'optimisation de l'espace disque et la protection contre les virus. Les logiciels de gestion de bases de données gèrent les données stockées dans les bases de données, contrôlent les accès aux bases de données et font des sauvegardes automatiques. Les logiciels d'application sont, par exemple, les logiciels comptables utilisés pour le traitement des transactions ainsi que d'autres types de logiciels (tels que les logiciels de traitement de texte et les tableurs) qui permettent aux utilisateurs finaux d'exécuter les tâches qui leur ont été assignées. Les pare-feux servent à faire appliquer les contrôles d'accès entre deux réseaux en ne laissant que les données autorisées traverser le pare-feu dans les deux sens.

Base de données

Vaste ensemble de données, habituellement stockées dans de nombreux fichiers reliés entre eux d'une manière qui permette d'y accéder, de les récupérer et de les manipuler facilement.

Copyright © 2015 Eyrolles.

Exemple : chaque ordinateur de bureau, ordinateur portable, appareil intelligent (*smart device*), ordinateur central (*mainframe*) et serveur décrit à l'encadré 7-2 contient un système d'exploitation et les utilitaires nécessaires à leur bon fonctionnement et à l'échange d'informations entre les ordinateurs et l'imprimante. Les logiciels d'application génériques peuvent être installés sur chaque ordinateur de bureau et ordinateur portable, ou être stockés sur le serveur applicatif mis en commun entre les utilisateurs des ordinateurs de bureau et portables. Les programmes d'application plus volumineux peuvent résider sur le serveur applicatif ou sur l'ordinateur central (*mainframe*) et traiter les données à la demande des utilisateurs. Le serveur de bases de données et l'ordinateur central (*mainframe*) hébergent un logiciel de base de données qui gère les données stockées et spécifie les accès et les privilèges de chaque utilisateur. Les serveurs Web hébergent un logiciel qui dirige le flux d'informations entre Internet et l'intranet de l'organisation. Les pare-feux contiennent deux couches de logiciels qui empêchent les transmissions d'informations non autorisées depuis et vers l'organisation.

Big Data

Terme qui désigne le grand nombre d'informations numériques qui circulent en permanence, l'augmentation considérable des capacités de stockage de ces importants volumes de données, et la puissance de traitement des données nécessaire pour gérer, interpréter et analyser ces importants volumes d'informations numériques.

Bases de données. Une base de données est un vaste ensemble de données, habituellement stockées dans de nombreux fichiers reliés entre eux d'une manière qui permette d'y accéder, de les récupérer et de les manipuler facilement. Une base de données opérationnelle facilite le traitement des transactions quotidiennes et est actualisée en continu, à mesure que les transactions sont traitées ou selon une périodicité définie. Un entrepôt de données est un vaste ensemble de données stockées au fil du temps et destiné à faciliter l'analyse des données et la prise de décision en ligne. Les organisations étudient des concepts tels que le « Big Data » qui pourraient leur permettre d'utiliser l'ensemble des informations disponibles, et pas uniquement les données relatives aux transactions, afin d'augmenter leur chiffre d'affaires, d'améliorer leurs processus opérationnels, d'identifier de nouveaux produits et de recueillir des renseignements sur les données (data intelligence).

Exemple : chaque ordinateur de bureau, ordinateur portable et appareil intelligent décrit à l'encadré 7-2 peut accueillir des bases de données utilisées pour stocker des volumes relativement restreints de données utiles à leur utilisateur. Le serveur de bases de données héberge des bases de données plus étendues conçues pour contenir des volumes de données plus importants. Les ordinateurs centraux (*mainframe*) accueillent en général des bases de données encore plus vastes, qui requièrent un temps de réponse encore plus rapide étant donné le volume des requêtes et des besoins de traitement. Le SGBD contrôle quels utilisateurs peuvent accéder à telle ou telle donnée et ce qu'ils peuvent en faire.

Copyright © 2015 Eyrolles.

Information. « L'information est une ressource clé pour toutes les entreprises, et de sa création jusqu'à sa destruction la technologie joue un rôle important. »[3] Les systèmes d'information collectent et stockent les données, les transforment en informations utiles et procurent l'information aux décideurs internes et externes. Pour que l'information soit utile, elle doit être pertinente, fiable, complète, exacte et communiquée en temps opportun.

> **Exemple :** chaque ordinateur de bureau, ordinateur portable, appareil intelligent, serveur et ordinateur central (mainframe) décrit à l'encadré 7-2 contient des informations enregistrées dans différentes sortes de fichiers et qui sont utiles à leurs utilisateurs. L'information circule dans de multiples directions entre les différents ordinateurs, et également vers et depuis des parties à l'intérieur et à l'extérieur de l'organisation.

Ressources humaines. Les rôles propres à chacun au sein d'un système d'information varient largement d'une organisation à l'autre. Habituellement, ces rôles sont confiés à un directeur des systèmes d'information (DSI), à un administrateur de base de données, à des développeurs système, aux collaborateurs qui traitent les données et aux utilisateurs finaux.

- Le directeur des systèmes d'information (DSI) est chargé de la surveillance et de la direction quotidienne des SI et doit veiller à ce que les objectifs et la stratégie des SI concordent avec les objectifs et la stratégie de l'organisation.
- L'administrateur de base de données doit superviser la conception, le développement, la mise en œuvre et la maintenance de la base de données, en contrôler l'accès, en suivre le fonctionnement et la mettre à jour pour répondre aux besoins des utilisateurs. Dans les organisations plus importantes, le responsable de la sécurité des systèmes d'information et le responsable du plan de continuité d'activité contribuent généralement au traitement des problématiques liées à la technologie, telles que la confidentialité de l'information et la continuité d'activité.
- Les développeurs systèmes sont des analystes et des programmeurs. Les analystes étudient les besoins des utilisateurs, analysent les SI en comparant l'existant à ce qui devrait exister et conçoivent de nouveaux SI. Les programmeurs élaborent et testent les logiciels utilisés pour l'exécution du traitement des données.
- Les collaborateurs qui traitent les données gèrent les ressources SI centralisées et exécutent quotidiennement des opérations centralisées d'entrée, de traitement et de sortie.
- Les utilisateurs finaux sont les managers et les collaborateurs pour lesquels le système d'information a été conçu. Ils utilisent l'information produite par le système afin de remplir leur rôle et s'acquitter chaque jour de leurs responsabilités.

Copyright © 2015 Eyrolles.

Exemple : Les collaborateurs participant au système d'information décrit à l'encadré 7-2 recouvrent les utilisateurs des ordinateurs de bureau, des ordinateurs portables et des appareils intelligents, les administrateurs de bases de données chargés de gérer ces bases, les personnes qui doivent gérer et faire fonctionner les différents serveurs et pare-feux, ainsi que les programmeurs d'applications qui ont élaboré et testé les logiciels d'application. Les logiciels d'application peuvent avoir été conçus en interne ou achetés auprès d'un fournisseur. L'ordinateur central (*mainframe*) suppose des compétences spécialisées en raison de son degré élevé de complexité.

OPPORTUNITÉS ET RISQUES SI

Progiciel de gestion intégré (PGI)

Logiciel modulaire qui permet aux organisations d'intégrer leurs processus opérationnels à l'aide d'une seule base de données opérationnelle.

Les notions d'opportunité et de risque ont été présentées au chapitre 1, *Introduction à l'audit interne*, et traitées en détail au chapitre 4, *La gestion des risques*. L'*opportunité* est la possibilité qu'un événement se produise et ait une incidence *positive* sur la réalisation des objectifs d'une organisation, tandis que le *risque* désigne la possibilité qu'un événement se produise et ait une incidence négative sur la réalisation des objectifs de l'organisation. Les opportunités et les risques que rencontre une organisation du fait de ses SI représentent une part significative des opportunités et des risques qu'elle doit comprendre et gérer efficacement.

Opportunités offertes par les SI

Échange de données informatisées (EDI)

Échange d'ordinateur à ordinateur de documents sous forme électronique entre une organisation et ses partenaires.

La vente de marchandises en ligne peut constituer par exemple une opportunité offerte par la technologie du commerce électronique et que nombre d'organisations ont su saisir. Parmi les autres opportunités offertes par les progrès des SI, on peut citer les progiciels de gestion intégrés des ressources (PGI, ou ERP pour *Enterprise Resource Planning*) et l'échange de données informatisées (EDI).

- **Progiciels de gestion intégrés (PGI) –** Un PGI est un logiciel modulaire qui permet aux organisations d'intégrer leurs processus opérationnels à l'aide d'une seule base de données opérationnelle. Lorsqu'elles se dotent d'un PGI, les organisations espèrent pouvoir traiter leurs transactions en ligne et en temps réel, bénéficier d'une grande fluidité dans l'interaction et le partage de l'information entre les domaines fonctionnels, améliorer le fonctionnement de leurs processus, gagner en fiabilité, réduire ou éliminer les redondances ou les erreurs dans les données et pouvoir prendre leurs décisions plus rapidement. Cependant, installer un PGI efficace et efficient dans le délai et le budget prévus constitue une immense tâche, qui n'est pas dénuée de risques. Pour pouvoir exploiter les opportunités

Copyright © 2015 Eyrolles.

offertes par un PGI, il faut savoir maîtriser les risques qui sont susceptibles de mettre en péril cette initiative.

- **Échange de données informatisées (EDI) –** L'EDI est un échange d'ordinateur à ordinateur de documents sous forme électronique entre une organisation et ses partenaires. Lorsqu'elles se dotent d'un système d'EDI, les organisations espèrent améliorer l'efficience du traitement de leurs transactions et faire baisser le nombre d'erreurs de traitement. De plus, les progrès récents de la technologie liée au commerce électronique permettent désormais à l'EDI de passer par Internet, ce qui revient moins cher que l'EDI traditionnel. Cependant, une organisation ne peut pas utiliser un EDI de manière efficace et efficiente si ses partenaires ne font pas de même. De plus, réaliser des transactions *via* Internet ne se fait pas sans risques. Pour pouvoir exploiter pleinement les opportunités offertes par l'EDI, il faut savoir maîtriser les risques liés au commerce électronique.

Risques SI

Chacune des grandes composantes du système d'information décrites précédemment dans ce chapitre représente une source potentielle de risque. Par exemple :

- le matériel informatique est exposé à un risque de coupures d'électricité qui interrompent le traitement des transactions, notamment les traitements en cours ;
- les réseaux transmettent des informations qui peuvent être interceptées, volées ou utilisées à mauvais escient ;
- les logiciels qui sont mal programmés peuvent produire des informations non valides, incomplètes et/ou inexactes ;
- il est possible d'infiltrer les bases de données dans le but de détourner des informations ou de les utiliser à mauvais escient ;
- l'information qui est non valide, incomplète et/ou inexacte peut conduire à prendre de mauvaises décisions. (Le risque que des mauvaises informations se traduisent alors par de mauvaises décisions est en général appelé *risque informationnel*) ;
- il se peut qu'une personne exécute des fonctions relatives aux SI incompatibles entre elles et se retrouve dans une situation lui permettant de commettre des erreurs ou des fraudes et de les dissimuler.

Le recours aux systèmes d'information génère des risques SI spécifiques. Les risques SI auxquels une organisation devra faire face dépendent de la nature de l'activité et des opérations de l'organisation, du secteur dans lequel elle opère, de la configuration de son système d'information et de plusieurs autres facteurs internes et externes. De plus, le risque évolue sous l'influence

Copyright © 2015 Eyrolles.

de l'environnement interne et externe de l'organisation. Dans le monde actuel, rien n'évolue plus vite que les SI. Les organisations doivent donc se tenir en permanence au courant des progrès des SI et examiner les conséquences de ces avancées pour les risques auxquels elles doivent faire face.

Cependant, certaines catégories de risques SI sont communes à toutes les organisations et à tous les secteurs.

- **Risque de sélection.** La sélection d'une solution de SI qui ne se prête pas à la réalisation d'un objectif stratégique peut empêcher l'exécution d'une stratégie qui lui serait liée. De même, le choix d'une solution de SI qui n'est pas assez flexible et/ou évolutive peut engendrer des incompatibilités entre cette solution et les systèmes existants de l'organisation et/ou entraver les changements et la croissance à venir de l'organisation. Le risque de sélection peut par exemple résulter du manque de qualification des décideurs ou de l'insuffisance des informations qui sous-tendent la décision.

Commentaire du traducteur

L'acquisition d'un logiciel sans prendre en compte de nouvelles prestations en cours de commercialisation constitue un autre exemple de risque de sélection.

Le GTAG 4, « Management de l'audit des systèmes d'information », et le GTAG 11, « Élaboration d'un plan d'audit des SI » (qui font partie de la série des *Global Technology Audit Guides* de l'IIA), donnent de plus amples informations sur le risque de sélection, ainsi que des lignes directrices sur la manière dont l'audit interne devrait allouer ses ressources pour donner l'assurance que le risque de sélection est correctement maîtrisé.

- **Risque de développement/d'acquisition et de déploiement.** Les problèmes rencontrés lors du développement/de l'acquisition puis du déploiement de la solution de SI peuvent entraîner des retards ou des dépassements de coûts imprévus, voire l'abandon du projet. Ces risques peuvent être dus à un manque d'expertise en interne, à une assistance insuffisante de la part du fournisseur et à une résistance au changement. Le GTAG 12, « Audit des projets SI », et le GTAG 14, « *Auditing User-developed Applications* », identifient de nombreux autres exemples de risques, introduits par les projets SI, auxquels l'organisation peut être confrontée.
- **Risque d'indisponibilité.** Si un système n'est pas disponible alors que l'organisation en a besoin, cela peut retarder la prise de décision, interrompre l'activité, se traduire par un manque à gagner ou mécontenter le client. Le risque d'indisponibilité peut par exemple résulter de dysfonctionnements du matériel/des logiciels, d'une maintenance non planifiée et de virus ou autres

Copyright © 2015 Eyrolles.

actes malveillants. Le GTAG 10, « Gestion de la continuité d'activité », donne des lignes directrices sur les meilleures pratiques relatives à la reprise de l'activité.

- **Risque matériel/logiciel.** Les dysfonctionnements du matériel/des logiciels peuvent interrompre l'activité, endommager de manière temporaire ou permanente les données ou les détruire, et induire des coûts de réparation ou de remplacement du matériel/des logiciels. Ce risque peut résulter par exemple de l'usure normale, des dégradations causées par l'environnement (par exemple une humidité excessive), des catastrophes telles que les incendies ou les inondations, des virus ou autres actes malveillants.
- **Risque lié à l'accès.** Un accès physique ou logique non autorisé au système peut être à l'origine de vols ou d'utilisations abusives du matériel, de modifications logicielles malveillantes, ou encore de vols, d'utilisations abusives ou de destructions de données. Ce risque peut par exemple se produire lorsque des smartphones sont utilisés pour consulter, modifier et stocker les données de l'organisation, ou lorsque les tiers peuvent accéder à ces données *via* les réseaux sans fil. Le GTAG 9, « Gestion des identités et des accès », met en évidence un certain nombre de problématiques relatives aux contrôles d'accès et leurs solutions.
- **Risque lié au manque de fiabilité du système et d'intégrité de l'information.** Les erreurs systématiques ou les incohérences dans le traitement peuvent produire des informations non pertinentes, incomplètes, inexactes, et/ou qui ne sont pas disponibles en temps voulu. Ces informations défaillantes produites par le système peuvent nuire aux décisions qu'elles sont censées étayer. Il existe donc un risque lié au manque de fiabilité du système et d'intégrité de l'information. C'est le cas, par exemple, lors d'erreurs de programmation, de modifications non autorisées d'un logiciel ou d'une évolution de paramétrage non prévue. Le GTAG 8, « Audit des contrôles applicatifs », donne aux auditeurs des règles relatives à la vérification des contrôles intégrés au cœur des applications.
- **Risque lié à la violation de la confidentialité des données personnelles.** La communication non autorisée des informations confidentielles concernant les partenaires commerciaux ou des informations personnelles peut se traduire par la perte de marchés, par des poursuites judiciaires, des articles critiques dans la presse ou une atteinte à la réputation. Ce type de risque existe par exemple lorsqu'il n'y a aucune entrave à l'accès aux réseaux, aux logiciels et aux bases de données de l'organisation. Le guide pratique de l'IIA intitulé « L'audit des risques d'atteinte à la vie privée » aborde les risques d'atteinte à la vie privée, y compris ceux directement liés aux SI, ainsi que les contrôles y afférents. Il donne également des lignes directrices quant à la manière d'auditer efficacement la protection de la vie privée.

Copyright © 2015 Eyrolles.

- **Risque de fraude et d'actes malveillants.** Le vol de ressources SI, l'utilisation abusive intentionnelle de ces ressources ou la distorsion/destruction intentionnelle d'informations peuvent entraîner un préjudice financier et/ou la communication d'informations erronées sur lesquelles s'appuieront les décideurs. Il existe un risque de fraude et d'actes malveillants par exemple lorsque des collaborateurs mécontents et des pirates informatiques (*hackers*) cherchent à nuire à l'organisation pour en tirer un bénéfice personnel. Le GTAG 13, « *Fraud Prevention and Detection in an Automated World* », met l'accent sur les risques de fraude liés aux SI et donne des lignes directrices aux auditeurs internes quant à la manière d'utiliser la technologie pour parer efficacement à la fraude.

La description de ces risques SI a davantage vocation à servir d'illustration plutôt que de dresser une liste exhaustive. Il convient également de noter que ces risques ne s'excluent pas mutuellement. Par exemple, un système d'information peut être indisponible (risque d'indisponibilité) en raison de dysfonctionnements du matériel/des logiciels (risque matériel/logiciel). De même, les fraudes et autres actes malveillants peuvent entraîner l'apparition de tous les autres risques. La série des GTAG aborde l'ensemble des risques et des contrôles relatifs aux SI, et apporte des lignes directrices détaillées quant à la manière de réaliser un audit des SI efficace.

GOUVERNANCE DES SI

Gouvernance des SI

Activité comprenant la direction, les structures organisationnelles et les processus qui garantissent que les technologies de l'information soutiennent la stratégie et les objectifs de l'organisation.

La gouvernance est définie au chapitre 1, *Introduction à l'audit interne*, comme le processus piloté par le Conseil qui consiste à autoriser, diriger et surveiller les activités de la direction générale en vue de réaliser les objectifs de l'organisation. Suivant la description détaillée qui en est donnée au chapitre 3, *La gouvernance*, la structure de la gouvernance donne l'assurance que l'organisation opère dans les limites et conformément aux valeurs fixées par le Conseil et la direction générale.

Comme le précise l'introduction du présent chapitre, les organisations investissent massivement dans les SI, car ces derniers leur permettent d'exécuter leur stratégie et d'atteindre leurs objectifs. Face à l'impact généralisé des SI sur leur stratégie et leurs opérations, beaucoup d'organisations ont conclu que la gouvernance des SI méritait en elle-même une attention particulière.

Comme l'indiquent la Norme 2110.A2 et le GTAG 17, « *Auditing IT Governance* », la gouvernance des SI est très importante. La Norme 2110.A2 stipule que « l'audit interne doit évaluer si la gouvernance des systèmes d'information de l'organisation soutient la stratégie et les objectifs de l'organisation »[4]. Le GTAG 17, « *Auditing IT Governance* », insiste sur ce point : « La gouvernance des SI

Copyright © 2015 Eyrolles.

relève principalement de la responsabilité du Conseil et de la direction générale. Comme le stipule la Norme 2110.A2, l'audit interne doit évaluer si la gouvernance des systèmes d'information de l'organisation soutient la stratégie et les objectifs de l'organisation. »[5]

Commentaire du traducteur

En France, les associations professionnelles représentant des auditeurs et des DSI (l'AFAI, le CIGREF et l'IFACI) ont publié un guide d'audit sur la gouvernance des systèmes d'information en 2011.

L'IIA définit la gouvernance des SI en ces termes :

> « *La gouvernance des technologies de l'information comprend la direction, les structures organisationnelles et les processus qui garantissent que les technologies de l'information soutiennent la stratégie et les objectifs de l'organisation.* »[6]

Il ressort clairement de ces descriptions et définitions que le Conseil et la direction générale sont les « propriétaires » de la gouvernance des SI, de même qu'ils sont les propriétaires de tous les autres aspects de la gouvernance. Certains conseils ont mis en place des comités de gouvernance dont les compétences englobent les SI. Les comités d'audit jouent aussi un rôle important dans la gouvernance des SI. Le Conseil et ses comités doivent indiquer à la direction générale quelle doit être l'orientation de la gouvernance des SI et surveiller les activités de gouvernance des SI de la direction générale. Cette dernière est responsable de l'orientation et de la supervision de l'exécution quotidienne de la gouvernance des SI. Certaines organisations se sont dotées d'un comité de la gouvernance des SI, au sein duquel siègent le directeur des systèmes d'information ainsi que d'autres cadres supérieurs. Comme l'explique le GTAG 17, « *Auditing IT Governance* », la gouvernance des SI est une composante clé de la gouvernance globale, tel que l'illustre l'encadré 7-3.

LA GESTION DES RISQUES SI

Gestion des risques SI

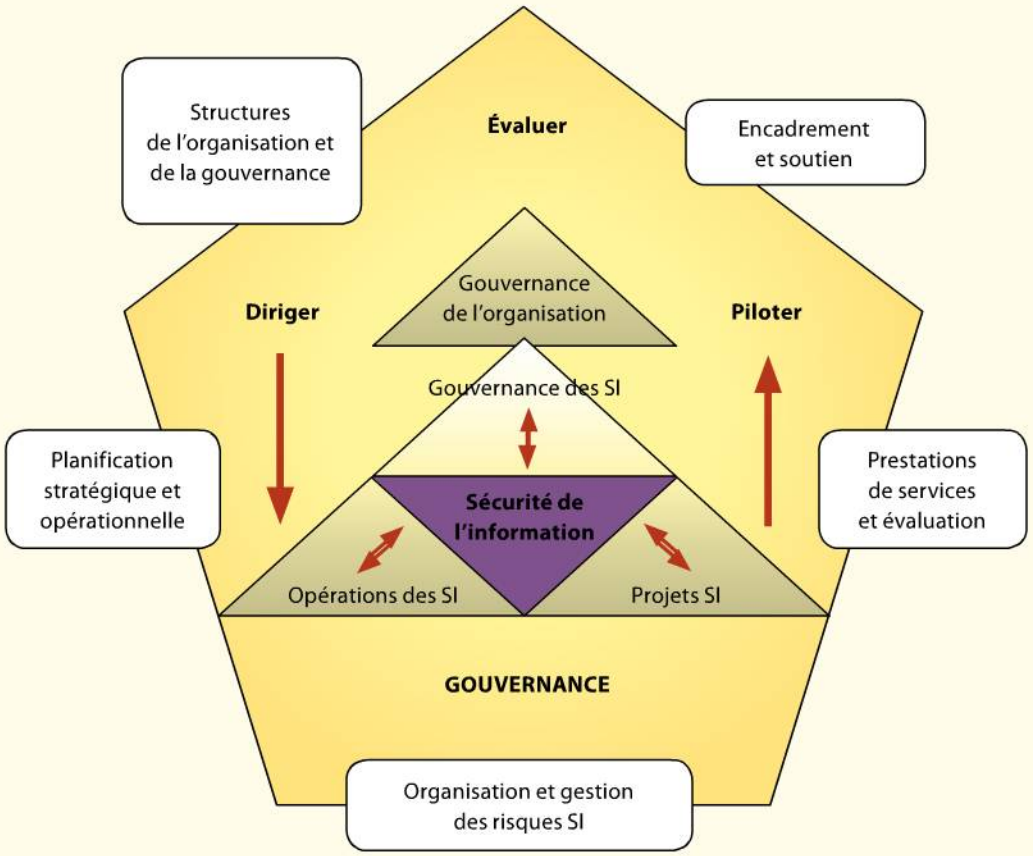
Processus piloté par le management qui consiste à appréhender et à traiter les risques et opportunités liés aux SI susceptibles d'affecter la capacité de l'organisation à réaliser ses objectifs.

La gestion des risques est définie au chapitre 1, *Introduction à l'audit interne*, comme le processus piloté par le management qui consiste à appréhender et à traiter les incertitudes (risques et opportunités) susceptibles d'affecter la capacité de l'organisation à réaliser ses objectifs. Le chapitre 4, *La gestion des risques*, décrit en détail comment le processus de gestion des risques opère au sein de la structure de gouvernance de l'organisation pour :

- détecter et maîtriser les risques susceptibles d'entraver la réussite de l'organisation ;
- exploiter les opportunités qui conduisent au succès de l'organisation.

Copyright © 2015 Eyrolles.

CADRE DE RÉFÉRENCE DE LA GOUVERNANCE DES SI



GTAG 17 : *Auditing IT Governance*, Figure 2 (Altamonte Springs, Floride : *The Institute of Internal Auditors*, juillet 2012), p. 3.

ENCADRÉ 7-3

Comme le précisent l'ouvrage *Enterprise Risk Management – Integrated Framework* du *Committee of* Sponsoring Organizations of the Treadway Commission (COSO) ainsi que le chapitre 4, *La gestion des risques*, le management des risques de l'entreprise comporte huit éléments reliés entre eux : environnement interne, fixation des objectifs, identification des événements, évaluation des risques, traitement des risques, activités de contrôle, information et communication, et pilotage.[7] Chacun de ces éléments est pertinent pour la gestion des risques SI. Par exemple :

- **environnement interne :** l'environnement interne d'une organisation inclut l'« exemplarité au plus haut niveau » de l'organisation. Comme indiqué dans la section précédente du présent chapitre, le Conseil et la direction générale doivent diriger et superviser le processus de gouvernance des SI de l'organisation. Ils doivent également définir l'appétence pour le risque SI de l'organisation ainsi que ses seuils de tolérance au risque SI ;

Copyright © 2015 Eyrolles.

- **fixation des objectifs :** comme indiqué dans la section précédente du présent chapitre, le processus de gouvernance des SI commence par la fixation des objectifs des SI, lesquels donnent la direction des activités des SI. Parce que les SI permettent l'exécution de la stratégie et la réalisation des objectifs de l'organisation, la gestion stratégique des opérations des SI doit concorder avec la gestion stratégique globale de l'organisation ;
- **identification des événements :** il convient d'identifier les événements potentiels survenant dans ou en dehors de l'organisation et qui sont susceptibles de nuire à l'exécution de la stratégie et à la réalisation des objectifs de l'organisation. Des exemples de ces risques ont été décrits plus haut, dans la section intitulée « Risques SI » ;
- **évaluation des risques :** il convient ensuite d'évaluer la probabilité d'occurrence et l'impact inhérent des risques SI identifiés. Cette évaluation suppose une analyse des conséquences négatives et des causes potentielles de ces risques. Il convient aussi de tenir compte de l'impact et de la probabilité d'occurrence résiduelle des risques SI identifiés en prenant en considération les déficiences de la gestion des risques ;
- **traitement des risques :** il convient de définir un traitement des risques approprié pour les risques SI identifiés. L'acceptation du risque constitue un traitement approprié pour les risques SI dont les niveaux d'impact inhérent et de probabilité d'occurrence ne dépassent pas la tolérance au risque du management. Les modalités de traitement possibles pour les risques SI dont l'impact inhérent et la probabilité d'occurrence dépassent la tolérance au risque du management sont l'évitement, la réduction ou le partage du risque ;
- **activités de contrôle :** il convient de définir des règles appropriées de traitement des risques et de concevoir des procédures de manière adéquate (actions menées pour faire appliquer les règles) et de les appliquer de manière effective afin de donner l'assurance que les niveaux de risque SI résiduel ne sortent pas des seuils de tolérance définis par le management. Les contrôles des SI sont décrits dans la section suivante du présent chapitre ;
- **information et communication :** le système d'information d'une organisation a pour but d'identifier, de saisir et de communiquer en temps voulu des informations de grande qualité aux décideurs. Par exemple, l'information pertinente pour l'identification, l'évaluation et le traitement des risques SI doit être communiquée dans toute l'organisation. La gestion des risques SI doit veiller à ce que les systèmes d'information de l'organisation, reposant sur la technologie, produisent avec fiabilité des informations de grande qualité ;

Copyright © 2015 Eyrolles.

- **pilotage :** le management est chargé de piloter le processus de gestion des risques SI, y compris le contrôle relatif aux SI, sur la durée afin de veiller à ce que le processus reste efficace et efficient à mesure de l'évolution des facteurs environnementaux internes et externes qui influent sur l'organisation.

CONTRÔLES DES SI

Le chapitre 1, *Introduction à l'audit interne*, définit le contrôle comme un processus intégré à la gestion des risques, conduit par le management et qui consiste à ramener les risques à un niveau acceptable. Le chapitre 6, *Le contrôle interne*, décrit en détail le contrôle interne et introduit le concept de contrôles des SI. Les contrôles des SI se répartissent habituellement entre les contrôles généraux et les contrôles applicatifs, évoqués au chapitre 6.

- « Les *contrôles généraux* s'appliquent à l'ensemble des composantes, processus et données d'une organisation ou d'un environnement système. »[8]
- « Les *contrôles applicatifs* portent sur l'étendue des processus de l'organisation ou ses applications et incluent les contrôles au niveau des entrées, des traitements et des sorties des applications. »[9]

On peut aussi classer les contrôles « en fonction du groupe chargé de veiller à leur mise en œuvre et de leur correcte actualisation »[10]. Par exemple, comme le montre l'encadré 7-4, les contrôles des SI peuvent être classés selon une hiérarchie descendante : gouvernance des SI, gestion et contrôles techniques. Les six strates supérieures des contrôles des SI présentées à l'encadré 7-4 représentent les contrôles généraux des SI, tandis que la strate inférieure représente les contrôles applicatifs. Il importe toutefois de comprendre que « les différents éléments de contrôle placés dans cette hiérarchie ne sont pas mutuellement exclusifs ; ils sont tous reliés les uns aux autres, se chevauchent et se confondent souvent »[11]. La suite de cette section décrit les contrôles des SI du point de vue de ceux qui en sont responsables.

Les contrôles relatifs à la gouvernance des SI

Comme indiqué précédemment dans le présent chapitre, la gouvernance des SI fait partie intégrante de la gouvernance. De même, les contrôles relatifs à la gouvernance des SI constituent un sous-ensemble important du système de contrôle interne d'une organisation. Les contrôles relatifs à la gouvernance des SI relèvent de la compétence du Conseil et de la direction générale. Le Conseil a toutefois la responsabilité de surveiller le système de contrôle interne de l'organisation, et non d'exécuter les contrôles. C'est à la

Copyright © 2015 Eyrolles.

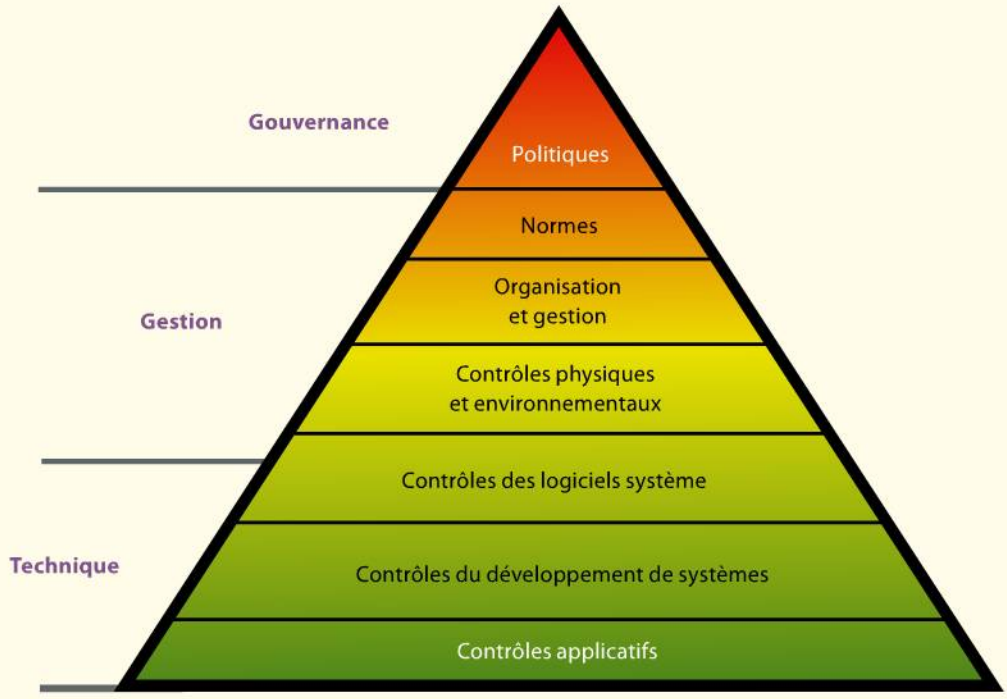
direction générale qu'il appartient de conduire quotidiennement le processus de contrôle.

Comme le montre l'encadré 7-4, les contrôles relatifs à la gouvernance des SI sont définis dans la politique des SI. Cette politique définit la nature des contrôles qui doivent être en place et règle par exemple les aspects suivants :

- une politique générale sur le niveau de sécurité et le respect de la vie privée pour l'ensemble de l'organisation ;
- une politique sur la classification des données et les droits d'accès applicables selon celle-ci ;
- une définition des concepts de propriété des systèmes et des données, ainsi que de l'habilitation nécessaire pour créer, modifier ou supprimer les données ;
- des politiques de ressources humaines qui définissent les conditions de travail dans les domaines sensibles et en vérifient la bonne application ;
- la définition des exigences en matière de plans de continuité d'activité.[12]

ENCADRÉ 7-4

LES CONTRÔLES DES SI



GTAG 1 : Les contrôles et le risque des systèmes d'information, 2e édition (Altamonte Springs, Floride : *The Institute of Internal Auditors*, mars 2012), p. 25.

Copyright © 2015 Eyrolles.

Les contrôles relatifs à la gestion des SI

Le management doit veiller à ce que les contrôles des SI soient conçus de manière adéquate et fonctionnent de manière effective, compte tenu des objectifs de l'organisation, des risques qui menacent la réalisation de ces objectifs et des processus opérationnels, ainsi que des ressources de l'organisation. Comme le montre l'encadré 7-4, les contrôles relatifs à la gestion des SI comprennent les normes, l'organisation ainsi que les contrôles physiques et environnementaux.

Normes des SI

Normes qui étayent les exigences définies par les politiques en matière de SI, en déterminant des méthodes de travail qui permettent la réalisation des objectifs de l'organisation.

Les *normes des SI* étayent les exigences définies par les politiques en matière de SI, en déterminant des méthodes de travail qui permettent la réalisation des objectifs de l'organisation. Ces normes doivent, par exemple, couvrir les aspects suivants :

- **les procédures de développement des systèmes :** lorsque des organisations développent leurs propres applications, des normes définissent les procédures de conception, développement, test, mise en œuvre et maintenance des systèmes et programmes ;
- **la configuration de logiciels :** parce que les logiciels procurent une part importante du contrôle de l'environnement SI, les normes relatives à la configuration sécurisée de systèmes sont de plus en plus largement acceptées par les organisations et fournisseurs de technologies leaders ;
- **les contrôles applicatifs :** toutes les applications qui supportent les activités métiers doivent être contrôlées ;
- **la structure des données :** si l'on dispose de définitions de données homogènes dans la totalité des applications, des systèmes distribués peuvent accéder sans difficulté aux données, et des contrôles de sécurité peuvent être mis en place uniformément sur toutes les données à caractère personnel et autres données sensibles ;
- **la documentation :** des normes doivent spécifier le niveau de détail minimal de documentation requis pour chaque application ou implémentation informatique, ainsi que pour les différentes catégories d'applications, de procédures et de centres de traitement.[13]

Contrôles relatifs à l'organisation et à la gestion des SI

Contrôles qui donnent l'assurance que l'organisation est structurée selon des voies hiérarchiques et des responsabilités clairement définies et qu'elle applique des processus de contrôle efficaces.

Les *contrôles relatifs à l'organisation et à la gestion des SI* donnent l'assurance que l'organisation est structurée selon des voies hiérarchiques et des responsabilités clairement définies et qu'elle applique des processus de contrôle efficaces. Les trois aspects essentiels de ces contrôles sont la séparation des tâches, les contrôles financiers et les contrôles de la gestion du changement.

- La séparation des tâches est un élément crucial de nombreux contrôles. Une organisation doit être structurée de sorte que

Copyright © 2015 Eyrolles.

tous les aspects du traitement des données ne reposent jamais sur une seule personne. Les fonctions d'émission, d'autorisation, de saisie, de traitement et de vérification des données doivent être séparées afin qu'aucun individu ne puisse être à l'origine d'une erreur ou d'une omission ou de toute autre irrégularité et l'autoriser et/ou en masquer les preuves. Les contrôles de séparation des tâches concernant les applications sont mis en place par l'octroi d'accès privilégiés en fonction des exigences du poste en termes de traitement et d'accès aux données.[14]

- Étant donné que les organisations réalisent des investissements considérables dans les SI, des contrôles d'ordre budgétaire et financier sont nécessaires pour s'assurer qu'ils aboutissent au retour sur investissement ou aux économies annoncés. Il convient de mettre en place des procédures de gestion permettant de recueillir, d'analyser et de rendre compte de ces aspects. Malheureusement, les évolutions des SI induisent souvent des dépassements de coût massifs et ne se traduisent pas par les économies ou les revenus attendus, en raison d'estimations erronées ou d'une planification insuffisante.[15]
- Les procédures de gestion du changement s'assurent que les modifications apportées à l'environnement de SI, aux logiciels, aux applications et aux données doivent permettre de respecter une bonne séparation des tâches, d'assurer le bon fonctionnement des changements, d'empêcher l'exploitation de ces changements à des fins frauduleuses. Une faiblesse dans la gestion du changement pourrait sérieusement impacter le système et le service disponibles.[16]

Les *contrôles physiques et environnementaux des SI* protègent les ressources des systèmes d'information (matériel, logiciels, documentation et informations) d'une détérioration accidentelle ou intentionnelle, d'une utilisation abusive ou de la destruction. Voici quelques exemples de ces contrôles :

Contrôles physiques et environnementaux des SI

Contrôles qui protègent les ressources des systèmes d'information d'une détérioration accidentelle ou intentionnelle, d'une utilisation abusive ou de la destruction.

- l'installation des serveurs dans des locaux verrouillés et à accès restreint ;
- la limitation de l'accès aux serveurs à des personnes autorisées ;
- la mise en place de dispositifs de détection incendie et d'extincteurs ;
- l'installation des équipements, applications et données sensibles à distance des risques environnementaux, par exemple loin de zones inondables, des couloirs aériens ou de lieux de stockage de liquides inflammables.[17]

Les contrôles techniques des SI

« Les contrôles techniques sont souvent le socle des référentiels de contrôle du management. […] Ces contrôles sont différents selon

Copyright © 2015 Eyrolles.

les technologies en usage au sein de l'infrastructure SI de l'organisation. »[18] Comme le montre l'encadré 7-4, les contrôles techniques des SI sont les contrôles des logiciels système, les contrôles du développement des systèmes et les contrôles applicatifs.

Les logiciels « système » facilitent l'utilisation du matériel des systèmes. Il peut s'agir de systèmes d'exploitation, de logiciels de gestion de réseau, de systèmes de gestion de bases de données, de pare-feux ou d'antivirus. Les contrôles des logiciels système restreignent l'accès logique aux systèmes et applications de l'organisation, pilotent l'utilisation des systèmes et génèrent des pistes d'audit. Voici quelques exemples de contrôles des logiciels système :

- les droits d'accès sont attribués et contrôlés conformément à la politique énoncée par l'organisation ;
- les principes de séparation des tâches sont respectés grâce à des contrôles logiciels et d'autres contrôles de configuration ;
- des évaluations et des actions de prévention et de détection des intrusions et des vulnérabilités sont en place et suivies en continu ;
- des tests d'intrusion sont régulièrement réalisés ;
- des services de chiffrement sont mis en œuvre lorsque la confidentialité est explicitement requise ;
- des procédures de gestion des changements, y compris la gestion des patchs, sont en place, si bien que les changements et les patchs sont appliqués aux logiciels, systèmes, composants réseau et données selon une procédure étroitement encadrée.[19]

Qu'ils soient développés en interne ou achetés auprès d'un fournisseur, les systèmes d'application doivent traiter l'information avec efficacité et efficience, conformément aux besoins des utilisateurs. Voici quelques exemples de contrôles de l'acquisition et du développement des systèmes :

- les besoins des utilisateurs doivent être formalisés, et leur satisfaction mesurée ;
- la conception des systèmes doit suivre une procédure formelle qui permet de s'assurer que les besoins des utilisateurs et les contrôles sont bien intégrés dans le système ;
- le développement des systèmes doit être mené de manière structurée, afin que les besoins et les spécifications requis soient bien pris en compte dans le produit final ;
- les tests doivent vérifier que les différentes composantes du système opèrent de la façon requise, que les interfaces fonctionnent comme prévu, que les utilisateurs participent au processus de test et que les fonctionnalités attendues sont bien présentes ;

Copyright © 2015 Eyrolles.

- les procédures de maintenance des applications doivent permettre de s'assurer que tous les changements apportés aux applications répondent à un schéma de contrôle homogène. La gestion des changements doit faire l'objet de procédures structurées de validation de l'assurance.[20]

Les *contrôles applicatifs* veillent à ce que :

- toutes les données saisies soient exactes, complètes, autorisées et correctes ;
- toutes les données soient traitées comme prévu ;
- toutes les données stockées soient exactes et complètes ;
- tous les résultats soient exacts et complets ;
- le traitement des données fasse l'objet de traces (*logs*) depuis la saisie jusqu'au stockage et à la production de données de sortie.[21]

Les *contrôles applicatifs* sont par exemple :

- **les contrôles des données d'entrée :** ils servent essentiellement à vérifier l'intégrité des données saisies dans une application, qu'elles soient saisies directement par les utilisateurs, à distance par un partenaire ou à travers une application Web ;
- **les contrôles du traitement :** ils procurent un moyen automatisé de s'assurer que le traitement est complet, exact et autorisé ;
- **les contrôles des données de sortie :** ils portent sur ce qui est fait des données. Ils doivent comparer les résultats obtenus aux résultats attendus, et les vérifier par rapport à ce qui a été saisi ;
- **les contrôles d'intégrité :** ils peuvent s'appliquer de façon permanente sur les données en cours de traitement et/ou stockées, afin de s'assurer qu'elles restent cohérentes et exactes ;
- **la traçabilité :** le fait de traiter l'historique des contrôles, ce qu'on appelle souvent une piste d'audit, permet au management de suivre les transactions depuis la source jusqu'au résultat final ou de remonter à partir des résultats jusqu'aux transactions et aux événements enregistrés qui les ont générés.[22]

L'encadré 7-5 présente des exemples spécifiques de contrôles applicatifs.

Les contrôles de la sécurité de l'information

L'encadré 7-4 ne présente pas spécifiquement les contrôles de la sécurité de l'information, car « la sécurité informatique fait partie

Copyright © 2015 Eyrolles.

ENCADRÉ 7-5

EXEMPLES DE CONTRÔLES APPLICATIFS DES SI

Contrôles des données d'entrée : conçus pour veiller à ce que les données d'entrée dans le système soient valides, complètes et exactes.

- **Contrôles des documents « sources »**
  L'accès aux documents utilisés pour engager les transactions est restreint aux personnes autorisées.
  Les documents utilisés pour engager les transactions sont prénumérotés lorsque cela est possible. Les documents source sont utilisés par ordre numérique et l'ordre est vérifié périodiquement.
- **Totaux de contrôle**
  - Nombre d'enregistrements**. Décompte des enregistrements d'entrées pour le traitement. Exemple : le nombre de cartes de pointage présentées pour le traitement de la paye.**
  - Total du lot. **Total d'un montant inclus dans chaque enregistrement mis dans un lot pour le traitement. Exemple : le nombre total d'heures travaillées dans le lot des cartes de pointage présentées pour le calcul des heures payées.**
  - Total factice. **Total par ailleurs dépourvu de signification qui sert à veiller à l'exhaustivité des données d'entrée en vue du traitement. Exemple : la somme du nombre de collaborateurs dans le lot de cartes de pointage présentées pour calculer le nombre de payes.**
- **Contrôles d'édition programmés**
  - **Contrôle d'exhaustivité.** Examine les données d'entrée afin de vérifier que tous les champs critiques contiennent des valeurs.
  - **Contrôle de champ.** Examine un champ afin de vérifier s'il contient le type de données approprié (alpha ou numérique).
  - **Contrôle du signe.** Examine un champ afin de vérifier si le signe du chiffre est correct (positif ou négatif).
  - **Contrôle de valeur limite.** Examine un champ afin de vérifier si le montant est inférieur ou égal au plafond fixé ou supérieur ou égal au plancher fixé.
  - **Contrôle de la fourchette.** Examine un champ afin de vérifier si le montant entre dans une fourchette donnée.
  - **Contrôle de vraisemblance.** Compare les données présentes dans un champ avec celles présentes dans les champs voisins afin de vérifier si la valeur est vraisemblable.
  - **Contrôle de validité.** Compare les données présentes dans un champ avec un ensemble prédéterminé de valeurs autorisées afin de vérifier si le champ contient des données valides.
- **Correction des erreurs d'entrée :** les documents sources contenant des erreurs détectées pendant la saisie sont corrigés et soumis une nouvelle fois avant le traitement.

Contrôles du traitement : conçus pour prévenir ou pour détecter et corriger les erreurs qui se produisent pendant le traitement.

- **Totaux de contrôles intermédiaires :** les totaux de contrôles sont calculés et vérifiés à des points prédéterminés à mesure que les transactions se déroulent.
- **Listings d'erreurs :** les listings d'erreurs sont générés automatiquement par l'ordinateur et les erreurs détectées sont corrigées rapidement.

Contrôles des données de sortie : conçus pour veiller à ce que les données de sortie du système soient valides, complètes et exactes et à ce que la sécurité des sorties soit correctement assurée.

- **Contrôles d'examen des sorties :** examen de la validité, de l'exhaustivité et de l'exactitude des sorties des systèmes d'application avant leur distribution aux utilisateurs.
- **Contrôles de la distribution :** les sorties des systèmes d'application ne peuvent être distribuées qu'aux destinataires autorisés.
- **Contrôles par les utilisateurs finaux :** les utilisateurs finaux examinent la validité, l'exhaustivité et l'exactitude des sorties des systèmes d'application qu'ils reçoivent.

Contrôles de la traçabilité : conçus pour assurer un enregistrement permanent des entrées, des traitements et des sorties.

- **Journal des transactions :** le système d'application enregistre automatiquement dans un journal les transactions traitées.
- **Journal des contrôles programmés :** le système d'application enregistre automatiquement dans un journal les contrôles intégrés exécutés au moment des entrées, des traitements et des sorties.
- **Conservation des listes d'erreurs :** les listes d'erreurs générées automatiquement pendant le traitement et qui donnent lieu à des corrections sont conservées, non modifiables et d'accès facile.

Copyright © 2015 Eyrolles.

intégrante des contrôles des SI »[23]. Les contrôles de la sécurité de l'information protègent un système d'information d'un accès physique ou logique non autorisé. Les contrôles de l'accès physique assurent la sécurité des ressources de SI matérielles et peuvent revêtir la forme de portes verrouillées, de caméras de surveillance et de personnels de sécurité. Les contrôles de l'accès logique assurent la sécurité des logiciels et de l'information contenus dans le système et peuvent revêtir la forme de pare-feux, de chiffrement des données, d'identifiant d'accès, de mots de passe modifiés régulièrement, de tables d'autorisation et de journaux de l'activité des ordinateurs (*computer activity logs*). Les déficiences des contrôles de la sécurité de l'information menacent l'efficacité de la gouvernance et de la gestion des SI ainsi que des contrôles techniques.

Compte tenu du risque accru, lié à la cybersécurité, auquel les organisations sont confrontées, la *Securities and Exchange Commission* (SEC), aux États-Unis, a imposé une nouvelle réglementation en matière de reporting financier, en vigueur depuis octobre 2011. L'audit interne des contrôles de sécurité de l'information permettra de veiller à ce que les organisations adoptent une approche proactive pour gérer le risque lié à la cybersécurité et respectent les exigences de reporting plus strictes de la SEC.

CONSÉQUENCES DES SI POUR LES AUDITEURS INTERNES

Les sections précédentes du présent chapitre décrivent l'incidence des SI sur les organisations. Les SI font évoluer la manière dont les organisations formulent leurs stratégies, conduisent leurs opérations quotidiennement et prennent leurs décisions. Ces changements génèrent de nouveaux risques et contraignent les organisations à revoir leurs processus de gouvernance, de gestion des risques et de contrôle. En raison de l'incidence des SI sur toute l'organisation, les auditeurs internes sont contraints d'améliorer leur connaissance et leur maîtrise des SI et d'adapter leur façon de travailler.

Compétences dans les SI et conscience professionnelle

Deux Normes de qualification traitent spécifiquement des compétences que les auditeurs internes doivent posséder dans le domaine des SI et de la manière dont ils doivent envisager d'utiliser des techniques d'audit informatisées :

1210.A3 – Les auditeurs internes doivent posséder une connaissance suffisante des principaux risques et contrôles relatifs aux technologies de l'information, et des techniques d'audit informatisées susceptibles d'être mises en œuvre dans le cadre des travaux

Contrôles de l'accès physique

Contrôles assurant la sécurité des ressources de SI matérielles.

Contrôles de l'accès logique

Contrôles assurant la sécurité des logiciels et de l'information contenus dans le système.

Copyright © 2015 Eyrolles.

qui leur sont confiés. Toutefois, tous les auditeurs internes ne sont pas censés posséder l'expertise d'un auditeur dont la responsabilité première est l'audit informatique.

1220.A2 – Pour remplir ses fonctions avec conscience professionnelle, l'auditeur interne doit envisager l'utilisation de techniques informatiques d'audit et d'analyse des données.

Les Normes 1210.A3 et 1220.A2 indiquent clairement que tous les auditeurs internes qui réalisent des activités d'assurance ont besoin de disposer au minimum d'un niveau élémentaire d'expertise concernant les risques, les contrôles et l'audit des SI. Les concepts fondamentaux de risques et de contrôles relatifs aux SI que tous les auditeurs internes doivent comprendre sont présentés dans les sections précédentes du présent chapitre. Les techniques d'audit informatisées, encore appelées « techniques d'audit assistées par ordinateur » ou « outils informatiques d'aide à l'audit » (CAAT), sont décrites au chapitre 10, *Les preuves d'audit et les papiers de travail*. Les CAAT sont les logiciels d'audit généralisés comme ACL et IDEA. Les logiciels généraux d'audit constituent un exemple d'outil d'audit des SI que les fonctions d'audit interne demandent de plus en plus à leurs auditeurs de maîtriser et de savoir utiliser efficacement. Les logiciels utilitaires, les données de test, la cartographie et l'exécution pas à pas des logiciels d'application, les systèmes experts d'audit ainsi que l'audit continu sont les autres techniques d'audit informatisées décrites au chapitre 10.

En outre, la plupart des fonctions d'audit interne disposent d'un système *ad hoc* servant à automatiser l'élaboration des papiers de travail, comme TeamMate, afin de documenter, d'organiser et de citer en référence les travaux d'audit interne. Ce type de système a permis d'améliorer considérablement la documentation sous-jacente aux travaux d'audit interne, dans la mesure où ceux-ci sont réalisés de manière plus efficace et efficiente.

La Norme 1210.A3 précise cependant que tous les auditeurs internes ne sont pas censés posséder l'expertise d'un auditeur spécialiste des SI dont la responsabilité première est l'audit informatique. Cependant, dans la mesure où la demande d'auditeurs des SI très qualifiés continue d'excéder l'offre, les lecteurs intéressés par ce domaine sont vivement encouragés à se renseigner davantage sur les compétences et les qualifications nécessaires pour réussir dans la profession d'auditeur spécialiste des SI. Ces personnes souhaiteront peut-être obtenir des certifications dans le domaine du contrôle des SI afin de compléter leur qualification de *Certified Internal Auditor* (CIA, auditeur interne certifié). Il existe notamment la certification *Certified Information Systems Auditor* (CISA, certification en audit des systèmes d'information), délivrée par l'ISACA (www.isaca.org), et la certification *Certified Information Systems Security Professional* (CISSP, certification professionnelle

Copyright © 2015 Eyrolles.

en sécurité des systèmes d'information), délivrée par l'*Information Systems Security Association* (www.issa.org).

Comme pour tous les autres domaines d'expertise pertinents, le responsable de l'audit interne doit veiller à ce que son service dispose des compétences nécessaires dans les SI pour pouvoir remplir ses missions d'assurance. Certaines fonctions d'audit interne disposent de compétences suffisantes dans les SI en interne. Lorsque ce n'est pas le cas, elles doivent chercher en externe cette expertise. Dans certains cas, elles peuvent demander à des personnes qualifiées travaillant dans d'autres services de l'organisation de participer aux missions d'audit requérant des compétences dans les SI qui font défaut au service d'audit interne. Dans d'autres cas, le responsable de l'audit interne fera appel à des prestataires extérieurs pour combler cette absence de compétence.

Responsabilités relatives aux SI pendant les missions d'assurance

Trois Normes de fonctionnement traitent spécifiquement des responsabilités des auditeurs internes concernant les systèmes et les technologies de l'information pendant les missions d'assurance :

2110.A2 – L'audit interne doit évaluer si la gouvernance des systèmes d'information de l'organisation soutient la stratégie et les objectifs de l'organisation.

2120.A1 – L'audit interne doit évaluer les risques afférents […] aux systèmes d'information de l'organisation […].

2130.A1 – L'audit interne doit évaluer la pertinence et l'efficacité du dispositif de contrôle choisi pour faire face aux risques relatifs […] aux systèmes d'information de l'organisation […].

Ces trois normes traduisent le fait qu'une fonction d'audit interne ne peut pas évaluer correctement les processus de gouvernance, de gestion des risques et de contrôle sans prendre dûment en considération les systèmes et technologies de l'information. Pour pouvoir assumer ses responsabilités dans le domaine des SI, une fonction d'audit interne doit :

- inclure les systèmes d'information de l'organisation dans son processus de planification annuel des travaux d'audit ;
- repérer et évaluer les risques SI qu'encourt l'organisation ;
- veiller à disposer d'une expertise suffisante dans le domaine des SI ;
- évaluer les contrôles relatifs à la gouvernance et à la gestion des SI ainsi que les contrôles techniques ;

Copyright © 2015 Eyrolles.

- affecter des auditeurs présentant un niveau de compétences suffisant dans les SI à chaque mission d'assurance ;
- utiliser à bon escient les techniques d'audit informatisées.

Externalisation des SI (ou infogérance)

Externalisation des SI (ou infogérance)

Transfert d'une partie des fonctions SI à un prestataire extérieur, afin de réduire les coûts tout en améliorant la qualité et l'efficience du service.

L'externalisation des processus opérationnels a été traitée au chapitre 5, *Les processus et les risques*, et décrite comme l'acte qui consiste à transférer une partie des processus opérationnels d'une organisation à un prestataire extérieur, afin de réduire les coûts tout en améliorant la qualité et l'efficience du service. Ce sont ces raisons qui poussent les organisations à externaliser de plus en plus leurs fonctions SI à des prestataires spécialisés dans ces services.

Comme c'est le cas pour tout type d'externalisation, l'externalisation des SI, ou infogérance, comporte des risques que le Conseil et la direction générale doivent comprendre et gérer. Ils rechercheront donc à obtenir une assurance à propos des informations sur lesquelles ils fonderont leurs décisions d'externalisation. L'audit interne peut leur donner cette assurance et les informer des conséquences d'une externalisation des SI sur les risques et les contrôles à mettre en place.

Le Conseil et la direction générale conservent également la responsabilité des contrôles sur les fonctions SI externalisées et demanderont au responsable de l'audit interne de leur donner une assurance concernant l'adéquation de la conception et le fonctionnement effectif de ces contrôles. Suivant les circonstances, le responsable de l'audit interne pourra, dans une certaine mesure, s'appuyer sur les rapports communiqués par les auditeurs externes et/ou les auditeurs internes du prestataire de services SI afin de formuler une conclusion sur les contrôles des fonctions SI externalisées. Si des fonctions SI très risquées ont été externalisées, le responsable de l'audit interne doit affecter le niveau requis de ressources d'audit interne à la vérification des contrôles sur ces fonctions. Le GTAG 7, « L'infogérance », décrit en détail certains des principaux aspects de l'externalisation des SI que les auditeurs internes doivent prendre en considération.

Audit intégré et continu

Dans le passé, les audits internes étaient habituellement exécutés rétrospectivement, par exemple une fois que les transactions étaient réalisées. Cette approche est en train de devenir obsolète, car les progrès de la technologie donnent naissance à des processus opérationnels informatisés permettant le traitement en ligne et en temps réel des transactions. Les pistes d'audit sur papier du traitement des transactions et des contrôles sont de plus en plus

Copyright © 2015 Eyrolles.

souvent remplacées par des pistes virtuelles et des contrôles automatisés intégrés conçus pour tester l'adéquation des transactions au moment où elles se déroulent. Dans un tel environnement, les preuves directes du traitement des transactions et de la mise en œuvre des contrôles sont produites en temps réel et donc, par nature, souvent temporaires. Il est donc de moins en moins possible pour les auditeurs internes de mener leur audit « autour » de l'ordinateur afin de parvenir à une conclusion valide à propos de l'efficacité globale des contrôles relatifs au reporting financier, aux opérations et à la conformité. Ils doivent aujourd'hui mener leur audit « par l'ordinateur », à l'aide des techniques d'audit assistées par ordinateur (CAAT), afin d'évaluer les contrôles des SI intégrés au système.

Intégration de l'audit des SI dans les missions d'assurance. L'intégration des contrôles des SI directement dans les processus opérationnels, ainsi que l'existence d'outils informatiques conviviaux, incitent de plus en plus de fonctions d'audit interne à modifier leur approche d'audit. Au lieu de réaliser des missions d'assurance distinctes, strictement consacrées aux risques et aux contrôles relatifs aux SI au niveau des processus, ces fonctions d'audit interne intègrent l'évaluation des risques et des contrôles des SI dans les missions d'assurance visant à évaluer les risques et les contrôles relatifs au reporting financier, aux opérations et/ou à la conformité au niveau des processus.

Audit intégré

Intégration de l'évaluation des risques et des contrôles des SI dans les missions d'assurance visant à évaluer les risques et les contrôles relatifs au reporting financier, aux opérations et/ou à la conformité au niveau des processus.

Les fonctions d'audit interne qui ont opté pour cette approche constatent que leur organisation en tire des avantages, car elle améliore l'efficacité et l'efficience de leurs activités d'assurance. Les missions d'assurance intégrées sont plus efficaces, car les auditeurs internes sont bien mieux placés pour évaluer l'intégralité du portefeuille de risques de l'audité et en tirer une conclusion globale à propos de l'adéquation de la conception et du fonctionnement effectif des contrôles. L'efficience du processus d'audit s'en trouve renforcée du fait que :

- les missions qui étaient autrefois menées séparément sont aujourd'hui regroupées ;
- la détection et l'évaluation de tous les principaux risques et contrôles sont fusionnées dans les missions d'audit intégré.

Audit continu. Le GTAG 3, « Audit continu : répercussions sur l'assurance, le pilotage et l'évaluation des risques », définit l'audit continu comme « toute méthode utilisée par les auditeurs pour accomplir leurs activités d'audit de manière plus continue ou continuelle »[24]. Comme l'indique le GTAG 3, l'audit continu est constitué de deux composantes majeures :

- l'*évaluation continue des contrôles*, « qui attire dès que possible l'attention des auditeurs sur les défaillances des contrôles » ;

Copyright © 2015 Eyrolles.

- l'*évaluation continue du risque*, « qui fait ressortir les processus et les systèmes qui affichent un niveau de risque supérieur à celui qui est prévu »[25].

Cependant, il est possible de définir une troisième composante de l'audit continu qui est relative à l'évaluation du pilotage continu. En effet, comme nous l'avons précisé précédemment dans ce chapitre, le management a un rôle essentiel dans le pilotage du processus de gestion des risques et du dispositif de contrôle interne. Il doit s'assurer notamment que le dispositif fonctionne de manière efficace et efficiente. La responsabilité de l'audit interne est alors d'évaluer l'efficacité de cette activité de pilotage continue menée par le management. Dans les services au sein desquels le management a mis en place un processus de pilotage continu efficace, les auditeurs internes pourront alléger leurs diligences en matière d'évaluation des risques et des contrôles. En revanche, si le pilotage continu est inexistant ou inefficace, l'audit interne doit procéder à des évaluations continues plus strictes des risques et des contrôles.

PRINCIPALES SOURCES DE LIGNES DIRECTRICES RELATIVES À L'AUDIT DES SI

L'IIA dispose d'un corpus, en constant développement, de lignes directrices relatives à l'audit des SI. Les deux principales références sont les *Global Technology Audit Guides* (Guides pratiques d'audit des technologies de l'information, GTAG) et les *Guides to the Assessment of IT Risk* (Guides de l'évaluation des contrôles informatiques généraux basée sur les risques, GAIT), compris dans le Cadre de référence international des pratiques professionnelles de l'audit interne de l'IIA.

- **Les GTAG.** Les GTAG « aborde[nt] une question d'actualité liée à la gestion, au contrôle ou à la sécurité des technologies de l'information »[26]. L'encadré 7-1 énumère les GTAG disponibles à l'heure où le présent manuel est publié.
- **Les GAIT.** Les GAIT décrivent « la relation entre les risques opérationnels, les principaux contrôles des processus opérationnels, les contrôles automatisés et les autres fonctions SI critiques, ainsi que les contrôles généraux des SI. Chaque guide couvre un aspect spécifique de l'évaluation des risques et des contrôles relatifs aux SI »[27]. L'encadré 7-1 énumère les GAIT disponibles à l'heure où le présent manuel est publié.

Les membres de l'IIA peuvent télécharger gratuitement ces guides pratiques sur le site de l'IIA ou sur celui d'Instituts locaux tels que l'IFACI. Il est également possible de les acheter auprès de la librairie de la fondation pour la recherche de l'IIA, The IIA Research Foundation Bookstore, à l'adresse http://www.theiia.org/bookstore/.

GTAG (*Global Technology Audit Guides*)

Guides fournissant aux auditeurs internes des orientations qui leur permettront de mieux comprendre les questions relatives à la gouvernance, à la gestion des risques et aux contrôles qui entourent les SI.

GAIT (*Guides to the Assessment of IT Risk*)

Guides décrivant la relation entre les risques liés au reporting financier, les principaux contrôles des processus, les contrôles automatisés et les autres fonctions SI critiques, ainsi que les contrôles généraux des SI.

Copyright © 2015 Eyrolles.

On peut aussi se procurer auprès de l'IIA divers autres documents sur l'audit des SI :

- de nombreuses publications, y compris les manuels et monographies de l'IIA Research Foundation, que l'on peut acquérir auprès de la librairie de cette fondation ;
- la section *ITAudit Internal Auditor Online* propose des articles en ligne sur l'audit des SI. Le public peut télécharger les derniers articles parus ainsi que les archives depuis l'adresse : www.theiia.org/intAuditor/itaudit/.

Beaucoup d'autres organisations mettent en ligne des informations sur l'audit des SI qui peuvent intéresser les auditeurs internes et que l'on peut télécharger. Ces organisations sont notamment :

- l'IT Governance Institute (www.itgi.org) ;
- l'IT Compliance Institute (www.itcinstitute.com) ;
- l'IT Process Institute (www.itpi.org) ;
- l'ISACA (www.isaca.org) ;
- l'Information Systems Security Association (www.issa.org) ;
- l'American Institute of Certified Public Accountants (www.aicpa.org) ;
- l'Institut canadien des comptables agréés (www.icca.org).

Problématiques relatives aux risques associés aux systèmes d'information émergents.

De nouveaux systèmes d'information continueront d'émerger à un rythme effréné. Ces systèmes d'information sont généralement développés dans un but précis. Des contrôles sont ensuite introduits afin de maîtriser les risques SI. Les progrès des SI constatés à l'extérieur de l'organisation ne peuvent plus être ignorés. Comme indiqué plus haut dans ce chapitre, nombre des progrès récemment observés dans le domaine des SI, tels que les smartphones, les réseaux sociaux et le *cloud computing*, influent sur le profil de risque d'une organisation, même si celle-ci n'utilise pas la technologie considérée. Il est important que l'organisation anticipe les innovations technologiques à venir et les prenne en compte dans son évaluation des risques SI. L'audit interne peut apporter un point de vue utile à l'organisation en lui expliquant comment les nouvelles technologies influeront sur son avenir et comment elle pourra traiter les risques imminents de manière proactive.

Copyright © 2015 Eyrolles.

OPPORTUNITÉS POUR UN POINT DE VUE DE L'AUDIT INTERNE

Comme indiqué tout au long de ce chapitre, les SI sont essentiels pour assurer la réussite d'une organisation. L'audit interne peut réaliser des activités de conseil afin d'aider le management à traiter les nouveaux risques SI au fur et à mesure qu'ils émergent. L'encadré 7-6 présente 10 opportunités pour l'audit interne d'apporter son point de vue concernant les risques et les contrôles relatifs aux SI.

ENCADRÉ 7-6

APPORTER SON POINT DE VUE SUR LES RISQUES ET LES CONTRÔLES RELATIFS AUX SI
10 OPPORTUNITÉS POUR L'AUDIT INTERNE

- S'assurer que les risques SI sont pris en compte dans l'évaluation annuelle des risques.
- Apporter un point de vue dans le cadre des projets de développement de nouveaux systèmes et d'infrastructure des SI.
- Intégrer la revue des SI dans chaque audit.
- Comprendre comment les SI peuvent améliorer la productivité de l'audit interne et le processus de contrôle au sein de l'organisation.
- Formuler des recommandations en matière de contrôle dans le cadre du déploiement de nouvelles technologies.
- Informer le management sur les risques SI émergents et sur les contrôles qui peuvent être mis en œuvre pour maîtriser ces risques.
- Se porter volontaire pour piloter les projets SI émergents et apporter un point de vue en matière de contrôle avant le déploiement de nouvelles technologies.
- Employer des spécialistes des SI en qualité d'experts du domaine lors des missions d'audit qui impliquent un haut degré de complexité des SI.
- Tenir la direction générale et le Conseil informés des risques SI majeurs susceptibles d'affecter l'organisation.
- Comprendre les nouvelles technologies qui ont un impact sur l'organisation, que celle-ci les utilise ou non.

RÉSUMÉ

L'omniprésence des SI dans les stratégies, les systèmes et les processus des organisations exerce une influence significative sur la profession d'audit interne. Ce chapitre couvre les concepts fondamentaux des SI que tout auditeur interne a besoin de comprendre.

- Il décrit et illustre les six principales composantes des systèmes d'information : matériel informatique, réseaux, logiciels, bases de données, informations et ressources humaines.
- Il analyse les opportunités et les risques résultant des SI. Parmi les opportunités, citons le commerce électronique, l'intégration

Copyright © 2015 Eyrolles.

des processus opérationnels et l'échange électronique de données entre partenaires. Mais les organisations et les secteurs ont aussi en commun plusieurs risques :

- sélection ;
- développement/acquisition et déploiement ;
- indisponibilité ;
- matériel/logiciel ;
- accès ;
- manque de fiabilité du système et d'intégrité de l'information ;
- violation de la confidentialité des données personnelles ;
- fraude et actes malveillants.

- Ce chapitre décrit la gouvernance des SI comme un sous-ensemble important de la gouvernance. Il explique la gestion des risques SI dans le contexte du dispositif de management des risques du COSO et présente les contrôles relatifs aux SI selon une hiérarchie descendante, qui va des contrôles relatifs à la gouvernance des SI aux contrôles relatifs à la gestion des SI, puis enfin aux contrôles techniques.
- Ce chapitre traite des conséquences des SI pour les auditeurs internes. Les fonctions d'audit interne ont besoin de comprendre les systèmes d'information de leur organisation, ainsi que les risques SI qui menacent la réalisation de ses objectifs. Ils doivent également savoir évaluer la gouvernance, la gestion des risques et les contrôles relatifs aux SI de leur organisation et être capables d'appliquer correctement les techniques d'audit informatisées.
- Ce chapitre présente les principales sources de lignes directrices relatives à l'audit des SI. Les deux principales composantes du corpus, en constant développement, publié par l'IIA à propos de l'audit des SI, sont les GTAG et les GAIT. D'autres lignes directrices sont disponibles auprès de l'IIA. Il est également possible d'acheter de nombreux documents auprès de la librairie de la fondation pour la recherche de l'IIA, *The IIA Research Foundation Bookstore*, et de télécharger des documents relatifs aux tendances et pratiques actuelles dans la section *ITAudit Internal Auditor Online*.

En résumé, les SI ont radicalement transformé les compétences que les auditeurs internes doivent posséder et leur manière de travailler. Pour qu'une fonction d'audit interne soit en mesure de réaliser des activités d'assurance et de conseil de qualité, elle doit maîtriser les aspects liés aux SI, que ce soit par ses propres compétences en interne ou par le recours à une compétence externe. Tous les auditeurs internes doivent posséder des connaissances et des compétences technologiques élémentaires. Ils doivent notamment maîtriser les systèmes servant à automatiser l'élaboration des papiers de travail, les outils informatiques d'aide à l'audit et

Copyright © 2015 Eyrolles.

la terminologie relative aux SI. L'audit interne peut apporter un point de vue quant à la manière dont l'organisation peut tirer le meilleur parti des progrès des SI.

Copyright © 2015 Eyrolles.

Questions de révision

1. Quelles sont les six composantes des SI décrites dans le présent chapitre ?

2. En quoi les SI ouvrent-ils des opportunités ? Citez deux exemples.

3. Quels sont les effets potentiels (conséquences négatives) de chacune des catégories de risques SI suivantes ?
   a. Développement/acquisition et déploiement.
   b. Matériel/logiciel.
   c. Manque de fiabilité du système et d'intégrité de l'information.
   d. Fraude et actes malveillants.

4. Quelles sont les causes habituelles de chacune des catégories de risques SI suivantes ?
   a. Sélection.
   b. Indisponibilité.
   c. Accès.
   d. Violation de la confidentialité des données personnelles.

5. Comment l'IIA définit-il la gouvernance des SI ?

6. Dans quelle mesure chacun des éléments suivants du dispositif de management des risques du COSO est-il pertinent pour la gestion des risques SI ?
   a. Fixation des objectifs.
   b. Évaluation des risques.
   c. Traitement des risques.
   d. Information et communication.

7. Quelle est la différence entre les contrôles généraux et les contrôles applicatifs ?

8. Sur quoi portent les contrôles relatifs à la gouvernance des SI (c'est-à-dire à la politique des SI) ?

9. Quelles sont les trois catégories de contrôles relatifs à la gestion des SI décrites dans le présent chapitre ? Citez deux exemples pour chacune.

10. Quelles sont les trois catégories de contrôles techniques des SI décrites dans le présent chapitre ? Citez deux exemples pour chacune.

11. Quelle est la différence entre les contrôles relatifs à l'accès physique et les contrôles relatifs à l'accès logique ?

Copyright © 2015 Eyrolles.



Questions de révision

12. Quelles sont les deux Normes de qualification qui traitent spécifiquement des compétences que les auditeurs internes doivent posséder dans le domaine des SI et de la manière dont ils doivent envisager d'utiliser des techniques d'audit informatisées ?

13. Quelles sont les trois Normes de fonctionnement qui traitent spécifiquement des responsabilités des auditeurs internes concernant les systèmes et les technologies de l'information pendant les missions d'assurance ?

14. Que doit faire une fonction d'audit interne pour respecter ses responsabilités relatives aux SI concernant une évaluation efficace de la gouvernance, de la gestion des risques et des contrôles ?

15. Quel peut être l'impact pour l'audit interne d'une externalisation des SI ?

16. Comment l'intégration de l'audit des SI dans les missions d'assurance peut-elle améliorer l'efficacité et l'efficience de l'audit ?

17. Quels sont les trois types d'évaluations pratiquées dans l'audit continu ?

18. Quels sont les deux types de guides pratiques sur les SI compris dans le Cadre de référence international des pratiques professionnelles de l'audit interne de l'IIA ?

Copyright © 2015 Eyrolles.

Questions à choix multiples

Sélectionnez la meilleure réponse pour chacune des questions suivantes.

1. Un logiciel qui gère l'interconnectivité des éléments matériels du système est :
   a. Un logiciel d'application.
   b. Un utilitaire.
   c. Un système d'exploitation.
   d. Un logiciel de gestion de bases de données.

2. Un pare-feu sur Internet est conçu pour apporter une protection contre :
   a. Les virus informatiques.
   b. Les accès non autorisés des tiers.
   c. La foudre et les surtensions.
   d. Les incendies.

3. Parmi les propositions suivantes, laquelle illustre le mieux l'utilisation de l'échange de données informatisées (EDI) ?
   a. L'achat de marchandises sur le site Internet d'une organisation.
   b. Le placement informatisé d'un ordre d'achat par un client chez son fournisseur.
   c. Le transfert de données d'un ordinateur de bureau vers un serveur de bases de données.
   d. Le retrait d'argent liquide à un distributeur automatique de billets.

4. La possibilité que quelqu'un bloque de manière malveillante un système d'information relève essentiellement :
   a. Du risque d'indisponibilité.
   b. Du risque lié à l'accès.
   c. Du risque lié à la violation de la confidentialité.
   d. Du risque de déploiement.

5. Le comité chargé de la gouvernance des SI au sein d'une organisation est investi de plusieurs responsabilités importantes. Parmi les propositions suivantes, laquelle ne désigne pas normalement l'une de ces responsabilités ?
   a. Aligner l'investissement dans les SI sur la stratégie de l'organisation.
   b. Superviser les changements apportés aux SI.
   c. Piloter les procédures de sécurité des SI.
   d. Concevoir des contrôles applicatifs des SI.

Copyright © 2015 Eyrolles.

6. Si la saisie d'une transaction de vente est refusée parce que le numéro de compte client saisi ne figure pas dans la liste des clients du fichier maître, l'erreur sera, selon toute probabilité, détectée par un :
   a. Contrôle d'exhaustivité.
   b. Contrôle de valeur limite.
   c. Contrôle de validité.
   d. Contrôle de vraisemblance.

7. Les contrôles relatifs à la sécurité logique ont pour objectif :
   a. De restreindre l'accès aux données.
   b. De limiter l'accès au matériel.
   c. D'enregistrer les résultats du traitement.
   d. De veiller à un traitement des données complet et exact.

8. Parmi les affirmations suivantes concernant les responsabilités d'une fonction interne s'agissant de l'audit continu, laquelle/lesquelles est/sont vraie(s) ?
   I. L'audit interne est chargé d'évaluer l'efficacité des activités de pilotage continu du management.
   II. Dans les services au sein desquels le management a mis en place un processus de pilotage continu efficace, les auditeurs internes pourront alléger leurs diligences en matière d'évaluation des risques et des contrôles.
   a. Seule l'affirmation I est vraie.
   b. Seule l'affirmation II est vraie.
   c. Les affirmations I et II sont vraies.
   d. Aucune affirmation n'est vraie.

Copyright © 2015 Eyrolles.

Thèmes de discussion

1. a. Comme indiqué dans le présent chapitre, tous les auditeurs internes doivent posséder *a minima* des notions élémentaires de l'audit des SI.
   I. Citez six compétences spécifiques liées aux SI (savoir et compétences) que tous les auditeurs internes débutants doivent posséder.
   II. Décrivez comment un étudiant à l'université peut commencer à acquérir le savoir et les compétences décrits ci-dessus.

   b. Tous les auditeurs internes doivent-ils obligatoirement posséder le niveau de maîtrise de l'audit des SI attendu d'un auditeur des SI ? Expliquez pourquoi.

2. Le risque, le risque inhérent et la fraude sont définis comme suit dans le glossaire du présent manuel :

   Risque – Possibilité qu'un événement se produise et ait une incidence défavorable sur la réalisation des objectifs.
   Risque inhérent – Combinaison de facteurs de risque internes et externes sous leur forme pure, non maîtrisée, autrement dit le risque brut qui existe en l'absence de mesures correctives internes.
   Fraude – Tout acte illégal caractérisé par la tromperie, la dissimulation ou la violation de la confiance sans qu'il y ait eu violence ou menace de violence. Les fraudes sont perpétrées par des personnes et des organisations afin d'obtenir de l'argent, des biens ou des services, d'éviter un paiement ou la perte de services ou de s'assurer un avantage personnel ou commercial.

Le présent chapitre définit le risque de fraude et d'actes malveillants dans le domaine des SI de la manière suivante :

> **Risque de fraude et d'actes malveillants dans le domaine des SI –** Le vol de ressources SI, l'utilisation abusive intentionnelle de ces ressources ou la distorsion/destruction intentionnelle d'informations peuvent entraîner un préjudice financier et/ou la communication d'informations erronées sur lesquelles s'appuieront les décideurs. Il existe un risque de fraude et d'actes malveillants par exemple lorsque des collaborateurs mécontents et des pirates informatiques (*hackers*) cherchent à nuire à l'organisation pour en tirer un bénéfice personnel.

En vous fondant sur les définitions ci-dessus, citez six risques de fraude et d'actes malveillants propres au domaine des SI qui sont susceptibles de porter atteinte à l'organisation.

3. Téléchargez sur le site Internet de Deloitte États-Unis (www.deloitte.com) le livre blanc « *The Risk Intelligent IT Internal Auditor* » et lisez-le.

   a. Quelles sont les caractéristiques d'un groupe d'audit interne des SI de type 1 (« *Drifting Along* ») ?

   b. Quelles sont les problématiques relatives à un :
   - groupe d'audit interne des SI de type 2 (« Getting Aloft ») ?
   - groupe d'audit interne des SI de type 3 : (« Flying High ») ?

Copyright © 2015 Eyrolles.

4. Les contrôles de la gestion du changement correspondent à un type de contrôle relatif à l'organisation et à la gestion des SI. Ils forment un sous-ensemble des contrôles (généraux) relatifs à la gestion SI.
   a. Que sont les contrôles de la gestion du changement ?
   b. Supposez que les contrôles de la gestion du changement d'une organisation concernant un logiciel d'application soient inefficaces. Quel impact cela aurait-il sur la confiance que le management peut placer dans les contrôles applicatifs ?
   c. Supposez au contraire que les contrôles de la gestion du changement concernant un logiciel d'application soient efficaces. Supposez également que l'audit interne a déterminé que les contrôles intégrés dans le logiciel d'application du processus d'achat ont été conçus de manière adéquate et ont fonctionné de manière effective au cours de l'exercice passé. Quel impact cela aurait-il sur les tests pratiqués cette année par l'audit interne sur les contrôles intégrés dans le logiciel d'application du processus d'achat ?
   d. Sur la base des réponses aux questions 2.b. et 2.c. ci-dessus, quelle conclusion générale peut-on tirer à propos de la relation entre les contrôles (généraux) relatifs à la gestion SI et les contrôles applicatifs ?

5. Téléchargez *COBIT® 5: A Business Framework for the Governance and Management of Enterprise IT* sur le site Internet de l'ISACA (www.isaca.org). (Remarque : déposez une demande à l'adresse suivante pour recevoir ce document par courriel : www.isaca.org/COBIT/Pages/Cobit-5-Framework-product-page.aspx.). Lisez la Synthèse (pages 13-14).
   a. Que dit la Synthèse à propos de l'information et des SI ?
   b. Quel est l'objectif du *COBIT® 5* ?
   c. Quels sont les cinq principes du *COBIT® 5* ?
   d. Selon le *COBIT® 5*, quelle est la différence entre la gouvernance et la gestion ?

6. Rendez-vous sur le site www.webtrust.org. Lisez la « Présentation des services Trust » ainsi que les paragraphes suivants relatifs aux « Principes et critères » :
   - Introduction (paragraphes .01– .18).
   - Paragraphe .19, qui décrit le principe de sécurité.
   - Paragraphe .21– .22, qui décrit le principe de disponibilité.
   - Paragraphe .24– .26, qui décrit le principe d'intégrité du traitement.
   - Paragraphe .28– .31, qui décrit le principe de confidentialité.
   - Paragraphe .33– .44, qui décrit le principe de protection de la vie privée.

   a. Que sont les services Trust ? Qu'est-ce que le service WebTrust ? Qu'est-ce que le service SysTrust ?
   b. Quels sont les principes, les critères et les exemples de contrôles des services Trust ?
   c. Comment le terme « système » est-il défini ?

Copyright © 2015 Eyrolles.

Thèmes de discussion

d. Qu'est-ce que le principe de *sécurité* ?

e. Qu'est-ce que le principe de *disponibilité* ?

f. Qu'est-ce que le principe d'*intégrité du traitement* ? Quelle est la différence entre l'*intégrité du traitement* et l'intégrité des données ?

g. Qu'est-ce que le principe de *confidentialité* ? Quelles informations peuvent être confidentielles ?

h. Que signifie le terme « protection de la vie privée » ? Donnez des exemples d'« informations personnelles ». Donnez des exemples d'« informations personnelles sensibles ». Quelle est la différence entre protection de la vie privée et confidentialité ? Qu'est-ce que l'objectif de protection de la vie privée ? Quels sont les 10 principes de protection de la vie privée généralement reconnus ?

7. Téléchargez « Le contrôle interne du système d'information des organisations »[28] sur le site de l'IFACI dans la base documentaire métier, rubrique informatique. Lisez les parties suivantes de ce document : l'introduction et le chapitre 5.

a. Quels sont les trois types de contrôle selon le référentiel *COBIT* ?

b. Quelles sont les différentes responsabilités en termes de risque SI entre le responsable des risques et le directeur du système d'information ?

c. Quels sont les objectifs du dispositif de sécurité logique ?

d. Quelles sont les bonnes pratiques qui permettent de réduire le risque lié à la confidentialité ?

Copyright © 2015 Eyrolles.

ÉTUDE DE CAS

L'organisation MVF fabrique des pièces de moteur pour des tondeuses à gazon, des canons à neige et d'autres types de machines d'entretien de jardin. Elle emploie environ 300 ouvriers de production. Ces ouvriers sont répartis en deux équipes qui alternent et doivent parfois faire des heures supplémentaires.

Le responsable de l'audit interne de MVF a demandé à Alyssa Worcshard, auditrice interne dans sa première année d'exercice, de collecter des informations sur les contrôles du processus de paye des collaborateurs de la production. Alyssa Worcshard a examiné le processus, interviewé certains collaborateurs et réuni des pièces corroborant les informations suivantes à propos du processus.

Le service du personnel établit un formulaire lorsqu'un collaborateur de la production est embauché ou quitte l'organisation. Ces formulaires servent également à enregistrer les changements tels que les révisions de salaires, les retenues, les changements de nom et d'adresse, etc. Un collaborateur du service du personnel saisit les informations figurant dans le formulaire sur ordinateur chaque semaine, afin d'actualiser le fichier maître du personnel.

Les collaborateurs de la production utilisent une horloge de pointage pour enregistrer leurs heures de travail. À la fin de chaque semaine, les superviseurs collectent les cartes de pointage, vérifient le nombre d'heures travaillées pour chaque collaborateur et inscrivent le nombre total d'heures travaillées sur la carte de chaque collaborateur. Chaque superviseur compte aussi le nombre de cartes collectées et envoie le résultat par courriel au trésorier de MVF.

Tous les lundis matins, un collaborateur du service de la paye collecte les cartes de pointage de la semaine précédente auprès des superviseurs de la production, les trie par numéro de collaborateur, recalcule le total des heures pour chaque carte, saisit les données dans l'ordinateur et traite les salaires pour les collaborateurs de la production. Le système attribue automatiquement un numéro séquentiel à chaque chèque de salaire produit. Les chèques en blanc sont stockés dans une boîte à proximité de l'imprimante, afin d'être accessibles immédiatement. Des contrôles sont intégrés dans le logiciel d'application afin de détecter les numéros de collaborateurs invalides, les totaux horaires irréalistes, etc. L'ordinateur détermine également si des heures supplémentaires ont été effectuées ou si une prime de poste se justifie. Les données non valides sont imprimées sur un listing des erreurs.

Ensuite, le collaborateur du service de la paye :

- imprime le registre des payes et les chèques de paye ;
- classe les chèques en deux lots : l'un regroupe les chèques considérés comme valides, l'autre regroupe les chèques dont le numéro du collaborateur figure sur le listing des erreurs ;
- utilise les résultats de la procédure d'émission des chèques de paye pour actualiser le fichier maître du personnel ;

Copyright © 2015 Eyrolles.

- prépare l'entrée hebdomadaire dans le journal de la paye et inscrit l'entrée dans le grand livre général ;
- indique au manager du service paye que le traitement hebdomadaire des transactions de paye est terminé.

Le manager du service paye prépare une sauvegarde du fichier maître du personnel sur un DVD-ROM, qui sera stocké dans la salle informatique.

Les lots valides et invalides de chèques de paye sont envoyés directement au trésorier de MVF. Le trésorier confirme le nombre de chèques valides reçus en le comparant avec le nombre de cartes de pointage communiqué par les superviseurs de la production, signe les chèques valides et déchiquète les chèques non valides. Le trésorier range les chèques signés dans le coffre jusqu'à ce qu'ils soient remis aux superviseurs de la production, qui les distribuent le vendredi. Si un collaborateur est absent lorsque les chèques sont distribués, le superviseur retourne le chèque non réclamé au trésorier, qui le conserve dans le coffre jusqu'au retour du collaborateur.

A. Sur la base des informations présentées ci-dessus, et en tenant compte des contrôles manuels et automatisés, veuillez décrire :

   1. les points forts des contrôles du processus de traitement des payes de l'organisation MVF ;
   2. les déficiences de contrôle du processus de traitement des payes de l'organisation MVF.

B. La direction générale de l'organisation MVF, y compris le responsable de l'audit interne, comprend que le processus de traitement des payes doit être amélioré :

   1. trouvez plusieurs idées pour que l'organisation puisse utiliser plus efficacement les SI afin d'améliorer son processus de traitement des payes ;
   2. analysez les conséquences pour les risques et les contrôles des idées énoncées en réponse à la question B.1.

Copyright © 2015 Eyrolles.



Copyright © 2015 Eyrolles



CHAPITRE 8
LES RISQUES DE FRAUDE ET D'ACTES ILLÉGAUX

Objectifs pédagogiques

- Comprendre l'importance de la fraude et des actes illégaux dans le monde d'aujourd'hui.
- Présenter les différentes définitions de la fraude et des actes illégaux.
- Décrire le « Triangle de la fraude » et comprendre les raisons pour lesquelles ses trois éléments doivent coexister pour qu'il y ait fraude.
- Définir les types de fraude et les facteurs qui induisent un risque de fraude.
- Définir la gouvernance, la gestion des risques et le contrôle dans le contexte de la fraude.
- Décrire les techniques de prévention, de dissuasion et de détection de la fraude.
- Comprendre le comportement des fraudeurs.
- Décrire les responsabilités des auditeurs internes en matière de conformité et de lutte contre la fraude qui contribuent à la protection de l'organisation contre les infractions réglementaires.
- Comprendre l'évolution des responsabilités de l'audit interne, notamment le recours à des spécialistes de la lutte contre la fraude.

Le risque de fraude reste l'un des plus grands risques auxquels les organisations contemporaines sont confrontées. Qu'il s'agisse d'une fraude commise par un collaborateur, de collusion entre plusieurs collaborateurs ou d'une fraude commise par un tiers, il est probable que non seulement l'organisation qui en est victime subira une importante perte financière, mais également que sa réputation sera fortement entachée. Dans de nombreux cas, la fraude dans une société cotée entraîne rapidement une nette baisse du cours de Bourse et de la capitalisation boursière et peut être le signe avant-coureur de difficultés financières. Il semble effectivement exister une corrélation entre la fraude et les difficultés financières : la fraude peut engendrer des difficultés financières, mais il est fréquent que celles-ci favorisent la fraude. La fraude ayant de graves conséquences économiques, la direction générale et les organes de gouvernance s'attachent de plus en plus aux contrôles et aux programmes antifraude liés aux activités clés de l'organisation, à sa conformité réglementaire et aux marchés sur lesquels

Copyright © 2015 Eyrolles.

elle opère. Cet intérêt accru de la part des organes de gouvernance vient de la prise de conscience qu'un reporting financier frauduleux peut rapidement conduire à la faillite d'une organisation.

Les actes illégaux sont des activités menées par une entité en violation des lois et règlements auxquels elle est soumise dans une juridiction donnée. Ces dernières années, le ministère de la Justice américain (U.S. Department of Justice) a intensifié ses efforts pour poursuivre des organisations qui ont enfreint les dispositions du Foreign Corrupt Practices Act de 1977. Les auditeurs internes des grandes organisations ont souvent la responsabilité de veiller à la conformité réglementaire. L'évaluation du risque de fraude fait généralement partie des premières étapes de ce processus. De nouveaux rôles, tels que celui de responsable de la conformité (*chief compliance officer* – CCO) ou de directeur des risques (*chief risk officer* – CRO), apparaissent de plus en plus fréquemment dans de nombreuses organisations. La fonction d'audit interne peut être amenée à collaborer étroitement avec ces nouveaux responsables. En outre, dans certains cas, le responsable de l'audit interne peut se voir attribuer la responsabilité de la fonction conformité. Comme toujours, dans de telles circonstances, le responsable de l'audit interne devrait en premier lieu examiner toute atteinte potentielle à son indépendance ou à son objectivité.

Ce chapitre compare les différentes définitions de la fraude afin d'en illustrer ses diverses perceptions. Puis il s'intéresse au « Triangle de la fraude », qui permet de comprendre les principaux facteurs qui sont en général réunis pour qu'une fraude soit commise. Il énonce également les principes fondamentaux d'un programme de prévention et de détection de la fraude. Une bonne connaissance de ces principes permet de bien définir le rôle que l'audit interne peut jouer dans ce type de programme. L'analyse montre ensuite comment un programme de prévention et de détection de la fraude peut soutenir la structure de gouvernance d'une organisation. Cet aspect conduit tout naturellement à examiner l'importance d'une évaluation des risques de fraude et la façon dont cette évaluation permet à une organisation d'élaborer des contrôles préventifs et détectifs. Enfin, ce chapitre explore les répercussions de la fraude sur le rôle et les priorités de l'audit interne. Les *Normes internationales de l'IIA pour la pratique professionnelle de l'audit interne* (les *Normes*) font plusieurs fois référence aux responsabilités de l'audit interne en ce qui concerne la fraude.

LA FRAUDE DANS LES ORGANISATIONS AUJOURD'HUI

La fraude ne se limite pas à certains pays ou à certains secteurs. Elle peut toucher n'importe quelle organisation, n'importe quand. À l'aube du XXIe siècle, les grands scandales financiers qui ont éclaté aux États-Unis (affaires Enron et WorldCom, en particulier) ont fait la une des journaux dans le monde entier. Ils ont non

Copyright © 2015 Eyrolles.

seulement coûté des milliards aux investisseurs, mais aussi largement érodé la confiance dans les marchés financiers du monde entier. Cette situation a conduit notamment à l'adoption de la loi *Sarbanes-Oxley Act* (2002) aux États-Unis. Ces textes sont destinés à améliorer la gouvernance et à restaurer la confiance des investisseurs dans les marchés financiers.

ENCADRÉ 8-1

DISPOSITIONS DU CRIPP PERTINENTES RELATIVES AU CHAPITRE 8

Norme 1210 – Compétence
Norme 1220 – Conscience professionnelle
Norme 2060 – Rapports à la direction générale et au Conseil
Norme 2110 – Gouvernement d'entreprise
Norme 2120 – Management des risques
Norme 2210 – Objectifs de la mission

Modalité Pratique d'Application 1210-1 :	Compétence
Modalité Pratique d'Application 1210.A1-1 :	Recours à des prestataires externes
Modalité Pratique d'Application 1220-1 :	Conscience professionnelle
Modalité Pratique d'Application 2030-1 :	Gestion des ressources
Modalité Pratique d'Application 2060-1 :	Rapports à la direction générale et au Conseil

ENCADRÉ 8-2

EXEMPLES DE FRAUDES DANS LE MONDE

L'affaire SATYAM en Inde

En janvier 2009, B. Ramalinga Raju, président de *Satyam Computer Systems*, la quatrième plus grande entreprise indienne d'externalisation de technologies, a fait des révélations publiques surprenantes. Non seulement il a révélé que son groupe avait gonflé des chiffres pendant une longue période, mais il a également déploré que, malgré des efforts concertés pour truquer les comptes, il subsistait des différences entre le bénéfice réel et celui comptabilisé. Il a résumé ainsi la situation : « C'était comme chevaucher un tigre sans savoir comment en descendre sans être dévoré. »[1] Les révélations de M. Raju, qui dirigeait depuis une vingtaine d'années une organisation ayant pour clients plus d'une centaine d'organisations du classement Fortune 500 et qui, leader de son secteur, représentait l'Inde au Forum économique mondial de Davos, ont soulevé des questions peu confortables à propos de la gouvernance en Inde. Le *Central Bureau of Investigation* (CBI) du pays – l'équivalent du *Federal Bureau of Investigation* (FBI) des États-Unis – chargé des crimes les plus graves et les plus complexes commis en Inde a transmis en avril 2009 au tribunal d'Hyderabad des documents laissant présager selon lui d'un scandale qui vaudra à cette affaire le nom d'« Enron à l'indienne ».

Le CBI pense que M. Raju, deux de ses frères et quatre cadres de Satyam ont commis une fraude en établissant plus de 7 000 fausses factures et en créant des douzaines de faux relevés bancaires afin de gonfler le résultat de Satyam. Tout a commencé en décembre 2008, lorsque M. Raju a cherché à diversifier les activités de son groupe en rachetant Maytas Properties et Maytas Infra, deux organisations dirigées par ses fils. Dans le monde, un certain nombre d'investisseurs institutionnels ont fustigé cette stratégie impudente, qui consistait à intimider le Conseil d'administration de Satyam pour qu'il se plie à la volonté de son président (la plupart des administrateurs avaient démissionné avant les aveux de M. Raju). Le groupe Satyam emploie quelque 53 000 personnes dans 66 pays et est coté en bourse à Bombay, Amsterdam et New York.

Copyright © 2015 Eyrolles.

Le CBI a affirmé que les deux auditeurs, S. Gopala Krishnan et Srinivas Talluri, entre-temps suspendus, la division indienne de PricewaterhouseCoopers (PwC), avaient reçu des banques de Satyam des certificats de dépôt présentant « des écarts considérables par rapport aux chiffres fournis par le management du groupe ». Les auditeurs ont néanmoins certifié les comptes truqués[2]. MM. Krishnan et Talluri sont aujourd'hui en prison à Hyderabad, ainsi que d'autres inculpés.

En outre, le CBI affirme que ces auditeurs ont reçu pour les travaux d'audit qu'ils ont effectués pour Satyam une rémunération correspondant à plusieurs fois le prix du marché. Depuis janvier, un certain nombre d'investisseurs, furieux, exigent de savoir pourquoi les auditeurs n'ont pas décelé une fraude aussi systématique, qui a ébranlé la confiance dans les autorités de régulation et de supervision indiennes. Il est intéressant de noter qu'en Inde la presse n'a encore jamais évoqué l'existence d'une fonction d'audit interne chez Satyam Computer Services.

L'affaire du CBI pourrait venir alourdir les sanctions légales potentiellement énormes qu'encourt Satyam, notamment dans la perspective d'un recours collectif en justice (*class-action lawsuit*) de ses investisseurs américains et mondiaux. Cette affaire aura également des répercussions sur les autres grandes sociétés indiennes d'externalisation de SI, telles qu'Infosys, Wipro et Tata Consultancy Services entre autres, et sur la manière dont celles-ci renforcent leurs mécanismes et leurs structures de gouvernance et de contrôle interne, y compris leur fonction d'audit interne.

Le 13 avril 2009, Tech Mahindra, groupe du secteur des SI détenu en partie par BT (British Telecom), a accepté de racheter Satyam, même si la nature exacte du scandale restait un mystère. Au cours de la vente, réalisée aux enchères et facilitée par l'État indien, Satyam a été évaluée à un montant de 670 millions de livres environ. Cette vente a permis à Tech Mahindra de devenir un groupe d'externalisation comptant 75 000 collaborateurs.

D'autres affaires dans le monde

Il existe d'autres exemples notables de fraude financière massive dans le monde. On peut notamment citer : la fraude commise à la *Bank of Credit and Commerce International* (BCCI), au Royaume-Uni ; celle portant sur plusieurs milliards chez Parmalat, le géant italien des produits laitiers ; les nombreux retraitements des comptes de Nortel Networks, l'une des plus grandes organisations du Canada, qui a fini par déposer son bilan ; l'échec de la gouvernance d'Olympia, société japonaise spécialisée dans les appareils médicaux, dont les dirigeants ont dissimulé les pertes par le biais d'acquisitions inattendues et sans rapport entre elles ; des pots-de-vin « d'une ampleur et d'une portée géographique sans précédent » versés en Allemagne par le groupe Siemens à des fonctionnaires partout dans le monde ; la facilitation de l'évasion fiscale pour des clients d'UBS Suisse, le plus important gérant mondial de fonds de clients fortunés (N.B. : la soustraction fiscale n'est pas illégale en Suisse) ; l'implication du géant néerlandais de l'alimentation, Royal Ahold NV, dans une vaste manipulation de résultats financiers et dans une fraude de grande ampleur portant sur des titres ; et le reporting financier frauduleux réalisé pendant des années par Kanebo, grand groupe japonais de cosmétiques et de textiles.

L'« affaire Parmalat »

Parmalat (Italie) a été secouée fin 2003 par l'un des plus gros scandales financiers européens, qui l'a obligée à déclarer banqueroute avec un trou de 14 milliards d'euros dans les comptes de l'entreprise. Environ 135 000 épargnants italiens ont vu leurs économies englouties dans le krach de Parmalat. Avant sa faillite, fleuron de l'économie italienne, cette entreprise, qui employait 36 000 personnes dans 30 pays, regroupait une myriade de sociétés et était présente dans des domaines tels que le football avec le club de Parme ou encore dans le tourisme.

Le procès s'est ouvert le 5 juin 2006 au tribunal de Parme. L'ex-patron du groupe était jugé pour manipulation de cours de Bourse, entrave à l'activité des organes de surveillance et complicité de faux en bilan. Il a été condamné à dix ans de prison.

L'« affaire Ahold »

Aux Pays-Bas, Ahold, le numéro trois mondial de la grande distribution et le numéro deux continental, a reconnu en 2003 des manipulations comptables sur trois exercices portant sur quelque 500 millions de dollars et liées essentiellement à la surévaluation des profits opérationnels de sa filiale américaine

Copyright © 2015 Eyrolles.

L'« affaire Vivendi »

Le 2 juillet 2002, Jean-Marie Messier est débarqué de la présidence de Vivendi Universal après la publication d'une perte de 13,6 milliards d'euros en 2001. Quelques jours plus tard, l'ancienne direction du groupe devra répondre de ses actes devant la COB, l'Association de défense des actionnaires minoritaires (Adam), l'Association des petits porteurs actifs (Appac), et certains actionnaires américains qui intentent une procédure de « *class action* ». Le parquet de Paris ouvre une information judiciaire contre X pour publication de faux bilans et « diffusion d'informations fausses ou trompeuses sur les perspectives de VU en 2001 et 2002 ». Même s'il est toujours coupable, aux yeux de l'AMF, d'avoir menti à ses actionnaires, le 29 juin 2005, la cour d'appel de Paris rejette plusieurs reproches faits par l'autorité administrative et réduit les amendes infligées à 500 000 euros pour Jean-Marie Messier et 300 000 pour VU.

En janvier 2008, la brigade financière établit que le groupe a mis en œuvre « une communication financière résolument optimiste » et « des pratiques comptables agressives ». En juillet 2008, la SEC inflige à VU une amende de plus de 48 millions de dollars pour indemniser quelque 12 000 investisseurs bernés par des informations trompeuses. Le 22 octobre 2009, malgré l'avis du parquet qui avait demandé un non-lieu général, l'ancien PDG de Vivendi est renvoyé devant le tribunal correctionnel de Paris, pour être jugé pour « diffusion d'informations fausses ou trompeuses, manipulation de cours et abus de biens sociaux ». Les avocats du groupe de communication et de Jean-Marie Messier plaident l'erreur.

L'« affaire Kerviel »

Le 24 janvier 2008 la Société Générale annonce une perte record de 4,9 milliards d'euros. L'entreprise les impute à un de ses traders, Jérôme Kerviel, qui aurait délibérément fraudé en essayant de masquer le montant de ces opérations et aurait déjoué les contrôles grâce à des opérations fictives et à de fausses écritures. La commission bancaire a constaté des carences dans le contrôle interne et afflige à la banque une amende de 4 millions d'euros. Après plusieurs semaines de procès, le 5 octobre 2010 l'ex-trader de la Société Générale est condamné à 5 ans de prison dont 3 ans fermes et à payer la somme de 4.9 milliards d'euros de dommages et intérêts. Verdict dont il a fait appel considérant que sa hiérarchie était au courant de sa très forte exposition sur les marchés financiers.

L'« affaire BNP PARIBAS »

En mai 2014, une amende de 8.93 milliards de dollars était prononcée à l'encontre de BNP Paribas. La banque française était accusée par les autorités américaines d'avoir réalisé des opérations en dollars avec des pays sous embargo, comme le Soudan et l'Iran. BNP Paribas a accepté le 30 juin 2014 de plaider coupable de deux chefs d'accusation : « falsification de documents commerciaux » et « collusion ». Au total, ce sont 45 salariés qui ont été sanctionnés sous diverses formes.
Rappelons que la banque française n'est pas la seule à avoir été sanctionnée par les autorités américaines, d'autres banques l'ont été mais pour des montants inférieurs. En 2012, la banque néerlandaise ING avait dû s'acquitter d'une pénalité de 619 millions de dollars. Le Crédit suisse a également écopé d'une amende de 2 milliards de dollars.

---

1 Source : Courrier de B. Ramalinga Raju, en date du 7 janvier 2009, à l'intention du Conseil de Satyam Computer Systems.

2 Les références au rapport du CBI portant sur Satyam ont été supprimées du bulletin d'information en ligne envoyé aux membres de l'Institute of Chartered Accountants of India (avril 2009).

Ces informations proviennent de *Certified Fraud Examiners* (CFE) qui ont enquêté sur les différents cas.

- Les participants à l'étude de l'ACFE estiment que la fraude fait perdre aux organisations 5 % de leur chiffre d'affaires annuel, ce qui représente une légère baisse par rapport à l'estimation de

Corruption

Acte par lequel une personne exerce une influence indue lors d'une transaction commerciale, afin d'en tirer un avantage pour elle-même ou pour un tiers (par exemple, pots-de-vin, délits d'initié ou conflits d'intérêts), en violation de ses obligations vis-à-vis de son employeur ou des droits d'un tiers.

Copyright © 2015 Eyrolles.

6 % (pour les États-Unis uniquement) figurant dans le rapport de 2010. Ramenées au produit intérieur brut (PIB) mondial de 2011, les prévisions de pertes imputables à la fraude s'élèvent au total à plus de 3 500 milliards de dollars par an.

- Les cas de fraude sur le lieu de travail sont en règle générale extrêmement coûteux. Selon le rapport, la perte médiane due à ce type de fraude s'élève à 140 000 dollars. Comme mentionné plus haut, plus d'un cinquième des cas de fraude ont causé des pertes d'au moins un million de dollars.
- Il est fréquent qu'une fraude soit commise dans une organisation pendant plusieurs années avant d'être découverte. Il s'écoule généralement 18 mois entre le moment où une fraude commence et le moment où l'organisation qui en est victime la découvre.
- Le type de fraude le plus courant est le détournement d'actifs (87 % des cas) et correspond à une perte médiane de 120 000 dollars. La fraude dans les états financiers (seulement 8 % des cas dans l'étude) est la plus coûteuse : elle représente une perte médiane de 250 000 dollars.
- Il est bien plus probable de détecter les fraudes en entreprise grâce à un lanceur d'alerte que par les audits, les contrôles ou d'autres moyens.
- La corruption et la facturation frauduleuse constituent les plus grands risques pour les organisations du monde entier. Dans l'ensemble des régions géographiques étudiées, ces deux types de fraude représentaient plus de 50 % des cas constatés.
- Le montant des pertes imputables à la fraude est proportionnel à l'ancienneté du fraudeur dans l'organisation. Les personnes possédant plus de 10 ans d'expérience dans l'organisation victime de la fraude ont provoqué une perte médiane de 229 000 dollars.

En comparaison, la perte médiane imputable à des personnes qui réaliseraient une fraude au cours de leur première année dans l'organisation ne s'élève qu'à 25 000 dollars.

- Aucun type d'organisation n'est épargné par la fraude, mais certains secteurs sont plus exposés que d'autres, comme le secteur bancaire, les services financiers, l'administration et les services publics, et l'industrie.
- Les fraudes au sein d'une organisation sont le plus souvent commises par des personnes qui travaillent dans l'un des services suivants : comptabilité, opérations, ventes, direction, service client et achats. Évidemment, les fraudes commises par les propriétaires et les cadres supérieurs sont particulièrement coûteuses, entraînant une perte médiane de 573 000 dollars, contre 180 000 dollars pour les managers et 60 000 dollars pour les collaborateurs.

Signaux d'alerte les plus fréquents

– Le fraudeur vit au-dessus de ses moyens.
– Il a des difficultés financières.
– Il subit des pressions excessives de la part de l'organisation.

Copyright © 2015 Eyrolles.

- En règle générale, les fraudeurs en entreprise n'ont jamais commis de délit auparavant. Parmi les personnes identifiées en situation de fraude, près de 67 % n'avaient jamais commis de délit et possédaient un historique professionnel irréprochable, et 84 % n'avaient jamais été sanctionnés ou licenciés par un de leurs employeurs pour fraude.
- Les fraudeurs ont souvent des comportements pouvant révéler une conduite illégale, fait constaté dans 81 % des cas. Les signaux d'alerte les plus fréquents sont : un train de vie apparemment au-dessus des moyens financiers (36 %), des difficultés financières (27 %), une proximité inhabituelle avec des prestataires ou des clients (19 %), et des problèmes liés à un contrôle excessif (18 %)[1].

Il est ici essentiel de souligner qu'aucune organisation n'est à l'abri de la fraude. Celle-ci peut toucher aussi bien les grandes organisations que les petites, et n'importe quel pays et secteur d'activité. Tant que les organisations se composent d'êtres humains avec leurs fragilités inhérentes, le risque de fraude est réel. Des études récentes montrent par ailleurs que le risque est accru en contexte de crise car les facteurs de pression sur les salariés sont plus nombreux et les opportunités plus grandes (réductions des effectifs, attention du management absorbée sur la survie de l'organisation…).

DÉFINITIONS DE LA FRAUDE

Même si la plupart des personnes comprennent globalement ce qu'est la fraude et peuvent probablement en donner un ou plusieurs exemples, il n'est pas très facile de la définir. La plupart des fraudes étant des actes condamnés par la loi, il convient de commencer par une définition juridique. L'encadré 8-3 donne une

ENCADRÉ 8-3

UNE DÉFINITION QUI FAIT AUTORITÉ

La fraude est un terme juridique et nécessite souvent une détermination juridique des faits. La définition large qu'en donne le *Black's Law Dictionary* est donc peut-être la plus pertinente dans ce contexte :

« [La fraude] est un terme générique englobant l'ensemble des divers moyens résultant de l'ingéniosité humaine, auxquels un individu a recours pour obtenir un avantage par rapport à un autre individu en faisant usage de fausses suggestions ou en dissimulant la vérité, et comprend toute tromperie par surprise, astuce, ruse, dissimulation ou toute autre méthode déloyale… Les éléments justifiant des poursuites judiciaires pour « fraude» incluent la description fallacieuse d'un fait présent ou passé par le défendeur, des actions entreprises en conséquence par le demandeur et des dommages encourus par le demandeur en raison de cette présentation erronée des faits. »

Source : *Black's Law Dictionary*. 1979, p. 594.

Copyright © 2015 Eyrolles.

définition provenant du *Black's Law Dictionary*, le dictionnaire juridique le plus utilisé aux États-Unis. Bien que certains des termes qu'il contient puissent différer de ceux utilisés tout au long de ce chapitre, il est lui aussi axé sur les agissements permettant à une personne d'en exploiter une autre.

Il existe de nombreuses autres définitions de la fraude, qui expriment à la fois le point de vue des auditeurs internes et celui des auditeurs externes. Les organisations qui représentent les auditeurs, ainsi que les professionnels de la lutte contre la fraude, ont cherché à définir la fraude et à délimiter les rôles et les responsabilités de leurs membres respectifs. En 2008, l'*Institute of Internal Auditors* (IIA), l'*American Institute of Certified Public Accountants* (AICPA) et l'*Association of Certified Fraud Examiners* (ACFE) ont élaboré ensemble une note d'orientation intitulée *Managing Business Risk of Fraud: A Practical Guide* (*Fraud Guide*). Cette publication énonce cinq grands principes pour la gestion du risque de fraude et recommande des méthodes permettant au Conseil, à la direction générale et aux auditeurs internes de lutter contre la fraude dans l'organisation. Elle est le fruit de deux années de travaux d'un groupe d'action, qui a rassemblé plus de 20 spécialistes de l'identification, de la maîtrise et de l'examen des risques de fraude. Cette note d'orientation contient la définition suivante :

> *« Une fraude est tout acte intentionnel ou toute omission intentionnelle ayant pour but de tromper autrui, et qui entraîne une perte pour la victime et/ou un avantage pour le fraudeur*[2]*. »*

Les principaux points essentiels de cette définition seront analysés plus en détail tout au long de ce chapitre. Cependant, chacun des organismes qui ont participé à la rédaction du présent ouvrage a sa propre définition, qui correspond à sa vision de la fraude. Ces différentes définitions sont présentées dans l'encadré 8-4.

Fraude

Tout acte illégal caractérisé par la tromperie, la dissimulation ou la violation de la confiance. Les fraudes sont perpétrées par des personnes et des organisations afin d'obtenir de l'argent, des biens ou des services, ou de s'assurer un avantage personnel ou commercial.

ENCADRÉ 8-4

DIFFÉRENTES DÉFINITIONS DE LA FRAUDE

Institute of Internal Auditors (IIA)

(extrait du glossaire des Normes de l'IIA, qui font partie du Cadre de référence international des pratiques professionnelles de l'audit interne)

« Tout acte illégal caractérisé par la tromperie, la dissimulation ou la violation de la confiance sans qu'il y ait eu violence ou menace de violence. Les fraudes sont perpétrées par des personnes et des organisations afin d'obtenir de l'argent, des biens ou des services, ou de s'assurer un avantage personnel ou commercial. »

American Institute of Certified Public Accountants (AICPA)

(extrait du *Statement on Auditing Standard* 99) :

« La fraude est un acte intentionnel qui se traduit par des anomalies graves dans les états financiers audités. [Il existe] deux types d'anomalies graves : […] des anomalies résultant d'un reporting financier frauduleux et des anomalies résultant d'un détournement d'actifs. »

Association of Certified Fraud Examiners (ACFE)

(extrait de l'édition 2008 du *Report to the Nation on Occupational Fraud*)

« Cas dans lequel une personne profite de sa situation professionnelle à des fins d'enrichissement personnel, par un usage abusif délibéré ou une utilisation inappropriée des ressources ou des actifs de l'organisation qui l'emploie. »

Copyright © 2015 Eyrolles.

La définition retenue par l'IIA est probablement la plus large : « Tout acte illégal caractérisé par la tromperie, la dissimulation ou la violation de la confiance ». Cette définition cadre avec le rôle étendu de l'audit interne au sein d'une organisation. La définition de l'IIA énumère ensuite les catégories de fraudeurs et les avantages potentiels que leurs agissements peuvent leur permettre d'obtenir. Là encore, il apparaît clairement que l'IIA a une conception large du rôle de la fonction d'audit interne dans une organisation. Nombre d'aspects de cette définition seront examinés plus loin dans ce chapitre.

La définition proposée par l'AICPA est beaucoup plus étroite, ce qui n'est pas surprenant. Elle est spécifiquement axée sur les anomalies qui résultent d'un reporting financier frauduleux ou d'un détournement d'actifs. Étant donné que les auditeurs externes se concentrent sur l'audit des états financiers, qui est désormais étendu – aux États-Unis et dans d'autres pays – à l'audit du contrôle interne relatif au reporting financier, il n'est pas surprenant que l'AICPA débatte du concept de fraude en évaluant sa relation avec les états financiers d'une organisation et ses effets sur ses comptes. L'encadré 8-5 énumère les normes auxquelles les auditeurs externes doivent se référer.

ENCADRÉ 8-5

LES AUDITEURS EXTERNES ET LA LUTTE CONTRE LA FRAUDE

Sociétés cotées aux États-Unis

Le *Public Company Accounting Oversight Board* (PCAOB) publie des normes qui contiennent des recommandations pour l'émission d'opinions sur les états financiers des sociétés cotées aux États-Unis. En ce qui concerne la fraude, ces normes indiquent que l'auditeur a la responsabilité de planifier et de réaliser l'audit de manière à obtenir une assurance raisonnable quant à l'absence, dans les états financiers, d'anomalies importantes dues à une erreur ou à une fraude (AU Section 110.02, *Responsibilities and Functions of the Independent Auditor*). Les normes du PCAOB traitent plus spécifiquement de la fraude dans l'AU Section 316, *Consideration of Fraud in a Financial Statement Audit*, qui se fonde sur la norme *Statement of Auditing Standard (SAS) 99*. Voir ci-dessous pour les orientations spécifiques énoncées dans la norme SAS 99.

Sociétés non cotées aux États-Unis

La compétence du PCAOB se limite aux audits réalisés pour des sociétés cotées aux États-Unis. Les sociétés non cotées continuent de se conformer aux normes de l'AICPA. La norme SAS 99, *Consideration of Fraud in a Financial Statement Audit*, indique que : « Les auditeurs [externes] doivent planifier et mener des audits pour obtenir une assurance raisonnable quant à l'absence d'anomalies graves, imputables à une erreur ou à une fraude, dans les états financiers ». Plus précisément, la norme SAS 99 donne les orientations suivantes pour les auditeurs (externes) aux États-Unis :

- se recentrer sur la sensibilisation au problème de la fraude et sur le scepticisme professionnel ;
- encourager la discussion entre les membres de l'équipe chargée de la mission d'audit (« séance de réflexion collective ») ;
- collecter les informations nécessaires à l'identification du risque d'anomalies graves imputables à une fraude ;
- synthétiser les éléments de fraude identifiés et ce que l'auditeur prévoit de faire ;
- imposer des procédures d'audit empêchant le management de contourner les activités de contrôle ;
- évaluer les résultats de l'audit ;
- signaler les cas de fraude au management, à la direction générale, au comité d'audit et à d'autres intervenants.

Organisations non basées aux États-Unis

L'*International Auditing and Assurance Standards Board* (IASB) a publié la norme International Standard on Auditing (ISA) 240, *Les obligations de l'auditeur en matière de fraude lors d'un audit d'états financiers*, qui indique que « lorsque l'auditeur planifie et effectue l'audit afin de ramener le risque d'audit à un niveau suffisamment faible, il doit prendre en compte les risques d'anomalies graves, dues à une fraude, dans les états financiers ». La norme ISA 240 donne des orientations supplémentaires analogues à celles de la norme SAS 99 ci-dessus.

Copyright © 2015 Eyrolles.

Le reporting financier frauduleux contient des anomalies ou des omissions intentionnelles de montants ou des informations destinées à tromper les utilisateurs. En raison de ces indications erronées ou de ces omissions, la présentation de ces états financiers n'est pas conforme, dans ses principaux aspects, aux principes comptables applicables (selon les normes IFRS ou les normes comptables locales). Le reporting financier frauduleux peut résulter des opérations suivantes :

- manipulation, falsification ou modification des documents comptables ou des pièces justificatives à partir desquels les états financiers sont élaborés ;
- présentation inexacte, ou omission intentionnelle, dans les états financiers, d'événements, de transactions, ou d'autres informations importantes ;
- mauvaise application intentionnelle des principes comptables concernant les montants, la classification, le mode de présentation ou la communication.

Commentaire du traducteur

Selon la Compagnie nationale des commissaires aux comptes (CNCC) : « La fraude se distingue de l'erreur par son caractère intentionnel. » (cf. Norme d'exercice professionnel [NEP] 200).

Les inexactitudes découlant d'un détournement d'actifs sont liées au vol d'actifs d'une organisation, qui se traduit par la présentation d'états financiers non conformes aux normes applicables, pour tous les aspects importants. On peut, par exemple, détourner des actifs en volant des recettes ou des actifs ou en faisant en sorte que l'entité paie des biens ou des services qu'elle n'a pas reçus. Le détournement d'actifs peut s'accompagner de documents ou de pièces comptables mensongers ou trompeurs, de la suppression de preuves, résultant éventuellement d'un contournement du contrôle interne. Les fraudeurs agissent souvent en collusion avec d'autres collaborateurs ou avec des tiers.

La définition retenue par l'ACFE est axée sur la fraude dans l'organisation, c'est-à-dire sur le lieu de travail. Ce type de fraude recouvre divers agissements répréhensibles de collaborateurs, de managers ou de dirigeants. Il peut s'agir d'un simple vol dans la caisse ou d'une fraude complexe telle que la présentation d'un reporting financier frauduleux. Quatre éléments semblent caractériser l'incidence d'une fraude dans les organisations. Un tel acte :

- est clandestin, c'est-à-dire secret ;
- constitue un manquement aux obligations du fraudeur vis-à-vis de l'organisation qui en est la victime ;

Copyright © 2015 Eyrolles.

- est commis dans le but de procurer un avantage financier, direct ou indirect, au fraudeur ;
- représente pour l'organisation qui emploie le fraudeur un coût en termes de perte d'actifs, de recettes ou de réserves.

Le système de classification des fraudes et abus dans les organisations établi par l'ACFE décrit trois grands types de fraude : le reporting financier frauduleux, qui résulte généralement de la falsification des états financiers d'une organisation (par exemple, pour surestimer le chiffre d'affaires et sous-estimer les engagements et charges) ; le détournement d'actifs, qui résulte du vol ou de l'utilisation abusive d'actifs d'une organisation (par exemple, l'écrémage des recettes, le vol dans les stocks ou une fraude portant sur la paie) ; et la corruption, qui consiste, pour les fraudeurs, à exercer une influence indue lors d'une transaction commerciale, afin d'en tirer un avantage pour eux-mêmes ou pour un tiers (par exemple, pots-de-vin, délits d'initié ou conflits d'intérêts), en violation de leurs obligations vis-à-vis de leur employeur ou des droits d'un tiers. L'encadré 8-6 présente ce système de classification.

Exemples de détournement d'actifs

– Vol.
– Abus de biens sociaux.
– Malversation.

ENCADRÉ 8-6

APERÇU DU SYSTÈME DE CLASSIFICATION DES FRAUDES ET ABUS DANS LES ORGANISATIONS ÉTABLI PAR L'ACFE

- Manipulation intentionnelle des états financiers, qui peut entraîner :
  - la comptabilisation inappropriée du chiffre d'affaires ;
  - la comptabilisation inappropriée de charges ;
  - l'établissement d'un bilan qui ne reflète pas les montants réels, y compris en ce qui concerne les réserves ;
  - la dissimulation d'informations financières ou le maquillage d'informations financières ;
  - la dissimulation d'un détournement d'actifs ;
  - la dissimulation de recettes ou de dépenses non autorisées ;
  - la dissimulation d'une acquisition, d'une cession ou d'une utilisation d'actifs non autorisée.
- Détournement :
  - d'actifs corporels par :
    - des collaborateurs ;
    - des clients ;
    - des fournisseurs ;
    - d'anciens collaborateurs ou des tiers ;
  - d'actifs incorporels ;
  - d'opportunités commerciales exclusives.
- Corruption, notamment :
  - des pots-de-vin et cadeaux à :
    - des personnes morales ;
    - des personnes physiques ;
    - des fonctionnaires ;
  - l'acceptation de pots-de-vin, de dessous-de-table ou de cadeaux ;
  - l'aide et la complicité dans une fraude commise par des tiers (clients, fournisseurs…).

Source : *Managing the Business Risk of Fraud: A Practical Guide*, IIA, AICPA et ACFE, p. 24.

Copyright © 2015 Eyrolles.

Au niveau international, la norme qui donne des orientations à l'intention des auditeurs est l'*International Standard on Auditing* (ISA) n° 240, *The Auditor's Responsibility Relating to Fraud and Error in an Audit of Financial Statements,* publiée par l'*International Federation of Accountants* (IFAC). Même si cette norme s'applique principalement aux auditeurs externes, son contenu et les orientations qu'elle contient intéressent aussi les auditeurs internes. En outre, étant donné que la fraude, le gaspillage et les abus préoccupent aussi beaucoup les pouvoirs publics, les *Governmental Auditing Standards* des États-Unis (le *Yellow Book*) consacrent plusieurs de leurs sections aux responsabilités des auditeurs internes des administrations publiques.

Commentaire du traducteur

En France

L'adaptation de la norme ISA 240 a été publiée en France au Journal officiel *du 3 mai 2007. Cette Norme d'exercice professionnel a fait l'objet d'amendements de conformité et a été homologuée par arrêté du 21 juin 2011 publié au J.O. n° 0178 du 3 août 2011.*

Elle vise les fraudes susceptibles d'entraîner des anomalies significatives dans les comptes, à savoir les actes intentionnels portant atteinte à l'image fidèle des comptes et le détournement d'actifs. En plus des dispositions prévues aux normes ISA, elle inclut aussi la spécificité suivante propre au contexte français : l'obligation pour les auditeurs internes de révéler au procureur de la République tout fait délictueux susceptible de recevoir une qualification pénale.

En outre la Norme d'exercice professionnel 9605 d'avril 2010 précise les obligations du commissaire aux comptes relatives à la lutte contre le blanchiment des capitaux et le financement du terrorisme.

Reporting financier frauduleux

Actes comprenant la falsification des états financiers d'une organisation (par exemple, une surestimation du chiffre d'affaires ou une sous-estimation du passif et des charges).

Chacune de ces définitions de la fraude correspond aux priorités de l'organisation professionnelle qui l'a élaborée. Cependant, dans la mesure où ces organismes ont œuvré ensemble pour publier le *Fraud Guide*, la définition utilisée dans ce guide, en particulier celle indiquant que « la fraude est tout acte intentionnel ou toute omission intentionnelle ayant pour but de tromper autrui, et qui entraîne une perte pour la victime et/ou un avantage pour le fraudeur », servira de base de discussion tout au long de ce chapitre. Il s'agit d'une définition simple, mais détaillée, qui jette les fondements des principes et autres orientations énoncés dans le *Fraud Guide*.

LE TRIANGLE DE LA FRAUDE

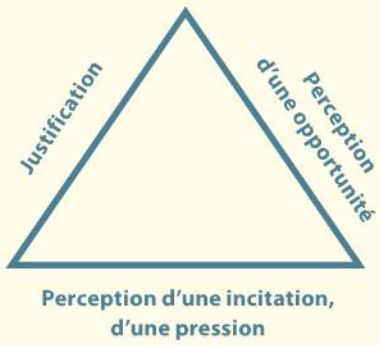
Le « Triangle de la fraude » de Cressey (1986) constitue un cadre de référence conceptuel important. Il s'inspire de ce que les policiers et enquêteurs ont coutume d'appeler « les moyens, les motivations et l'opportunité ». Imaginé par le sociologue Donald Cressey et largement diffusé par l'ACFE, le Triangle de la fraude se compose

Copyright © 2015 Eyrolles.

de trois éléments : les incitations/pressions perçues, la perception d'une opportunité et la justification du comportement frauduleux (encadré 8-7).

ENCADRÉ 8-7

LE TRIANGLE DE LA FRAUDE



Cressey, D.R., *Other People's Money: A Study in the Social Psychology of Embezzlement* (Glencoe, Illinois, The Free Press, 1986).

Le Triangle de la fraude met en évidence les trois éléments que l'on peut qualifier de « causes à l'origine de la fraude », qui sont toujours présents, quel que soit le type de fraude. Les fraudeurs veulent se soustraire à des pressions, réelles ou perçues, visant à leur faire obtenir un résultat (ce qui les incite par exemple à maquiller les chiffres lorsqu'ils ne peuvent pas atteindre les objectifs). Ils doivent percevoir une opportunité évidente afin de perpétrer la fraude facilement (par exemple, personne ne surveille le magasin, une confiance aveugle est accordée au collaborateur), et surtout, ils ont besoin de justifier leur acte pour le rendre acceptable à leurs yeux. Cette justification leur permet de croire qu'ils n'ont rien fait de mal et qu'ils sont « des gens comme les autres ». Plus précisément, les fraudeurs doivent être en mesure de se justifier leurs actes à eux-mêmes, ce qui constitue un mécanisme psychologique leur permettant de faire face à l'inévitable « dissonance cognitive » (c'est-à-dire le conflit entre leur impression d'être honnête et la nature frauduleuse de leurs actes ou comportements). Ils ont besoin d'excuses, par exemple :

- tout le monde le fait, et je fais comme tout le monde ;
- j'ai pris de l'argent dans la caisse, mais ce n'était qu'un « emprunt » temporaire. Je rendrai l'argent lorsque j'aurai gagné au casino/aux courses ;
- mon patron ne me paie pas suffisamment, et donc je mérite ces « primes », qui ne sont qu'une rémunération raisonnable que l'organisation peut certainement se permettre ;
- je ne fais de mal à personne. En fait, c'est pour la bonne cause !
- ce n'est pas très grave.

Copyright © 2015 Eyrolles.

Fraude en entreprise

Fraude sur le lieu de travail :
- falsification d'états financiers ;
- détournement d'actifs ;
- corruption.

Prenons deux exemples : l'employé d'un magasin de meubles qui vole dans le stock peut profiter de la faiblesse du contrôle interne (perçue comme une opportunité). Il a besoin de meubler son nouvel appartement « gratuitement » (il perçoit une pression de la part de son épouse) et il se justifie en se disant que les autres employés du magasin volent aussi probablement (que ce soit vrai ou non). Dans le cas d'une fraude perpétrée par le management, la pression perçue peut concerner la réalisation des objectifs de résultat, qui sera assortie de primes généreuses ; l'opportunité peut résider dans la faiblesse des activités de contrôle relatives au reporting financier ou la passivité du comité d'audit, et la justification peut être du type « c'est dans l'intérêt de l'organisation, et donc je peux utiliser les réserves pour surmonter un passage à vide temporaire ». Bien que le Triangle de la fraude constitue un outil conceptuel convaincant, il existe d'autres facteurs, tels que l'avidité et le goût de la possession matérielle, la volonté de prendre sa revanche et de faire payer l'organisation pour des injustices perçues, ou une attitude du type « attrapez-moi si vous pouvez ». De même, l'environnement et la culture de l'organisation peuvent entrer en jeu. Par exemple, le manque d'exemplarité de la direction, qui se manifeste par l'inertie ou une réticence à agir, par l'ignorance délibérée ou une simple réprimande, et l'absence de poursuites lors de fraudes antérieures peuvent contribuer à la probabilité d'une fraude. Les facteurs comportementaux sont analysés plus en détail dans la suite de ce chapitre.

LES GRANDS PRINCIPES DE LA GESTION DU RISQUE DE FRAUDE

Le *Fraud Guide* montre l'importance, pour les organisations, de déployer des efforts rigoureux et permanents pour se protéger contre la fraude. Il énonce cinq grands principes, résumés dans l'encadré 8-8, que les organisations ont tout intérêt à appliquer.

Causes à l'origine de la fraude (triangle de Cressey)

Perception d'une incitation ou d'une pression.
Perception d'une opportunité.
Justification.

Gouvernance du risque de fraude (Principe 1)

Comme indiqué dans le chapitre 3, *La gouvernance*, il est essentiel que les organisations disposent d'une solide structure de gouvernance pour surveiller la gestion des risques et les autres activités contribuant à la réalisation des objectifs de l'organisation. Il en va de même concernant la fraude : l'organisation doit mettre en place une structure pour veiller à l'identification et à la gestion du risque de fraude. Une gouvernance efficace permet d'instaurer et gérer un climat d'éthique au sein d'une organisation, ce qui peut aider à prévenir ou à dissuader la fraude. En faisant preuve d'exemplarité, la direction définit le seuil de tolérance de l'organisation vis-à-vis de la fraude.

Copyright © 2015 Eyrolles.

Comme le mode de gouvernance analysé au chapitre 3, la gouvernance du risque de fraude doit en premier lieu relever de l'organe de gouvernance. Celui-ci peut en effet faire preuve d'exemplarité pour la gestion du risque de fraude, et encourager le management à définir des politiques spécifiques qui encourageront un comportement éthique, ainsi que la prévention et la détection de la fraude. Le Conseil doit aussi veiller à l'efficacité du programme établi par l'organisation pour gérer le risque. À cette fin, il peut confier à un membre de la direction générale la responsabilité de ce programme et lui demander de lui rendre compte de son efficacité. Les éléments spécifiques d'un programme de gestion du risque de fraude sont analysés plus loin dans ce chapitre.

Évaluation des risques de fraude (Principe 2)

Un programme de gestion du risque de fraude est infructueux si le management ne cerne pas tout d'abord les risques de fraude inhérents auxquels l'organisation est confrontée. Les phases d'évaluation des risques de fraude sont analogues à celles suivies pour l'évaluation du risque de l'organisation décrites au chapitre 4, *La gestion des risques*. Une organisation doit commencer par identifier

ENCADRÉ 8-8

LES GRANDS PRINCIPES DE LA GESTION DU RISQUE DE FRAUDE

Principe 1 : Dans le cadre de la structure de gouvernance de l'organisation, un programme de gestion du risque de fraude doit être mis en place, notamment une politique (ou des politiques) présentée(s) par écrit, afin d'exprimer les attentes du Conseil et de la direction générale en ce qui concerne la gestion du risque de fraude.

Principe 2 : L'organisation doit évaluer périodiquement son exposition au risque de fraude, de manière à identifier des processus et des événements potentiels dont elle devra atténuer les effets.

Principe 3 : Des techniques de prévention destinées à empêcher les fraudes graves doivent être en place, dans la mesure du possible, afin d'atténuer les conséquences éventuelles sur l'organisation.

Principe 4 : Des techniques de détection doivent être mises en place pour déceler les fraudes lorsque les mesures préventives ne sont pas efficaces ou que des risques non maîtrisés se matérialisent.

Principe 5 : Un processus de reporting doit être mis en place pour permettre l'obtention d'informations sur la fraude potentielle, et il faut coordonner des investigations et des actions correctives, afin que la fraude potentielle soit traitée de manière appropriée et rapidement.

Les organisations qui ont participé à la rédaction du *Fraud Guide* estiment que celui-ci « peut servir à évaluer le programme de gestion instauré par une organisation pour gérer le risque de fraude, ou à élaborer un programme s'il n'en existe pas déjà un ».

Managing the Business Risk of Fraud: A Practical Guide, The Institute of Internal Auditors, The American Institute of Certified Public Accountants, et The Association of Certified Fraud Examiners. Téléchargeable sur www.theiia.org, p. 6.

Copyright © 2015 Eyrolles.

les scénarios de fraude potentiels auxquels elle est susceptible d'être vulnérable. Ces scénarios différeront d'une organisation à l'autre, en fonction de son modèle économique, du secteur, des zones d'implantation, de sa culture et d'autres facteurs similaires. Lorsque l'on dresse une liste des scénarios de fraude potentiels, il peut être utile de recueillir des informations auprès des autorités de régulation et de supervision extérieures, du secteur, des organismes qui établissent des lignes directrices et des organisations professionnelles. Le triangle de la fraude décrit dans la section précédente peut guider la réflexion collective portant sur les risques de fraude, et permettre notamment de définir les opportunités pouvant donner naissance à ces scénarios. Ainsi, la prise en compte des incitations et des pressions actuelles, ou la connaissance des failles connues de l'accès aux systèmes, peut faciliter l'élaboration d'un scénario de risque de fraude (par exemple, le management accède aux entrées des journaux et peut les modifier pour surévaluer le bénéfice et, ainsi, obtenir une prime de résultat).

Commentaire du traducteur

***Transposition des dispositifs d'alerte* (« whistleblowing »)**

La France a adopté de 2007 à 2013 cinq lois qui encadrent les signalements en lien avec :

- *les faits de corruption, pour les salariés du secteur privé : loi du 13 novembre 2007 ;*
- *la sécurité sanitaire des médicaments et produits de santé : loi du 29 décembre 2011 ;*
- *tout risque grave pour la santé publique ou l'environnement : loi du 16 avril 2013 ;*
- *les conflits d'intérêts (relatifs à une liste d'élus et fonctionnaires) : loi du 11 octobre 2013 ;*
- *tout crime ou délit, pour les salariés des secteurs public et privé : loi du 6 décembre 2013.*

Transparency International *France a publié un guide pratique à l'usage des lanceurs d'alerte, disponible sur son site Internet.*

Source : site de « Transparence France » section française de « Transparency International *», http://www.transparency-france.org.*

Après avoir identifié les risques de fraude potentiels, il faut évaluer l'impact et la probabilité de chacun. Il est essentiel de prendre en compte tous les effets possibles des fraudes, et non leurs seules conséquences financières. Si la fraude est fréquente, elle peut entacher la réputation d'une organisation ou enfreindre la législation, même si elle n'entraîne pas toujours des pertes financières importantes. L'évaluation des risques de fraude constitue une étape cruciale, car elle permet à l'organisation de déterminer le niveau des ressources à consacrer à la prévention ou à la détection des scénarios de fraude identifiés.

Copyright © 2015 Eyrolles.

Enfin, une organisation doit décider de ce qui doit être fait dans les différents scénarios de fraude, c'est-à-dire comment traiter les risques de fraude. Comme pour le traitement des risques décrit au chapitre 4, les organisations peuvent faire face au risque de fraude de plusieurs façons : en évitant ce risque, en le partageant, en le réduisant, en l'acceptant ou en combinant plusieurs de ces options. Il est fondamental de déterminer une option offrant un bon rapport coût-bénéfice, qui réduit le risque à un niveau acceptable en tenant compte de toutes les conséquences possibles.

Prévention et détection de la fraude (Principes 3 et 4)

Un programme de gestion du risque de fraude doit résulter d'un bon équilibre entre contrôles préventifs et contrôles détectifs. Les contrôles préventifs peuvent porter sur les politiques, les procédures, la formation et la communication qui visent toutes à empêcher la fraude. S'ils ne garantissent pas toujours qu'une fraude sera évitée, ils constituent un premier niveau de maîtrise important, qui permet de limiter le risque de fraude. Les contrôles préventifs, notamment ceux qui reposent sur un solide programme de sensibilisation au problème de la fraude, peuvent avoir un effet fortement dissuasif (c'est-à-dire décourager la fraude).

Même si, en général, une organisation préfère prévenir la fraude, ce n'est pas toujours possible. Elle doit donc également s'attacher à concevoir et appliquer des contrôles détectifs efficaces. Qu'ils soient manuels ou automatisés, ces contrôles doivent détecter rapidement une fraude déjà commise ou en cours. Ces contrôles peuvent dissuader la fraude, mais ils ne sont pas conçus pour l'empêcher. Ils donnent en fait des informations montrant qu'une fraude a eu lieu, ce qui peut être utile dans le cadre d'une enquête.

Notification d'une fraude, enquête et mesures mises en œuvre (Principe 5)

Comme indiqué plus haut dans ce chapitre, le rapport de l'ACFE indique qu'il est bien plus probable de détecter les fraudes grâce à un lanceur d'alerte que par les audits, les contrôles ou d'autres moyens. Il est par conséquent important qu'une organisation dispose d'un système de reporting pour faciliter et encourager le signalement de cas de fraude potentiels. Par exemple, un dispositif d'alerte professionnelle ou éthique (« *whistleblowing* ») permettant de dénoncer des fraudes potentielles constitue un moyen de notification rapide, facilite la collecte des informations nécessaires à une éventuelle enquête et permet au lanceur d'alerte de garder l'anonymat s'il le souhaite. Ce système peut être géré par un membre de la direction générale. La législation peut également imposer l'instauration d'un mécanisme permettant d'informer directement

Gouvernance (ou gouvernement d'entreprise)

Dispositif comprenant les processus et les structures mis en place par le Conseil afin d'informer, de diriger, de gérer et de piloter les activités de l'organisation en vue de réaliser ses objectifs.

Évaluation des risques

Identification et analyse (généralement en termes d'impact et de probabilité d'occurrence) des risques susceptibles d'affecter la réalisation des objectifs d'une organisation, de façon à déterminer comment ces risques doivent être gérés.

Copyright © 2015 Eyrolles.

le Conseil dans certaines circonstances, si le lanceur d'alerte pense que la direction générale risque d'être impliquée dans la fraude en question. La légalité de ce type de dispositifs est encadrée dans de nombreux pays, dont la France (*cf.* Commentaire du traducteur page 12-3).

Dès qu'une allégation a été reçue, un processus structuré doit permettre d'évaluer le cas de fraude potentiel et d'enquêter. Un processus d'enquête solide peut améliorer les chances de l'organisation de récupérer les sommes perdues et limiter au maximum la probabilité d'une action en justice. Suivant les circonstances, il peut être nécessaire de faire appel à un avocat-conseil, interne ou externe, dans le cadre de l'enquête, ainsi qu'à d'autres fonctions de l'organisation, telles que les Ressources humaines (RH), les Systèmes d'information (SI) et l'audit interne. Une approche formelle et structurée pour les investigations et le reporting de ses résultats aidera l'organisation à mener cette enquête rapidement, à obtenir et gérer les moyens d'appui nécessaires pour faciliter des actions correctives.

Traitement des risques

Mesure ou ensemble de mesures prises par le management pour déployer la stratégie de gestion des risques définie. Le traitement des risques consiste à éviter, réduire, partager ou accepter les risques.

Quelle que soit l'issue de l'enquête (procédure judiciaire, mesures disciplinaires ou inaction), il est essentiel qu'une organisation dispose de moyens conséquents pour rendre des conclusions à l'issue de l'enquête menée. Premièrement, une enquête rapidement menée permet de lancer une procédure judiciaire ou de prendre des mesures disciplinaires avant que « la piste ne se refroidisse » (expression familière souvent employée par les enquêteurs pour indiquer qu'il devient de plus en plus difficile, à mesure que le temps passe, de recueillir des preuves, et que celles-ci seront peut-être moins pertinentes). De surcroît, les personnes impliquées dans une fraude doivent pouvoir se défendre rapidement, et c'est même un droit dans de nombreux pays. Deuxièmement, les organisations doivent déterminer les causes à l'origine d'une fraude, afin que des actions correctives (par exemple, une amélioration des contrôles) puissent être mises en œuvre. Enfin, le management doit veiller de façon homogène à la discipline des collaborateurs, afin d'éviter toute décision perçue comme du favoritisme ou des mesures disciplinaires arbitraires. La direction peut ainsi faire preuve d'exemplarité en montrant clairement que la fraude ne sera pas tolérée, et qu'il y sera mis un terme de manière rapide et cohérente.

Les principes énoncés dans cette section revêtent une telle importance pour l'instauration et l'administration d'un programme efficace de gestion de la fraude que chacun d'eux sera analysé plus en détail dans les sections suivantes. Le lecteur pourra ainsi mieux comprendre comment suivre les étapes nécessaires pour appliquer ces principes.

Copyright © 2015 Eyrolles.

LA GOUVERNANCE DU PROGRAMME DE GESTION DU RISQUE DE FRAUDE

La solidité de la gouvernance est l'une des conditions préalables à l'efficacité du programme de gestion du risque de fraude. Selon le *Fraud Guide*, les principales parties prenantes des organisations « […] contribuent à accroître la prise de conscience et les attentes relatives au comportement et aux pratiques de gouvernance de l'organisation. Certaines organisations ont instauré une culture d'entreprise qui repose sur de solides pratiques de gouvernance, et en particulier sur les éléments suivants :

- maîtrise des plannings et du flux d'informations par le Conseil ;
- accès à plusieurs niveaux de management et gestion efficace d'un dispositif d'alerte permettant de signaler des abus ;
- indépendance des procédures de nomination ;
- efficacité de la direction générale […], évaluations, gestion des performances, rémunération et planification des changements de personnel ;
- code de conduite propre à la direction générale, qui vient s'ajouter au code de conduite de l'organisation ;
- priorité donnée à l'indépendance et à l'efficacité du Conseil, évaluation, réunion de l'encadrement à huis clos et participation active au suivi des efforts stratégiques et de réduction des risques. »[3]

Ces éléments montrent l'importance d'une culture d'entreprise permettant au Conseil d'obtenir une assurance sur le comportement éthique du management et des collaborateurs. Le *Fraud Guide* indique ensuite que « les codes de déontologie efficaces peuvent servir à la prévention, à la détection et à la dissuasion des actes frauduleux et délictueux. Si l'organisation traite ses collaborateurs, ses clients, ses fournisseurs et ses partenaires selon des principes éthiques, tous en bénéficieront. Un code de déontologie permet de créer un environnement dans lequel la prise de bonnes décisions est implicite. »[4]

Rôles et responsabilités

Les rôles et responsabilités associés à un programme de gestion du risque de fraude doivent faire l'objet d'un descriptif formel, qui sera également diffusé dans l'organisation. Les règles et procédures, les descriptifs des postes, les chartes et les délégations de pouvoir sont tous importants pour définir ces rôles et responsabilités. Généralement, les programmes efficaces de gestion du risque de fraude incluent les rôles et responsabilités suivants :

Détection de la fraude

D'après le rapport de l'ACFE, il est bien plus probable de détecter les fraudes en entreprise grâce à un lanceur d'alerte que par les audits, les contrôles ou d'autres moyens.

Copyright © 2015 Eyrolles.

Le Conseil. Comme nous l'avons déjà indiqué, le Conseil fait preuve d'exemplarité en adoptant les pratiques de gouvernance énumérées ci-dessus. Certaines responsabilités spécifiques relatives à la surveillance de la fraude peuvent être exercées par des comités émanant du Conseil, notamment le comité d'audit ou le comité chargé des nominations et de la gouvernance. Cette surveillance suppose le plus souvent :

- de comprendre de manière générale les politiques, procédures, plans d'incitations, etc. relatifs à la fraude ;
- de comprendre de manière approfondie les principaux risques de fraude ;
- d'assurer un suivi du programme de gestion du risque de fraude, y compris des contrôles internes mis en œuvre compte tenu de ce risque ;
- d'obtenir et de superviser des rapports donnant des informations sur les cas de fraude, sur l'avancée des investigations et sur les mesures disciplinaires ;
- de pouvoir faire appel, au besoin, à un avocat-conseil ou à des experts extérieurs ;
- de demander à la fonction d'audit interne et à l'audit externe de donner une assurance raisonnable quant au risque de fraude.

Les attributions du Conseil et de ses comités doivent être présentées dans la charte de ces organes, afin que les rôles et responsabilités de ces intervenants soient clairement délimités et bien compris. Le Conseil doit également s'assurer que des ressources suffisantes sont mises en œuvre pour permettre le bon déroulement du programme de gestion du risque de fraude.

La direction générale. Comme le Conseil, la direction générale joue un rôle très important en faisant preuve d'exemplarité pour toute l'organisation. Outre ses déclarations, ses actions influencent la perception de la culture et de son comportement vis-à-vis de la prévention de la fraude. De plus, la direction générale est chargée d'appliquer le programme global de gestion du risque de fraude. À cette fin, il doit donner une orientation et superviser le système de contrôle interne, lequel doit être conçu et déployé de manière à empêcher ou à détecter rapidement les fraudes. La direction générale doit aussi instaurer un système de pilotage et de reporting qui lui permettra de déterminer le fonctionnement effectif du programme de gestion du risque de fraude. Ce dispositif lui apportera rapidement des informations pertinentes, qu'elle pourra ensuite communiquer au Conseil.

Dans nombre d'organisations, il est fréquent de confier à un membre de la direction générale la surveillance du programme de gestion du risque de fraude. Cette surveillance peut consister

L'exemplarité au plus haut niveau

Les cadres supérieurs d'une organisation font preuve d'exemplarité de par leur intégrité et leur sensibilisation au contrôle dans l'ensemble d'une organisation. Voir également Environnement de contrôle.

Copyright © 2015 Eyrolles.

à vérifier les politiques relatives à la fraude et à l'éthique, évaluer le risque de fraude, superviser les contrôles destinés à traiter ce risque, observer l'efficacité du programme, coordonner le processus d'enquête et de reporting, ainsi que sensibiliser et former les collaborateurs à ce programme. Ce responsable devra, de préférence, occuper un poste suffisamment élevé dans l'organisation, afin de renforcer l'engagement de la direction générale à prévenir et dissuader la fraude. En général, un certain nombre d'autres fonctions, le plus souvent rattachées au service juridique et aux ressources humaines, lui apportent un appui bien défini.

Les collaborateurs. Tous les membres de l'organisation doivent participer au déploiement quotidien du programme de gestion du risque de fraude, et, plus précisément, des contrôles destinés à prévenir et détecter la fraude. Selon le *Fraud Guide*, « le personnel, à tous les niveaux, management compris, doit :

- comprendre les fondamentaux de la fraude et savoir reconnaître les signaux d'alerte ;
- comprendre le rôle qui lui est dévolu dans le cadre du contrôle interne. Les collaborateurs doivent savoir comment les procédures relatives à leurs tâches ont été conçues pour gérer les risques de fraude et dans quelles circonstances la non-conformité est susceptible de créer une opportunité de commettre une fraude qui pourrait passer inaperçue ;
- prendre connaissance des règles et procédures *ad hoc* (politique antifraude, code de conduite et politique relative aux lanceurs d'alerte), ainsi que des autres politiques et procédures opérationnelles, telles que les manuels d'achats ;
- le cas échéant, participer au processus visant à instaurer un solide environnement de contrôle, définir et mettre en œuvre des activités de lutte contre la fraude, et participer aux activités de pilotage ;
- faire part d'éventuels soupçons de fraude ;
- coopérer lors des enquêtes. »[5]

Environnement de contrôle

Attitude et actions du Conseil et du management au regard de l'importance du (dispositif de) contrôle dans l'organisation.

Pour des informations supplémentaires sur les activités de gestion du risque de fraude et sur la façon dont ces activités peuvent être harmonisées avec le référentiel de contrôle interne du COSO, veuillez vous reporter à l'annexe I du *Fraud Guide*.

La fonction d'audit interne. La fonction d'audit interne joue un rôle essentiel, car elle contribue à la gouvernance globale du programme de gestion du risque de fraude. C'est ce qui ressort clairement de l'assurance indépendante que l'audit interne apporte au Conseil et à la direction générale pour attester que les contrôles en place pour gérer le risque de fraude sont conçus de manière

Copyright © 2015 Eyrolles.

adéquate et fonctionnent de manière effective. Le rôle de la fonction d'audit interne est détaillé plus loin dans ce chapitre.

Un auditeur externe se doit lui aussi de détecter certains types de fraude (présentation d'un reporting financier frauduleux et détournement d'actifs, notamment). Ce rôle, qui est bien défini dans les normes applicables à la profession, ne fait pas partie du programme de gestion du risque de fraude mis en place par une organisation. Cette intégration serait incompatible avec le principe d'indépendance des auditeurs externes.

Éléments d'un programme de gestion du risque de fraude

Même s'il n'existe pas de méthode « universelle », les programmes les plus efficaces pour la gestion du risque de fraude ont plusieurs caractéristiques communes. La plupart des organisations disposent de règles et procédures écrites en ce qui concerne la fraude et mènent, en général, des activités destinées à évaluer les risques, concevoir des contrôles efficaces, vérifier la conformité, mener des enquêtes et sensibiliser leurs collaborateurs au problème de la fraude et aux signaux d'alerte. Cependant, rares sont les organisations qui réussissent à regrouper toutes ces activités dans un programme intégré. Le plus souvent, les programmes intégrés qui donnent de bons résultats comportent un certain nombre d'éléments fondamentaux.

- Un *engagement* du Conseil et de la direction générale, qui doit être présenté dans un document officiel et diffusé dans toute l'organisation.
- Des activités de *sensibilisation au problème de la fraude*, permettant aux collaborateurs de comprendre la finalité, les exigences et les responsabilités définies dans le cadre du programme. Ces activités peuvent inclure tous les processus suivants ou plusieurs d'entre eux : communications écrites destinées à tous les collaborateurs, communications orales au cours de réunions à l'échelle de toute l'organisation, messages sur l'intranet et sur la page Web du site de l'organisation et programmes de formation.
- Un *processus de déclaration sur l'honneur*, par lequel les collaborateurs sont tenus d'attester périodiquement, en général une fois par an, qu'ils comprennent les règles et procédures définies, et qu'ils les appliquent.
- Un protocole ou un processus de *notification des conflits*, qui permet aux collaborateurs de faire eux-mêmes état des conflits d'intérêts potentiels ou effectifs. Ce protocole ou ce processus peut également inclure un mécanisme de résolution rapide des problèmes signalés.
- Une *évaluation des risques de fraude*, qui facilite l'identification de tous les scénarios de fraude raisonnables. Cette évaluation est présentée plus en détail dans la section suivante.

Copyright © 2015 Eyrolles.

- Des *procédures de reporting* et de *protection des lanceurs d'alerte*, qui constituent, pour les personnes travaillant à l'intérieur ou à l'extérieur de l'organisation, un moyen simple de signaler des infractions ou des fraudes potentielles qui ont éveillé leurs soupçons.
- Un *processus d'enquête*, par lequel toutes les questions soulevées donnent lieu à des investigations rapides et approfondies, le cas échéant.
- Des *mesures disciplinaires et/ou correctives*, qui remédient aux aspects non conformes aux politiques établies et qui contribuent à dissuader les comportements frauduleux.
- L'*évaluation* et l'*amélioration des processus*, afin de donner une assurance qualité attestant que le programme va atteindre ses objectifs.
- Un *pilotage constant*, de façon à ce que le programme continue de fonctionner comme prévu.

L'intégration de tous ces éléments dans un programme de gestion du risque de fraude n'élimine pas complètement ce risque, mais apporte une assurance raisonnable quant à la possibilité de prévenir ou détecter rapidement les fraudes et les traiter de manière appropriée.

ÉVALUATION DES RISQUES DE FRAUDE

Comme indiqué plus haut, l'évaluation des risques de fraude s'apparente à celle des autres risques. Elle comporte trois grandes étapes :

- identification des risques inhérents de fraude ;
- évaluation de l'impact et de la probabilité d'occurrence des risques identifiés ;
- définition de solutions permettant de faire face aux risques qui ont un impact et une probabilité d'occurrence suffisamment élevés pour que leur effet potentiel dépasse le seuil de tolérance défini par le management.

Lorsque l'on évalue les risques de fraude, il importe de faire participer des personnes ayant des connaissances, des compétences et des points de vue différents. Ces personnes ne sont pas les mêmes d'une organisation à l'autre, mais l'évaluation des risques fait généralement intervenir les personnes suivantes :

- les collaborateurs du service comptable et financier, qui pourront identifier des scénarios de fraude portant sur le reporting financier et sur la conservation des actifs ;

Sensibilisation au problème de la fraude

Activités permettant aux collaborateurs de comprendre la finalité, les exigences et les responsabilités définies dans le cadre d'un programme de gestion du risque de fraude.

Copyright © 2015 Eyrolles.

- les collaborateurs des services extra-financiers, qui peuvent valoriser leur connaissance des opérations quotidiennes, des relations avec les clients et les fournisseurs, ainsi que leur connaissance des autres scénarios de fraude possibles dans le secteur concerné ;
- les collaborateurs du service juridique, ainsi que ceux en charge de la conformité, qui peuvent identifier des scénarios susceptibles d'entraîner une responsabilité au pénal, au civil ou réglementaire en cas de fraude ou de faute ;
- les collaborateurs chargés de la gestion des risques, qui peuvent identifier des scénarios de fraude sur le marché financier ou de fraudes à l'assurance, et veiller à ce que l'évaluation des risques de fraude soit intégrée dans l'évaluation globale des risques de l'organisation ;
- les auditeurs internes, qui connaissent bien les scénarios et contrôles des risques de fraude au sens large ;
- d'autres intervenants, internes ou externes, qui peuvent apporter des compétences supplémentaires.

Le processus d'évaluation des risques peut prendre de nombreuses formes différentes, dont les plus courantes sont les entretiens, les questionnaires et les réunions. Quelle que soit l'approche retenue, il est essentiel que les participants aient un esprit ouvert et fassent preuve de créativité pour couvrir un éventail de risques de fraude suffisamment large.

Identification des risques de fraude

La réflexion collective est un moyen efficace d'établir la liste des scénarios de fraude la plus complète. Même si la technique n'est pas toujours la même, la réflexion collective suppose la participation de tous les membres de l'équipe chargée d'évaluer les risques (voir plus haut). Elle peut aider l'organisation à définir et analyser les divers et nombreux scénarios potentiels. Lorsque la réflexion collective porte sur les risques de fraude, il faut veiller à ce que la discussion ne se limite pas aux scénarios dans lesquels une fraude est commise par une seule personne. Souvent, en effet, la fraude implique la collusion entre plusieurs personnes et, bien que la réflexion collective sur de tels scénarios soit plus ardue, elle n'en est pas moins importante.

Le *Fraud Guide* énumère un certain nombre d'éléments à considérer pour la réflexion collective sur des scénarios de risques de fraude. Il convient de prendre en compte la totalité de ces éléments pour couvrir tous les cas de risques de fraude possibles.

- **Incitations, pressions et opportunités.** Les motivations des fraudeurs peuvent être multiples. Lors d'une séance de réflexion collective portant sur des scénarios de risques de fraude, la

Copyright © 2015 Eyrolles.

Assurance raisonnable

Niveau d'assurance étayé par des procédures et des jugements d'audit généralement acceptés.

première difficulté est d'identifier le plus grand nombre possible de ces motivations. Comme l'a montré la section consacrée au Triangle de la fraude, une fraude est commise lorsqu'il existe une incitation ou une pression, qu'une opportunité se présente et que le fraudeur peut avancer une justification pour son comportement. Il n'est pas fréquent d'effectuer une réflexion collective sur les scénarios de justification, étant donné qu'il faut d'abord examiner les deux autres composantes du Triangle de la fraude et que la justification peut être propre à une personne. Néanmoins, en se concentrant sur les différentes incitations, pressions et opportunités potentielles, on peut identifier des scénarios auxquels l'organisation peut être confrontée. Parmi les incitations peuvent figurer l'argent ou d'autres gains susceptibles de donner à des individus une raison de ne pas se comporter normalement. De même, des personnes peuvent être amenées à agir différemment pour se soustraire à des pressions. Les opportunités sont les possibilités de commettre une fraude sans que celle-ci soit éventuellement détectée (par exemple lorsque les contrôles sont faibles). On peut probablement définir la plupart des scénarios de fraude en procédant à une réflexion collective sur les incitations, pressions et opportunités potentielles.

- **Risque de contournement des contrôles par le management.** Même lorsqu'un système solide de contrôle interne est en place, le risque de contournement des contrôles ne peut être totalement exclu. Il peut arriver que le management, auquel on fait généralement « confiance » pour prendre de bonnes décisions, contourne les contrôles car, le plus souvent, les autres collaborateurs ne contestent pas ses décisions et supposent qu'elle agit pour le bien de l'organisation. De nombreux cas de contournement des contrôles par le management dans le but de faciliter le reporting financier frauduleux ou le détournement d'actifs ont été rapportés. La réflexion collective sur les scénarios de contournement des contrôles par le management permet d'identifier des scénarios différents de ceux obtenus avec la réflexion collective portant sur les incitations, pressions et opportunités.
- **Classification des risques de fraude.** Il existe des risques de fraude « universels », qui concernent toutes les organisations, et d'autres propres à certains secteurs ou pays. Bien que la réflexion collective permette d'identifier la plupart de ces risques, ces scénarios sont parfois déjà documentés et disponibles auprès d'autres sources : organisations sectorielles, associations professionnelles, cabinets-conseil, etc. L'ACFE a établi une classification des risques de fraude en entreprise. Cette classification peut aider les organisations à procéder à la réflexion collective sur les scénarios de risques de fraude. Elle est présentée dans l'encadré 8-6.
- **Reporting financier frauduleux.** Les éléments décrits ci-dessus doivent permettre d'identifier la plupart des risques de fraude au sein d'une organisation. Il est néanmoins utile

Copyright © 2015 Eyrolles.

de prendre également en compte des types de scénarios spécifiques, afin de déterminer si d'autres scénarios pourraient se produire. Les scénarios de reporting financier frauduleux suscitent beaucoup de préoccupations depuis quelques années, au point qu'ils ont donné lieu à une législation dans de nombreux pays (à l'instar de la loi Sarbanes-Oxley). Ces textes visent à réduire la probabilité de fraudes graves dans le reporting financier. C'est un point qui mérite une réflexion collective avec les auditeurs externes, car ceux-ci sont susceptibles de travailler sur ce type de scénarios.

- **Détournement d'actifs.** Un autre scénario spécifique est le risque de détournement d'actifs. Il faut tout d'abord identifier les actifs de l'organisation qui pourraient être convoités par des collaborateurs ou par des tiers (fournisseurs ou clients, par exemple). On peut ensuite définir les scénarios qui permettraient le détournement de ces actifs. Il importe de se souvenir que les mesures de protection physique ne sont pas toujours suffisantes. Ce type de fraude concerne forcément des actifs corporels, tels que les liquidités, le stock, les matières premières et le matériel, mais aussi, éventuellement, des actifs incorporels, par exemple des données confidentielles relatives aux collaborateurs ou à la clientèle, ou des plans et dessins commerciaux. Les systèmes d'information jouent donc un rôle important dans la réduction de certains risques de détournement d'actifs.

- **Corruption.** Dans le *Fraud Guide*, la corruption « est définie, du point de vue opérationnel, comme l'utilisation abusive d'un pouvoir dans le but d'en tirer un avantage privé »[6]. La corruption consiste, par exemple, à verser des pots-de-vin à des fonctionnaires étrangers ou aider et encourager d'autres organisations à frauder. Le temps consacré à la réflexion collective sur les scénarios de corruption dépend du secteur d'activité de l'organisation, ainsi que des pays dans lesquels celle-ci opère, mais il ne faut pas négliger ces scénarios.

- **Autres risques de fraude.** Il peut exister d'autres risques de fraude potentiels. Le *Fraud Guide* cite à ce propos les infractions à la réglementation ou à la législation, telles que « […] les conflits d'intérêts, les délits d'initié, le vol de secrets commerciaux de concurrents, les pratiques anticoncurrentielles, les infractions au droit environnemental, les infractions à la réglementation sur les échanges et les infractions douanières à l'import/export »[7]. Ils peuvent aussi nuire à la réputation de l'organisation. Nombre des risques déjà identifiés peuvent avoir un impact sur la réputation, mais il peut aussi en exister d'autres.

Exemples de non-respect de la réglementation ou de la législation

Conflits d'intérêts, délits d'initiés, vol de secrets commerciaux de concurrents, pratiques anticoncurrentielles, infractions au droit environnemental, infractions à la réglementation sur les échanges et infractions douanières à l'import/export.

Avant de finaliser la liste des scénarios de risques de fraude, il importe de bien comprendre, pour chaque scénario, les causes qui peuvent en être à l'origine et les niveaux de l'organisation auxquels ce scénario peut se matérialiser. Si plusieurs scénarios ont la même cause, il peut être nécessaire d'évaluer cette cause, plutôt

Copyright © 2015 Eyrolles.

que de creuser les autres scénarios. Une organisation doit *in fine* déterminer les moyens de traiter les causes des risques, et non les symptômes éventuellement visibles. De même, en déterminant à quel niveau de l'organisation les scénarios sont susceptibles de se concrétiser, il est ultérieurement plus facile de définir des moyens d'action. Le temps supplémentaire consacré, à ce stade, à une telle analyse, renforce l'efficacité des autres éléments du programme d'évaluation des risques de fraude.

À l'évidence, l'identification de scénarios de risques de fraude n'est pas une science exacte. Elle nécessite d'obtenir des informations auprès de sources très diverses, régulièrement. De plus, la réflexion collective n'a jamais vraiment de fin : la liste des scénarios de fraude potentiels ne cesse d'évoluer. Néanmoins, comme l'évaluation des risques de l'organisation, l'identification des risques de fraude fonde les étapes suivantes de l'évaluation des risques de fraude.

Évaluation de l'impact et de la probabilité d'occurrence des risques de fraude

L'évaluation de l'impact et de la probabilité potentiels de chaque scénario de fraude est un processus très subjectif, qui met en œuvre les concepts décrits au chapitre 4. Les principaux éléments à prendre en compte sont les suivants.

- **Impact.** Comme indiqué plus haut, il importe de réfléchir à tous les effets possibles d'un scénario de risque de fraude, et pas seulement à l'impact monétaire ou sur les états financiers. Les autres effets peuvent être plus importants. Ainsi, il est essentiel de tenir compte de l'impact juridique (conséquences pénales ou civiles), de l'impact sur la réputation (tel que les dommages causés à une marque), de l'impact opérationnel (coût de production ou responsabilité dans le cas d'une garantie, par exemple) et de l'impact sur les ressources humaines (problèmes de santé et de sécurité ou impossibilité d'attirer et retenir les collaborateurs dans une organisation dans laquelle l'ambiance est morose). Il s'agit d'identifier des scénarios de risques de fraude dont les effets dépassent le seuil de tolérance défini par le management. Étant donné la difficulté à quantifier précisément ces effets, on classe habituellement l'impact mesuré dans l'une des catégories générales suivantes : impact très significatif, impact relativement significatif ou impact non significatif.

Impact

Gravité des conséquences d'un événement (risque). Se mesure en termes d'impacts financiers, juridiques, de réputation ou autres.

- **Probabilité.** L'appréciation de la probabilité ou de la fréquence d'un scénario de fraude dépend en partie des cas de fraude antérieurs, c'est-à-dire des occurrences précédentes de ce scénario au sein de l'organisation ou d'autres organisations opérant dans le même secteur d'activité ou dans la même zone géographique. Néanmoins, il convient d'estimer la probabilité d'un scénario de

Probabilité

Possibilité qu'un événement (risque) survienne.

Copyright © 2015 Eyrolles.

fraude même si l'on n'a pas connaissance de précédents. Comme pour l'évaluation de l'impact, il n'est habituellement pas possible, ni même nécessaire, de quantifier précisément cette probabilité. C'est pourquoi il est plus fréquent de recourir à des appréciations générales : impact probable, possible ou peu probable, par exemple.

Le management doit évaluer simultanément l'impact et la probabilité des scénarios de risques de fraude. Cette évaluation donne un contexte suffisant pour commencer à définir les ressources à consacrer à la gestion des scénarios et le niveau de priorité à y accorder.

Traitement du risque de fraude

Comme indiqué plus haut, le seuil de tolérance défini par le management influe sur l'évaluation des risques de fraude. En général, la tolérance d'une organisation vis-à-vis des risques de fraude est plus faible que sa tolérance à l'égard des autres risques. Plus précisément, lorsqu'une organisation évalue l'impact potentiel sur sa réputation ou sa responsabilité juridique éventuelle, elle peut fixer une « tolérance zéro » pour nombre des risques de fraude. Cette tolérance zéro influence, et peut-être limite, l'éventail des options dont l'organisation dispose pour faire face à ces risques. Cependant, certains effets éventuels des fraudes peuvent être acceptables et ces risques peuvent alors être traités avec davantage de souplesse.

La tolérance au risque étant variable d'une organisation à l'autre, le traitement du risque de fraude diffère lui aussi. Il s'appuie sur les concepts définis dans le cadre de référence relatif au management des risques de l'entreprise élaboré par le COSO (voir chapitre 3). Ce référentiel décrit quatre modalités possibles de traitement des risques.

- Si un risque est si inacceptable que l'organisation ne peut pas se permettre de laisser la moindre fraude survenir, le management doit réfléchir à des moyens d'*éviter* ce risque. Cela peut se traduire par exemple par la cession d'une activité dans un pays où le risque de corruption est beaucoup trop élevé.
- Si une organisation affiche une tolérance faible ou nulle vis-à-vis d'un risque en particulier mais qu'elle ne peut pas éviter ce risque sans compromettre la réalisation de ses objectifs, elle doit concevoir des contrôles destinés à *réduire* la probabilité d'occurrence d'une fraude ou l'impact de cette fraude si celle-ci survenait. À cette fin, elle peut mettre en place une combinaison appropriée de contrôles préventifs et détectifs (voir les deux sections ci-après).
- Si une organisation souhaite réduire l'impact ou la probabilité d'un risque, mais estime qu'il lui manque les compétences ou l'expérience nécessaires pour y parvenir de manière efficace

Copyright © 2015 Eyrolles.

et efficiente, elle peut *partager* la mise en œuvre des contrôles préventifs et détectifs avec une autre organisation qui, elle, est mieux à même de réaliser ces contrôles.

- Si l'occurrence d'un risque est acceptable, le management peut décider de *tolérer* ce risque à son niveau actuel et de ne pas déployer d'efforts particuliers pour le gérer.

Lorsque les décisions relatives au traitement des risques ont été prises, le management doit lancer les actions qui permettront leur mise en œuvre. Étant donné que la plupart des modalités de traitement du risque de fraude consistent à réduire ce risque, les deux sections suivantes sont consacrées à la prévention et à la détection de la fraude.

TRAITEMENT DES ACTES ILLÉGAUX

Tolérance au risque

Niveau de risque et d'écart acceptable entre les objectifs et la performance réelle ; elle doit être en adéquation avec l'appétence pour le risque de l'organisation.

La complexification, l'interconnexion et l'accélération croissantes de l'environnement économique ont conduit à une démultiplication des lois et règlements dans le monde. Les organisations appartenant aux secteurs les plus fortement réglementés, tels que les services financiers et la santé, sont pleinement conscientes de devoir mettre en place et maintenir une infrastructure de conformité sophistiquée.

La définition que l'IIA donne de la fraude est particulièrement intéressante : « Tout acte *illégal* caractérisé par la tromperie, la dissimulation ou la violation de la confiance ». Dans les organisations de nombreux secteurs très réglementés, il n'est pas rare de voir le responsable de l'audit interne rendre directement compte au chef du contentieux ou au directeur juridique car la conformité revêt une grande importance. Dans de nombreux cas, les actes illégaux sont également frauduleux, de sorte qu'il est parfaitement possible de transposer les techniques de gestion et de traitement du risque de fraude au domaine des actes illégaux. Néanmoins, il est important de savoir que les activités illégales, frauduleuses, ou contraires à la déontologie ou la morale, ne recouvrent pas toutes les mêmes aspects.

Imaginons que votre voiture soit garée sur une place payante pendant que vous assistez à une réunion qui s'éternise. Si vous n'avez pas mis assez d'argent dans le parcmètre, votre voiture sera garée « illégalement » mais il ne s'agira pas d'une fraude pour autant. Il n'est pas rare que des organisations qui mènent des activités à l'étranger ignorent certaines réglementations spécifiques (notamment si celles-ci sont rédigées dans une langue autre que l'anglais) ou qu'elles aient été mal conseillées par leurs avocats. On pourrait donc dire que les activités qu'elles mènent sans autorisation dans le pays concerné sont illégales, mais en aucun cas frauduleuses.

Copyright © 2015 Eyrolles.

Le non-respect de la législation applicable peut avoir de graves conséquences, comme le prouvent les poursuites judiciaires et les condamnations à des amendes en vertu du *Foreign Corrupt Practices Act* (FCPA). Aux termes du jugement attendu de longue date, rendu en décembre 2008, dans l'affaire opposant Siemens AG aux autorités de régulation et de supervision américaines et allemandes, l'organisation a été condamnée à des amendes cumulées d'un montant supérieur à 1,6 milliard pour des actes de corruption généralisée et de versements de pots-de-vin, contraires aux dispositions du FCPA. Ce jugement a été rapidement suivi de deux autres condamnations visant Kellogg Brown & Root, Inc. et Halliburton Company, en février 2009, pour un total de 579 millions d'amendes pénales et de restitution de profits, confirmant ainsi que le cas de Siemens n'était pas une exception. Au cours des deux premiers trimestres de 2012, plusieurs organisations, y compris Weatherford International, Avon et News Corp., ont informé la SEC qu'elles avaient dépensé bien plus de 100 millions dans des enquêtes en lien avec le FCPA. Peu après l'émergence de rumeurs concernant une opération de corruption chez Walmart's Mexique, l'organisation a annoncé qu'elle allait nommer un responsable FCPA au niveau mondial et procéder à une enquête rigoureuse.

Par conséquent, la conformité au FCPA de 1977 est récemment devenue une source majeure de préoccupation pour les organisations opérant à l'international. Au-delà de la résonance des jugements évoqués plus haut, ces évolutions ont eu plusieurs implications notables pour les organisations américaines et internationales qui opèrent dans le contexte réglementaire actuel. La priorité donnée à la lutte contre les actes illégaux ne faiblit pas. Pour preuve, le Royaume-Uni a voté une loi anti-corruption (*United Kingdom Bribery Act*) en 2010. Il semblerait que cette loi soit encore plus contraignante et son champ d'application encore plus large que ne l'est le FCPA.

Certains sujets se rapportant au FCPA sont pertinents pour les auditeurs internes qui traitent de questions liées à la conformité, comme :

- les dispositions anti-corruption et les questions de conformité liées ;
- les dispositions liées à la conservation de registres et au contrôle comptable interne ;
- les mesures liées à la *due diligence* et à la mise en œuvre de la conformité ;
- les enquêtes internes, les obligations de déclaration d'informations et le pilotage ;
- les questions contractuelles, opérationnelles et de recrutement ;
- les mesures permettant d'éviter les infractions au FCPA et de prévenir les actions répressives.

Copyright © 2015 Eyrolles.

Pour fournir des éclairages pertinents à leur organisation, les auditeurs internes doivent se tenir informés des évolutions récentes dans ce domaine, à savoir :

- qu'il existe une forte activité répressive et des pénalités associées de la part des régulateurs autres qu'américains dans le monde entier[8] ;
- que, d'après le procureur général adjoint Matthew Friedrich, les régulateurs américains poursuivront leurs efforts pour « restaurer des conditions équitables, éradiquer la corruption et rendre l'environnement économique ouvert à tous ceux qui souhaitent y participer », et n'hésiteront pas à enquêter et à entamer des poursuites à l'encontre d'organisations sises ailleurs qu'aux États-Unis[9] ;
- que l'État américain fait une interprétation très large de la portée juridictionnelle du FCPA[10] ;
- que les enquêtes réglementaires étrangères peuvent servir de base au ministère de la Justice américain et à la *Securities and Exchange Commission* (SEC) pour lancer une investigation, et que les régulateurs américains et étrangers collaborent aujourd'hui régulièrement dans des affaires de lutte contre la corruption[11] ;
- qu'il est nécessaire de posséder un cadre de conformité robuste et de répondre de manière appropriée aux signaux d'alerte ;
- qu'il est important de prendre des actions correctives appropriées contre les collaborateurs fautifs, notamment lorsqu'ils ont des niveaux de responsabilité élevée ; et
- que les services de répression américains se montrent ouverts à la création de mesures pour faciliter les enquêtes internes des organisations, notamment à travers des programmes de clémence et d'amnistie pour les collaborateurs et les dirigeants qui collaborent avec les autorités.

L'encadré 8-9 présente les activités illégales qui font l'objet d'enquêtes en vertu du FCPA et l'encadré 8-10 dresse la liste des signaux d'alerte d'actes illégaux que les auditeurs internes doivent anticiper.

PRÉVENTION DE LA FRAUDE

Dans un monde idéal, une organisation préfère appliquer des contrôles préventifs de la fraude suffisants pour empêcher la réalisation de tous les scénarios de fraude potentiels. Cependant, la prévention absolue n'est pas possible et, dans de nombreux cas, le coût de prévention de certains scénarios de fraude est supérieur aux effets positifs attendus. C'est pourquoi les organisations élaborent des programmes antifraude qui reposent sur un dosage approprié de contrôles préventifs et détectifs. Néanmoins, le vieil adage selon

Copyright © 2015 Eyrolles.

ENCADRÉ 8-9

EXEMPLES D'INFRACTIONS AU *FOREIGN CORRUPT PRACTICES ACT* (FCPA) ET D'ALLÉGATIONS DE BLANCHIMENT D'ARGENT

Si le *Foreign Corrupt Practices Act* (FCPA) date de 1977, ce n'est qu'à partir de 2007 que le ministère de la Justice américain a mis en place une politique véritablement répressive. Les amendes et pénalités imposées et l'atteinte à la réputation peuvent s'avérer telles que toutes les organisations américaines menant des activités à l'étranger ont investi d'importantes ressources pour s'assurer qu'elles respectaient bien le FCPA.

Les domaines suivants devraient faire l'objet d'une attention particulière pour toute organisation opérant à l'international, car ils peuvent représenter des « terrains minés » :

- le paiement d'intermédiaires sans réel motif opérationnel ou sans qu'un travail concret soit réalisé en contrepartie ;
- l'obtention et la conservation d'une documentation détaillée concernant la substance, l'objectif et l'approbation des transactions ;
- l'évaluation du fait que des paiements de facilitation puissent ou doivent être réalisés ;
- l'octroi de cadeaux et le paiement ou le remboursement des frais de déplacement ou de divertissement extravagants ;
- la réalisation d'importants versements en espèces ;
- la qualification erronée de paiements dans les registres comptables.

Pour les seules années 2011-2012, plusieurs organisations telles que Weatherford International, News Corp., et Avon Products ont informé la SEC qu'elles avaient dépensé plus de 100 millions par an dans des enquêtes en lien avec le FCPA (et ce, sans compter les amendes et pénalités potentielles qui pourraient être imposées par les régulateurs à une date ultérieure).

En juin 2008, le géant du secteur des cosmétiques Avon a ouvert une enquête interne après avoir pris connaissance d'allégations concernant le fait que ses activités en Chine auraient abusivement encouru des frais de déplacement, de divertissement et autres. En juillet 2009, Avon a dévoilé que ces infractions au FCPA s'étendaient à l'Amérique latine. Il n'est pas rare qu'une enquête liée au FCPA entamée dans un pays conduise à s'intéresser à un autre pays où l'organisation (ou le dirigeant suspecté) est présente. Dans son rapport annuel 2011, Avon a déclaré avoir dépensé depuis 2009 la somme astronomique de 247 millions (93,3 millions en 2011, 95 millions en 2010, et 59 millions en 2009) dans des frais professionnels et frais liés, en lien avec une enquête FCPA au niveau mondial. Comme il est précisé dans le rapport annuel : « Bien que ces frais soient difficiles à prévoir, ils devraient continuer d'exister et pourraient varier au cours de cette enquête. »

Selon un article de *ComplianceWeek* de juin 2012, les experts juridiques sont partagés sur la question de l'auto-déclaration d'une enquête interne aux services de répression. Ils s'accordent à dire que c'est une décision qui doit être soigneusement examinée ; il suffit peut-être tout simplement de mettre en œuvre rapidement des mesures correctives et de réviser et d'améliorer les règles et les procédures de conformité.

Sources : *The Ernst & Young Guide to Investigating Business Fraud*, AICPA, 2009 ; *ComplianceWeek*, juin 2012, article de Jaclyn Jaeger intitulé, « *High Cost of Conducting Full FCPA Investigations* » (Le coût élevé des enquêtes FCPA intégrales – pp. 1, 24–25).

lequel « mieux vaut prévenir que guérir » est un bon point de départ pour définir des actions destinées à ramener les risques de fraude à un niveau acceptable.

Il existe différentes catégories de techniques de prévention, dont plusieurs sont analysées ci-dessous. Toutefois, l'une des formes de prévention les plus importantes est la sensibilisation au sein

Copyright © 2015 Eyrolles.

de l'organisation. Le *Fraud Guide* indique que « l'un des grands principes de la prévention consiste à sensibiliser le personnel, dans toute l'organisation, au programme de gestion du risque de fraude, et notamment aux différents types de fraude et d'abus potentiels. On peut ainsi montrer que toutes les techniques prévues dans ce programme sont bien réelles et seront appliquées »[12]. En d'autres termes, une bonne sensibilisation au sein de l'organisation a un effet dissuasif sur la fraude.

Pour une organisation, la prévention est un moyen de prendre les devants pour lutter contre la fraude. En intégrant des contrôles préventifs dans le système de contrôle interne, le management peut dissuader la plupart des personnes d'envisager de commettre une fraude. Outre l'instauration d'un solide environnement de gouvernance antifraude, le *Fraud Guide* présente un certain nombre de processus qui peuvent largement contribuer à prévenir la fraude.

- **Enquête sur les antécédents.** Certaines personnes sont plus susceptibles que d'autres de céder à des tentations qui peuvent les amener à frauder. Une personne qui a déjà fraudé est également plus susceptible de recommencer qu'une autre qui n'a encore jamais fraudé. Une enquête détaillée sur les antécédents peut permettre d'écarter de l'organisation les personnes qui sont les plus susceptibles de frauder. Ce type d'enquête peut concerner des candidats à un poste dans l'organisation, mais aussi des fournisseurs, clients et partenaires commerciaux nouveaux ou anciens, afin de limiter le risque de fraude par ces tiers.
- **Formation à la lutte contre la fraude.** Même si les collaborateurs embauchés sont compétents et honnêtes, ils doivent comprendre en quoi consiste la fraude, les signaux d'alerte à surveiller, les procédures permettant de signaler des cas de fraude potentiels et les conséquences de la fraude. Cette formation doit être obligatoire et renouvelée périodiquement.
- **Évaluation des performances et systèmes de rémunération.** Les organisations doivent veiller à ne pas inciter à des comportements répréhensibles. Il faut examiner de près les systèmes de rémunération pour vérifier que, non seulement, ils encouragent les bons comportements, mais également qu'ils les récompensent. Ces systèmes ne doivent pas négliger les comportements susceptibles d'inciter (ou être considérés comme incitant) à des comportements potentiellement frauduleux.
- **Entretien de départ.** Des collaborateurs partent pour diverses raisons, et, souvent, ils souhaitent expliquer pourquoi. L'entretien de départ est souvent considéré comme un contrôle détectif parce qu'une personne peut vouloir « dénoncer » quelqu'un qu'elle n'a pas voulu mettre en cause lorsqu'ils étaient collègues. Cependant, le fait même de savoir que des entretiens de départ ont lieu peut également avoir un effet dissuasif sur la fraude. L'entretien de départ est donc aussi un contrôle préventif.

Copyright © 2015 Eyrolles.

- **Plafonnement des transactions autorisées.** On peut empêcher des fraudes potentielles en plafonnant les transactions autorisées. Il est fréquent, par exemple, d'interdire les virements externes dépassant un certain montant s'ils n'ont pas été autorisés par deux personnes. Dans l'hypothèse de l'absence de collusion entre ces personnes, un tel contrôle empêche les transactions frauduleuses portant sur un montant supérieur.
- **Vérification des transactions *ex ante*.** Nombre de cas de fraudes impliquent des tiers, notamment des parties liées. En imposant une vérification minutieuse de ces transactions avant qu'elles ne soient réalisées, une organisation peut empêcher des transactions inappropriées (exemple : référentiels fournisseurs validés en amont).

Contrôle préventif

Activité destinée à empêcher la survenue d'événements non souhaités.

Dans le cadre du système de contrôle interne de l'organisation, les contrôles préventifs doivent être documentés comme tous ces autres contrôles. Cela permet d'évaluer plus facilement l'adéquation de leur conception, et a également un effet dissuasif, dans la mesure où les collaborateurs savent que ces contrôles sont en place. L'évaluation de l'adéquation des contrôles préventifs de la fraude nécessite de l'expérience et une bonne capacité de jugement, mais il existe un certain nombre d'outils qui facilitent ce processus. Ainsi, l'annexe F du *Fraud Guide*, consacrée aux tableaux de bord de prévention de la fraude, vise à faciliter l'identification et l'évaluation

ENCADRÉ 8-10

SIGNAUX D'ALERTE D'ACTES POTENTIELLEMENT ILLÉGAUX

- Transactions non autorisées, transactions enregistrées de manière incorrecte, ou transactions enregistrées en retard ou de manière incomplète, rendant impossible le devoir de rendre compte en matière de gestion des actifs
- Enquête d'une agence gouvernementale, procédure d'exécution, ou paiement d'amendes ou de pénalités inhabituelles
- Violations de lois ou règlements citées dans des rapports d'examens rédigés par les autorités de régulation et de supervision et mis à disposition de l'auditeur
- Versements importants à des consultants, des sociétés affiliées ou des collaborateurs pour des services non spécifiés
- Commissions de vente ou honoraires des agents qui semblent excessifs par rapport à ceux normalement payés par le client ou par rapport aux services effectivement reçus
- Versements en espèces inhabituellement importants, achats de chèques de banque payables au porteur en grande quantité, transferts vers des comptes bancaires numérotés, ou transactions similaires
- Versements inexpliqués à des fonctionnaires ou représentants de l'État
- Manquements à l'obligation de déclaration d'impôts ou de paiements des redevances étatiques ou frais similaires qui s'appliquent au secteur dans lequel exerce l'entité ou à la nature de son activité

Source : Grant Thornton, *The Audit Committee Guide Series. Managing Fraud Risk: The Audit Committee Perspective*. Reproduction autorisée.

Copyright © 2015 Eyrolles.

de quelques-uns des aspects les plus courants d'un système de prévention de la fraude.

Le *Fraud Guide* souligne l'importance de contrôles préventifs solides en indiquant que, « pour être efficace, tout programme de prévention de la fraude doit, en permanence, être diffusé dans l'organisation et renforcé. En montrant clairement (par un affichage, une note d'information jointe aux factures clients et au règlement des factures fournisseurs, des messages entrant dans le cadre de la communication interne ou externe, etc.) qu'un programme de prévention de la fraude est en place, on fait savoir, à la fois en interne et à l'extérieur, que l'organisation s'attache à prévenir et à dissuader la fraude. »[13] Les travaux menés par l'*Institute for Fraud Prevention* sont également dignes d'intérêt (http://www.theifp.org/).

DÉTECTION DE LA FRAUDE

Collusion

Acte impliquant au moins deux personnes qui travaillent ensemble et qui, pour obtenir un avantage personnel, contournent des contrôles ou des procédures en place.

Comme indiqué plus haut, un programme efficace de gestion du risque de fraude ne peut pas reposer uniquement sur la prévention. En effet, non seulement le coût de prévention de certains scénarios de fraude est élevé, mais il n'est pas non plus possible d'empêcher tous les cas de fraude. La prévention de la fraude peut échouer si les contrôles préventifs ne sont pas adéquats ou efficaces. De plus, en cas de collusion entre des personnes ou de contournement par le management, les contrôles en place destinés à prévenir la fraude sont susceptibles d'être contournés. Il faut donc que l'organisation procède aussi à un dosage prudent des contrôles détectifs de la fraude.

Par définition, les contrôles détectifs visent à identifier les fraudes ou les signes susceptibles d'indiquer une fraude. Les méthodes de détection de la fraude peuvent être soit conçues spécifiquement dans le but de repérer les fraudes, soit intégrées dans le système de contrôle interne et ne pas servir uniquement à la détection de la fraude. Par exemple, la réalisation et la vérification d'un rapprochement bancaire peut avoir de nombreuses finalités, notamment l'identification de transactions inhabituelles ou suspectes. Le *Fraud Guide* décrit plusieurs méthodes de détection courantes.

- **Dispositifs d'alerte.** Comme indiqué plus haut dans ce chapitre, la méthode la plus courante pour détecter la fraude consiste à faire appel à des lanceurs d'alerte. Une ligne téléphonique dédiée permet à toute personne de faire part, anonymement, de ses soupçons à l'égard de certaines activités. Les dispositifs d'alerte sont fréquemment gérés par des tiers, pour permettre aux personnes de signaler plus facilement des problèmes, sans avoir peur de subir des représailles. S'il est largement connu, il peut avoir un effet dissuasif en montrant aux fraudeurs potentiels que chacun peut facilement faire part de ses soupçons.

Copyright © 2015 Eyrolles.

Le cas échéant, les organisations qui mettent en place ce type de ligne d'alerte doivent l'accompagner d'un système efficace de gestion des dossiers, qui permet aux allégations d'être notifiées à la personne compétente, d'être examinées de près, de donner lieu à des investigations et, le cas échéant, d'être traitées rapidement sur la base de données factuelles. La gestion des dossiers est généralement assurée par le responsable du programme de conformité, par le service des ressources humaines, par le service juridique ou par le service d'audit interne.

- **Contrôles des processus.** Les contrôles détectifs de la fraude les plus courants sont intégrés aux processus quotidiens : rapprochements, revues indépendantes, inspections physiques ou comptages, certains types d'analyse, audits internes ou autres activités de surveillance, par exemple. Les risques de fraude qui ont le plus fort impact potentiel peuvent nécessiter des contrôles détectifs à un niveau de sensibilité plus faible, afin que la détection soit rapide.
- **Détection de la fraude par anticipation.** Bien que la détection semble par nature réactive, il est possible de concevoir des procédures reposant davantage sur l'anticipation. Les plus courantes consistent à analyser des données, mener des audits en continu et utiliser d'autres outils technologiques qui permettent de repérer des anomalies, des tendances et des indicateurs de risques méritant une certaine attention. Certaines des techniques de détection de la fraude les plus innovantes s'appuient, grâce au système d'information, sur l'analyse de données provenant de nombreuses sources. Autre exemple : un logiciel qui recherche certains termes ou certaines expressions dans des courriels peut repérer des personnes susceptibles d'envisager de commettre une fraude ou qui sont déjà en train de le faire.

Une organisation peut s'aider de techniques de surveillance et de mesure en continu pour évaluer et améliorer ses techniques de détection de la fraude. Elle peut mesurer différents critères. L'encadré 8-11 en dresse une liste, qui peut servir aux organisations à surveiller, mesurer et évaluer l'efficacité de leurs dispositifs de détection de la fraude.

Les contrôles destinés à détecter la fraude sont très nombreux et variés. Les organisations doivent se concentrer sur ceux qui permettront le plus probablement de repérer rapidement les scénarios de fraude. L'annexe G du *Fraud Guide*, consacrée aux tableaux de bord de détection de la fraude, vise à faciliter l'identification et l'évaluation de quelques-uns des aspects les plus courants d'un système de détection de la fraude.

Les organisations peuvent évaluer l'efficacité de leurs dispositifs de détection de la fraude à partir des critères de mesure exposés dans le *Fraud Guide*, dont l'encadré 8-11 dresse la liste.

Copyright © 2015 Eyrolles.

ENQUÊTES ET ACTIONS CORRECTIVES

Bien sûr, il est important de détecter les fraudes, ou les symptômes d'une fraude, mais ce n'est pas suffisant. Qu'un cas de fraude fasse l'objet d'une action en justice ou soit traité dans l'organisation qui en est victime, il est impératif de comprendre tous les faits et circonstances qui entourent une fraude. La phase finale d'un programme efficace de gestion du risque de fraude est donc axée sur les investigations, le reporting et le traitement des cas de fraude potentiels. Elle comporte plusieurs étapes.

Réception des allégations

Les allégations peuvent provenir de diverses sources et se présenter sous de nombreuses formes différentes. Comme indiqué plus haut dans ce chapitre, le rapport de l'ACFE montre que les méthodes les plus courantes pour détecter les fraudes consistent à faire appel à des lanceurs d'alerte, ou à réaliser des audits ou des contrôles. Quelle que soit la source des allégations, une organisation doit disposer d'un processus ou protocole qui lui permette de rassembler les informations disponibles en ce qui concerne ces allégations. Elle pourra ainsi « […] élaborer un système permettant, avec rapidité, compétence et en toute confidentialité, d'examiner les allégations de fraude ou une faute potentielle, de mener une enquête et de trancher le cas »[14]. Il n'existe pas d'approche unique pour recevoir des allégations. Tout dépend de la nature de l'allégation, de l'identité de la personne susceptible d'être impliquée et des conséquences potentielles. Indépendamment du protocole mis en œuvre, le *Fraud Guide* spécifie que « le système d'enquête et de traitement des allégations doit inclure un processus destiné à :

- établir une classification des problèmes ;
- confirmer la validité de l'allégation ;
- déterminer la sévérité de l'allégation ;
- faire remonter le problème ou transmettre l'enquête à un niveau supérieur, le cas échéant ;
- se dessaisir des problèmes qui sortent du cadre du programme interne ;
- conduire les investigations et trouver des éléments factuels ;
- touver une issue satisfaisante à l'enquête ou clôturer l'enquête ;
- établir une liste des informations qui doivent rester confidentielles ;
- définir la façon dont l'enquête sera documentée ;
- gérer et archiver les documents et les informations. »[15]

Contrôle détectif

Activité destinée à mettre au jour des événements non souhaitables qui sont déjà survenus. Pour être jugé efficace, un contrôle détectif doit être appliqué rapidement (avant que l'événement en question ait eu un impact négatif sur l'organisation).

Copyright © 2015 Eyrolles.

Ce processus doit être suffisamment souple pour permettre le traitement des nombreux et différents types d'allégations, tout en étant suffisamment structuré pour permettre la mise en œuvre et la documentation de toutes les étapes clés. Un processus formel facilitera les autres phases.

Évaluer les allégations

Les allégations de fraude ne s'avèrent pas toutes fondées. Il faut évaluer les informations reçues et prendre de nombreuses décisions essentielles, qui peuvent avoir une influence déterminante sur l'efficacité du processus. Cette évaluation consiste à répondre aux questions suivantes.

- L'allégation nécessite-t-elle la conduite d'une enquête formelle ou dispose-t-on déjà de suffisamment d'informations pour rendre des conclusions ?
- Qui doit mener l'enquête ?
- Des compétences spécifiques ou des outils particuliers sont-ils nécessaires pour l'enquête ?
- Qui doit être informé et à quel moment ?

L'instauration de protocoles d'enquête formels, selon les principes énoncés ci-dessous, aidera à répondre à l'ensemble des questions fondamentales pour évaluer une allégation.

Mettre en place des protocoles d'enquête

La mise en place de protocoles d'enquête formels validés par la direction générale et le Conseil permet la réalisation des objectifs de l'enquête. Le *Fraud Guide* mentionne un certain nombre de « facteurs à prendre en compte pour élaborer le plan d'enquête.

- *Rapidité* – Il peut être nécessaire de mener les investigations rapidement, pour des raisons juridiques, afin de réduire les pertes ou les dommages potentiels, ou pour déclarer un sinistre à la compagnie d'assurance.
- *Notification* – Certaines allégations peuvent nécessiter une notification aux autorités de régulation et de supervision, aux autorités chargées de faire appliquer la loi, aux assureurs ou aux auditeurs externes.
- *Confidentialité* – Les informations recueillies doivent rester confidentielles et être diffusées aux seules personnes qui en ont effectivement besoin.
- *Protection juridique* – En faisant appel à un avocat-conseil dès le début du processus ou, dans certains cas, pour conduire

Copyright © 2015 Eyrolles.

l'investigation, on peut protéger le produit du travail et la confidentialité des communications entre l'avocat-conseil et son client.

- *Conformité* – Les enquêtes doivent respecter les lois et règles applicables concernant la collecte d'informations et l'interrogation des témoins.
- *Mise en lieu sûr des preuves* – Il convient de protéger les éléments de preuve afin qu'ils ne soient pas détruits et qu'ils puissent être présentés devant les tribunaux.
- *Indépendance* – L'équipe chargée de l'enquête doit être tenue suffisamment à l'écart des problèmes et des personnes faisant l'objet de l'enquête, afin qu'elle puisse procéder à une évaluation objective.
- *Objectivité* – Les problèmes ou préoccupations spécifiques doivent influer de manière appropriée sur l'orientation, le champ et le calendrier de l'enquête. »[16]

L'enquête doit être réalisée de façon à traiter chacun de ces facteurs. Le processus effectif dépendra de la nature des allégations, mais la plupart des enquêtes comportent habituellement un certain

ENCADRÉ 8-11

CRITÈRES DE MESURE POUR LA DÉTECTION DES FRAUDES

- Nombre de cas connus de fraudes commises à l'encontre de l'organisation
- Nombre et état des allégations de fraude reçues par l'organisation et qui ont donné lieu à une enquête
- Nombre d'enquêtes pour fraude qui ont été tranchées
- Nombre de collaborateurs ayant/n'ayant pas signé la déclaration de déontologie de leur organisation
- Nombre de collaborateurs ayant/n'ayant pas achevé leur formation aux questions de déontologie mis en place par leur organisation
- Nombre d'allégations reçues de personnes ayant recouru au dispositif d'alerte éthique mis en place par l'organisation
- Nombre d'allégations reçues par d'autres moyens
- Nombre de messages de l'encadrement incitant les collaborateurs à un comportement éthique
- Nombre de fournisseurs ayant/n'ayant pas signé le code de déontologie de l'organisation
- Comparaisons par rapport à des enquêtes mondiales sur la fraude, y compris en ce qui concerne le type de fraudes et le montant moyen des pertes
- Nombre de clients ayant signé le code de déontologie de l'organisation
- Nombre d'audits portant sur la fraude effectués par les auditeurs internes
- Résultats d'enquêtes menées auprès des collaborateurs ou d'autres parties prenantes concernant l'intégrité et la culture de l'organisation
- Ressources utilisées par l'organisation.

Source : *Fraud Guide*, pp. 38-39.

Copyright © 2015 Eyrolles.

nombre de tâches, telles que l'audition des personnes susceptibles de détenir des informations pertinentes pour l'enquête, la collecte de preuves tangibles auprès de sources internes et externes, l'analyse des données recueillies et la présentation par écrit des résultats, afin d'étayer les conclusions et de permettre aux tiers de comprendre leurs motivations. Enfin, un rapport adéquat est rédigé à l'intention des personnes qui ont besoin des résultats de l'enquête pour pouvoir évaluer les dispositions prises. Ces principes généraux doivent, bien sûr, être adaptés aux contraintes légales du pays concerné.

Prendre des dispositions appropriées

La dernière étape du processus consiste à prendre des dispositions appropriées, d'après les résultats de l'enquête. Les actions possibles sont les suivantes :

- poursuites au pénal et/ou au civil ;
- mesures disciplinaires, telles qu'un avertissement, une rétrogradation, un blâme, une suspension ou un licenciement ;
- déclaration de sinistre auprès de l'assureur si les pertes découlant de la fraude sont couvertes par une police ;
- réorganisation ou renforcement des processus et des contrôles qui ont peut-être été conçus de manière inadéquate, ou qui n'ont pas fonctionné de manière effective, et qui n'ont pas empêché la fraude.

Quelles que soient les mesures retenues, elles doivent être justes et rapides. Au sein de l'organisation, certaines personnes peuvent en effet souhaiter savoir comment les fraudeurs sont traités. Si les dernières dispositions prises ne sont pas rendues publiques, les collaborateurs doivent avoir la certitude qu'elles sont justes étant donné les circonstances, et que la direction générale traiterait d'autres fraudeurs de la même manière. Cela renforce le sentiment que la direction générale « fait preuve d'exemplarité », et cette exemplarité est fondamentale pour la gouvernance de la gestion du risque de fraude.

COMPRENDRE LES FRAUDEURS

Il est naturel de penser qu'un système de contrôle interne est neutre vis-à-vis des personnes. Ainsi, en supposant que des personnes compétentes occupent les postes de contrôle clés dans une organisation, un système de contrôle interne conçu de manière adéquate doit fonctionner de manière effective, même lorsque les personnes commettent des erreurs. Cependant, considérant que la fraude implique une intention d'agir d'une manière différente que

Copyright © 2015 Eyrolles.

Protection juridique

Protection des résultats des investigations, des papiers de travail et de la confidentialité des communications entre l'avocat-conseil et son client.

celle à quoi l'on pourrait s'attendre normalement, un autre élément doit être pris en compte : la façon d'agir des individus malhonnêtes. Les auditeurs internes doivent donc avoir un esprit critique aiguisé et envisager que les gens ne se comporteront pas nécessairement « comme il faut ». Autrement dit, les auditeurs internes doivent essayer de comprendre pourquoi une personne honnête va commettre une action malhonnête, afin de pouvoir déceler, et, dans certains cas, empêcher une fraude.

La science comportementale reste à ce jour incapable d'identifier une caractéristique psychologique ou un ensemble de caractéristiques susceptibles de servir de marqueur fiable de la propension à frauder. Par exemple, il serait simpliste d'affirmer que « l'appât du gain et la malhonnêteté » (refrain bien connu) expliquent tout ce qui s'est passé pendant la période « d'exubérance irrationnelle » des années 1990. Le monde de l'entreprise compte de nombreux professionnels extrêmement ambitieux, compétitifs et riches, mais qui n'en respectent pas moins les lois. Ces professionnels ne recourent pas forcément à la fraude pour satisfaire leur soif de succès. Mais quelque chose les motive, et la compréhension des différentes motivations des fraudeurs constitue un important point de départ. Thomas Golden, expert chevronné et spécialiste de la lutte contre la fraude chez PricewaterhouseCoopers, estime qu'il existe deux profils de fraudeurs qui manipulent les informations financières : ceux « agissant dans l'intérêt général » et les « intrigants et auto-centrés ». Les premiers sont « par ailleurs des personnes honnêtes qui faussent les chiffres en se disant qu'elles le font dans l'intérêt de leur organisation ». Les seconds sont « des individus qui affichent un mépris total pour la vérité, qui sont parfaitement conscients de ce qu'ils font et tentent d'atteindre leurs objectifs par des moyens malhonnêtes »[17]. Comprendre les signaux d'alerte potentiels qui peuvent signaler les personnes qui sont davantage susceptibles de commettre une fraude aide les auditeurs internes à comprendre à quel moment le risque de fraude est accru. Voici des exemples de signaux d'alerte :

- les individus qui affichent un train de vie bien supérieur à leurs moyens actuels ;
- les individus qui connaissent de graves problèmes financiers et/ou qui sont fortement endettés ;
- les individus qui ont une propension inhabituelle à dépenser ;
- les individus qui souffrent de dépression ou d'autres problèmes psychologiques ;
- les joueurs invétérés ;
- les individus qui veulent absolument obtenir un statut social et pensent que l'argent peut les y aider.

Copyright © 2015 Eyrolles.

Fraudeurs

Personnes correspondant généralement à l'un des deux profils de fraudeurs : ceux « agissant dans l'intérêt général » et les « intrigants et auto-centrés ».

Il peut également être utile de considérer la fraude du point de vue d'un criminologue. Les criminologues pensent que la fraude, comme n'importe quel autre délit, peut s'expliquer par trois facteurs : l'existence de contrevenants motivés, la disponibilité de cibles s'y prêtant et l'absence de gardiens compétents (systèmes de contrôles ou individus « qui gardent la boutique »)[18]. Ces éléments se rapprochent du Triangle de la fraude décrit dans la section précédente. La bonne connaissance de ces facteurs peut aider les auditeurs internes à être à l'affût des vulnérabilités à la fraude. Concernant ce dernier point, Joseph Wells, fondateur de l'ACFE, compare de façon instructive la vision des contrôles qu'ont les fraudeurs et leur perception du risque d'être pris. Cette opinion est synthétisée dans l'encadré 8-12.

Les auditeurs internes ne sont censés être ni des experts psychologues en comportement, ni des criminologues. Cependant, comprendre les motivations des fraudeurs peut les aider à « rester en alerte » sur leur lieu de travail et, peut-être, à repérer à l'avance les personnes les plus à même de commettre une fraude.

CONSÉQUENCES POUR LES AUDITEURS INTERNES ET D'AUTRES COLLABORATEURS

Les auditeurs internes jouent un rôle clé dans un programme de gestion du risque de fraude. Les *Normes* donnent des orientations spécifiques à l'intention des auditeurs internes :

Norme 1210.A2 – Les auditeurs internes doivent posséder des connaissances suffisantes pour évaluer le risque de fraude et la façon dont ce risque est géré par l'organisation. Toutefois, ils ne sont pas censés posséder l'expertise d'une personne dont la responsabilité première est la détection et l'investigation des fraudes.

Norme 1220.A1 – Les auditeurs internes doivent apporter tout le soin nécessaire à leur pratique professionnelle en prenant en considération […] la probabilité d'erreurs significatives, de fraudes ou de non-conformité […].

Norme 2060 – Le responsable de l'audit interne doit rendre compte périodiquement à la direction générale et au Conseil des […] risques de fraude […].

Norme 2120.A2 – L'audit interne doit évaluer la possibilité de fraude et la manière dont ce risque est géré par l'organisation.

Les *Normes* affirment clairement que les auditeurs internes doivent envisager la possibilité de fraude dans quasiment toutes leurs activités. Mais les *Normes* ne constituent pas la seule motivation conduisant l'audit interne à se concentrer sur la fraude. La

Copyright © 2015 Eyrolles.

législation récente, les mandats confiés aux autorités de régulation et de supervision, ainsi que le nombre croissant d'organisations axées sur la bonne gouvernance, mettent spécifiquement l'accent sur le rôle de l'audit interne. Par voie de conséquence, les gardiens de la pertinence des dispositifs de contrôle, dont les auditeurs internes, gagnent en importance et sont de plus en plus appelés à jouer un rôle clé dans la prévention, la dissuasion et la détection de la fraude au sein des organisations commerciales, des organismes publics et des entités sans but lucratif, dans le monde entier. Les auditeurs internes, sont invités à répondre à plusieurs questions.

- Quels risques de fraude sont à l'heure actuelle surveillés périodiquement ou régulièrement par le management ? Les facteurs de risque critiques font-ils l'objet d'une surveillance fréquente, voire permanente ?
- Quelles procédures particulières l'audit interne applique-t-il si le management contourne des dispositifs de contrôle interne ?
- Est-il survenu un événement conduisant l'audit interne à réévaluer le risque que le management contourne les contrôles ?
- Quelles compétences et qualifications les auditeurs internes doivent-ils posséder pour traiter le risque de fraude au sein des organisations ? Quand doivent-ils faire appel à des spécialistes pour gérer des aspects particulièrement complexes ?
- Outre le rattachement direct au comité d'audit, comment peut-on renforcer l'indépendance de l'audit interne au sein

ENCADRÉ 8-12

CONTRÔLES ET RISQUE D'ÊTRE PRIS : PERCEPTION DES FRAUDEURS

Joseph Wells, fondateur de l'ACFE, propose une analyse poussée de la manière de penser des fraudeurs. Faisant écho à Jeremy Bentham, économiste du XVIII^e siècle, il observe que la probabilité de commettre un délit (en col blanc) dépend de la perception, par son auteur, des risques et des récompenses. En d'autres termes, ceux qui estiment qu'il existe une forte probabilité de se faire prendre sont naturellement moins enclins à perpétrer une fraude. Du point de vue comportemental, il est donc possible de générer un « effet d'anticipation » (c'est-à-dire l'anticipation d'être audité) par le biais de vérifications surprises intégrées dans les dispositifs de prévention et de dissuasion des fraudes. Selon ce même raisonnement, les auditeurs externes et les auditeurs internes, par des approches innovantes recourant par exemple aux systèmes d'information (par exemple, le pilotage continu des contrôles) ou les avancées de la statistique (par exemple, les méthodes d'échantillonnage de dépistage, la loi de Benford), voire des « séances de réflexion collective sur les moyens de frauder » peuvent exercer un puissant effet dissuasif et dresser des barrières à la fraude, tout en améliorant les capacités de détection. Le management doit agir rapidement et avec fermeté à l'encontre des auteurs des fraudes lorsque ces derniers sont démasqués à la suite d'une enquête. De telles mesures peuvent largement consolider les efforts de dissuasion.

Wells, Joseph T., « Let Them Know Someone's Watching », *Journal of Accountancy*, mai 2002.

Copyright © 2015 Eyrolles.

de l'organisation ? Les auditeurs internes sont-ils considérés comme des professionnels compétents et objectifs pour traiter le risque de fraude et les aspects relatifs aux contrôles ?

- Comment l'audit interne doit-il se concentrer sur la prévention, la dissuasion, la détection et l'investigation de la fraude ?
- Comment l'audit interne peut-il utiliser un logiciel d'analyse de données pour réaliser une détection en amont ?

Pour s'acquitter de cette responsabilité vis-à-vis du comité d'audit et des autres parties prenantes, les auditeurs internes doivent posséder des compétences et une expérience plus importantes que celles qui sont nécessaires à la conduite de la plupart des missions d'assurance.

Scepticisme professionnel, et moyens techniques

L'exercice d'un jugement professionnel avisé est au centre des activités d'assurance et de conseil de la fonction d'audit interne. Lorsqu'il s'agit d'évaluer les risques de fraude, l'auditeur interne doit faire preuve d'un degré élevé de scepticisme professionnel, c'est-à-dire de la capacité à évaluer avec esprit critique les preuves et les données dont il dispose. C'est d'autant plus important que les fraudeurs ont l'habitude « d'effacer leurs traces » et qu'il faut faire preuve d'une certaine détermination pour mettre en évidence un projet de fraude bien dissimulé. Ainsi, la persévérance opiniâtre de Cynthia Cooper, désignée « personnalité de l'année » en 2004 par le magazine *Time*, et de son équipe d'audit interne chez WorldCom, a été déterminante pour faire éclater au grand jour la fraude massive perpétrée par la direction générale de WorldCom.

Tous les auditeurs internes ne font pas preuve du même degré de scepticisme professionnel : certains sont par nature plus sceptiques que d'autres, certains prennent les explications qu'on leur donne pour argent comptant, et d'autres tiennent à vérifier encore et encore et à creuser davantage. Ces derniers, qui semblent avoir une tendance naturelle à « fouiner », font également preuve d'un degré supérieur de scepticisme professionnel en général. Si la « paranoïa » se traduit souvent par un audit excessif, il est attendu et justifié que les auditeurs internes témoignent d'un fort degré de scepticisme professionnel à chaque fois que les faits et les circonstances semblent indiquer une probabilité de fraude.

Lorsqu'ils dirigent ou participent à une enquête sur une fraude, les auditeurs internes peuvent avoir à traiter des preuves dont ils n'ont pas l'habitude dans leurs missions. Ces missions peuvent se révéler plus complexes et nécessiter d'étudier différents éléments de preuve, avec des caractéristiques et des degrés de fiabilité variables. Dans un tel contexte, un auditeur interne expérimenté

Copyright © 2015 Eyrolles.

est mieux à même d'établir des liens et de reconstituer le tableau d'ensemble à partir d'informations et de preuves incomplètes. C'est la raison pour laquelle, la plupart du temps, les groupes d'enquête sur les fraudes sont composés de personnes qui possèdent une grande expérience des contrôles. D'ailleurs, les recherches sur les applications de l'intelligence artificielle (la technologie des réseaux neuronaux, par exemple) montrent que le regroupement de preuves dispersées constitue en fait un problème de reconnaissance des formes : toutes les preuves disponibles ne doivent pas être considérées les unes après les autres, mais une approche holistique tenant compte de toutes les preuves disponibles simultanément doit être développée. L'auditeur interne peut donc utilement utiliser des aides à la décision, des systèmes experts et l'intelligence artificielle pour augmenter à la fois l'efficacité et l'efficience de ses travaux (par exemple, la loi de Benford ou l'analyse des chiffres, les techniques d'audit informatisées, et l'analyse prédictive, y compris les modèles de régression et les réseaux neuronaux). Si les films et les séries télévisées ont tendance à donner une image idéalisée de ce processus, avoir l'esprit d'investigation est un atout pour les auditeurs internes qui évaluent les risques de fraude et réalisent des missions dans ce domaine.

La communication par des moyens technologiques étant omniprésente, l'examen des cas de fraude feront à l'avenir largement appel à des experts informatiques, à la recherche de preuves électroniques et à l'analyse des données. En d'autres termes, l'emploi de la technologie ne se borne pas à l'analyse des données (une fois les données structurées recueillies), mais permet aussi l'extraction et la préservation des preuves électroniques, généralement sous la forme de textes ou de données non structurées nécessitant des recherches par mots-clés. Les inspecteurs doivent donc bien maîtriser les techniques numériques, à savoir les outils et les technologies les plus avancés dans ce domaine.

Le recours à des spécialistes de la lutte contre la fraude

L'audit interne peut lutter contre la fraude de diverses façons au sein d'une organisation. Il peut, par exemple, organiser des sessions de sensibilisation au problème de la fraude, concevoir des programmes et des contrôles antifraude, tester le fonctionnement effectif de ces contrôles, examiner de manière approfondie les anomalies/pratiques répréhensibles et enquêter sur les signalements, ou conduire des enquêtes sur demande du comité d'audit. Cependant, l'audit interne peut ne pas disposer de l'expérience et des compétences nécessaires pour toutes ces activités. En conséquence, il est courant que le responsable de l'audit interne recoure à des spécialistes de la lutte contre la fraude afin de compléter les compétences des auditeurs.

Conscience professionnelle

La diligence et le savoir-faire que l'on peut attendre d'un auditeur interne raisonnablement averti et compétent ; la conscience professionnelle n'implique pas l'infaillibilité.

Copyright © 2015 Eyrolles.

Les auditeurs spécialisés dans la lutte contre la fraude peuvent obtenir le titre de CFE (*Certified Fraud Examiner*). Ils mènent des enquêtes d'expertise (habituellement *a posteriori*, lorsqu'il existe une suspicion), afin de trancher les allégations ou soupçons de fraude, et rendent compte à un niveau hiérarchique approprié (au responsable de l'audit interne, au comité d'audit ou au Conseil, suivant la nature du problème et le niveau hiérarchique des collaborateurs impliqués). Ils peuvent aussi épauler le comité d'audit et le Conseil dans différents aspects du processus de surveillance, soit directement, soit dans le cadre d'une équipe d'auditeurs, internes ou externes, afin de juger de l'évaluation du risque de fraude et des mesures de prévention mises en œuvre par la direction générale. Ils peuvent apporter une contribution plus objective à l'évaluation du risque de fraude effectuée par la direction générale (et surtout des fraudes perpétrées par des cadres dirigeants, comme la falsification des états financiers), ainsi qu'à l'élaboration de mesures de lutte contre la fraude qui soient moins susceptibles d'être contournées par les dirigeants. Ces dernières années, plusieurs professionnels de l'audit interne ont obtenu la certification CFE et, grâce à cette expertise spécialisée, sont mieux parés pour s'acquitter de leurs obligations dans ce domaine. De nombreuses fonctions d'audit interne essaient d'avoir au moins un membre titulaire du CFE dans leur équipe. Toutefois, les personnes possédant cette expertise ne sont pas suffisamment nombreuses. En conséquence, les organisations recherchent fréquemment cette compétence auprès de prestataires extérieurs.

Scepticisme professionnel

État d'esprit consistant à ne rien tenir pour acquis. Les auditeurs internes remettent constamment en question ce qu'ils entendent et voient, et portent un regard critique sur les preuves d'audit.

Bien que la certification CFE soit une référence essentielle pour les spécialistes de la fraude, d'autres spécialités peuvent s'avérer nécessaires. Par exemple, la compétence CPA/CA peut se révéler très utile lorsque les enquêtes portent sur le reporting financier frauduleux. De plus, les spécialistes de la technologie peuvent être en mesure d'utiliser des techniques d'investigation avancées et se servir d'outils sophistiqués.

Le recours à des spécialistes extérieurs de la lutte contre la fraude présente de nombreux avantages, en plus de l'indépendance que ces intervenants apportent dans le cadre de la mission. Par exemple, ils ont l'habitude d'identifier et d'analyser divers cas de fraude. Ainsi, ils peuvent contribuer à identifier et évaluer les « suspects habituels » et recommander les méthodes d'investigation optimales. En outre, ayant déjà travaillé avec des juristes indépendants, des chefs du contentieux, des procureurs, des autorités de régulation et de supervision, des représentants de l'ordre public, d'autres comptables et auditeurs, ainsi que des substituts du procureur général, ils savent :

- quelle est la meilleure approche à adopter pour enquêter sur une fraude donnée ;
- évaluer la qualité et la quantité des preuves nécessaires ;

Copyright © 2015 Eyrolles.

- évaluer l'admissibilité des preuves en concertation avec des juristes extérieurs ;
- préserver les preuves et la chaîne de conservation des pièces à conviction ;
- s'il est nécessaire, rechercher un témoin, factuel ou expert, ou agir en tant que tel.

Il est très important que les auditeurs internes mènent les enquêtes de manière équitable et consciencieuse, et qu'ils élaborent et tiennent à jour les documents nécessaires pour soutenir toute action résultant de l'enquête. Le recours à des spécialistes est une pratique courante pour faire en sorte que les objectifs soient atteints.

Communication des résultats d'un audit portant sur une fraude

Lors de l'élaboration du rapport sur les résultats des audits ou des investigations portant sur des cas de fraude, nombre des principes énoncés dans le chapitre 14, *La communication des résultats d'une mission d'assurance et les procédures de suivi,* s'appliquent. Par exemple, les auditeurs internes doivent s'efforcer d'identifier les critères, les conditions, les causes et les effets afin de résumer leurs constats à l'issue d'une enquête pour fraude. Ils doivent veiller à rédiger leurs constats de manière systématique et structurée afin d'en renforcer la clarté et d'en faciliter la compréhension, ce qui nécessite généralement :

- un exposé bref et clair des problèmes ;
- l'énumération des politiques, règles, normes, lois et règlements applicables à l'affaire en question ;
- l'analyse des preuves recueillies afin de donner leur opinion en tant que professionnels ;
- les conclusions, c'est-à-dire les constats et les recommandations.

Le rapport gagne ainsi en clarté et en utilité, en particulier s'il est utilisé par le chef du contentieux ou par le juriste extérieur qui conduit l'enquête et peut souhaiter l'intégrer à son propre rapport. Dans tous les cas, les rapports produits par les auditeurs internes ne doivent contenir que des faits, et les auditeurs doivent éviter le plus possible d'y inclure des opinions personnelles ou tout type de préjugé ou hypothèse susceptibles de fausser l'analyse. Ils ne doivent jamais chercher à faire porter la culpabilité sur un ou plusieurs collaborateurs en particulier, mais simplement indiquer que les preuves recueillies semblent corroborer la conclusion selon laquelle une fraude a pu être commise. C'est au tribunal, et non à l'auditeur interne, d'établir la culpabilité et de déterminer la sanction.

***Certified Fraud Examiners* (CFE)**

Personnes qui ont obtenu le titre de CFE et sont spécialisées dans les enquêtes d'expertise et dans les conseils sur les risques de fraude et autres questions relatives à la fraude.

Copyright © 2015 Eyrolles.

OPPORTUNITÉS POUR UN POINT DE VUE DE L'AUDIT INTERNE

En matière de prévention et de détection de la fraude et des actes illégaux, l'audit interne peut apporter un point de vue à la direction générale de nombreuses manières. L'encadré 8-13 présente 10 opportunités pour l'audit interne d'apporter son point de vue.

ENCADRÉ 8-13

APPORTER SON POINT DE VUE SUR LES RISQUES DE FRAUDE ET D'ACTES ILLÉGAUX 10 OPPORTUNITÉS POUR L'AUDIT INTERNE

- Aider l'organisation à développer une évaluation globale du risque de fraude.
- Développer des processus de détection de la fraude en amont.
- Développer des outils d'analyse des données qui peuvent être utilisés pour détecter la fraude en amont.
- Participer au développement des procédures d'appel pour le dispositif d'alerte éthique.
- Organiser des sessions de sensibilisation au problème de la fraude dans l'ensemble de l'organisation.
- Agir avec fermeté en cas d'événements frauduleux importants.
- Participer à l'analyse *a posteriori* lors de la survenue d'une fraude.
- Informer le management des actes illégaux potentiels qui sont des risques pour l'organisation.
- Aider le management à développer une culture favorisant un comportement éthique et une intolérance envers la fraude.
- Se tenir au courant et informer le management des problématiques nouvelles et émergentes autour de la conformité et des réglementations.

RÉSUMÉ

La fraude constitue une préoccupation majeure dans toutes les organisations. La sensibilisation croissante au problème de la fraude dans le monde entier pousse les autorités de régulation et de supervision des différents pays à s'intéresser aux responsabilités du management en matière de prévention, de dissuasion et de détection de la fraude. Les comités d'audit cherchent de plus en plus l'appui de l'audit interne pour contribuer à l'adéquation de la conception et au fonctionnement effectif des programmes de gestion du risque de fraude et des contrôles y afférents.

Pour être efficace, un programme de gestion du risque de fraude doit comporter certains éléments. Premièrement, une bonne gouvernance doit être en place, à la fois directement dans le cadre de ce programme et globalement au sein de l'organisation.

Copyright © 2015 Eyrolles.

Deuxièmement, il convient d'effectuer une évaluation complète du risque de fraude, comportant l'identification des scénarios de fraude possibles, l'évaluation de l'impact et de la probabilité de ces scénarios, ainsi que les décisions concernant le type de solution qu'il convient d'apporter à ces scénarios. Troisièmement, il faut concevoir et instaurer des contrôles efficaces. Il faut trouver le bon équilibre entre contrôles préventifs (afin d'éviter la survenue d'une fraude et de dissuader les fraudeurs potentiels d'envisager de commettre un acte frauduleux) et contrôles détectifs (qui garantissent une détection rapide des fraudes). Enfin, il faut établir un processus visant à faciliter la remontée des incidents de fraudes, l'investigation de ces dernières et la mise en œuvre de mesures disciplinaires et correctives.

L'audit interne joue un rôle essentiel dans la promotion et le soutien du programme de gestion du risque de fraude d'une organisation. Les *Normes* demandent aux auditeurs internes de tenir compte du risque de fraude dans la plupart de leurs activités. En conséquence, les auditeurs internes peuvent soutenir tous les éléments d'un programme efficace de gestion du risque de fraude. La compréhension des caractéristiques comportementales des fraudeurs potentiels aide les auditeurs internes à rester à l'affût des situations dans lesquelles une fraude a le plus de risques de survenir. Cette vigilance, associée à un scepticisme professionnel renforcé, peut aider les auditeurs internes à prévenir ou à dissuader des fraudes potentielles et à déceler rapidement les incidents qui sont survenus. Enfin, si les compétences que possèdent la plupart des auditeurs internes sont de grande valeur, il est important que le responsable de l'audit interne ait conscience de la nécessité de faire appel à des spécialistes de la lutte contre la fraude, tels que les *Certified Fraud Examiners*, et utilise une technologie spécialisée pour permettre à l'audit interne de s'acquitter encore mieux de ses responsabilités en matière de lutte contre la fraude.

Les actes illégaux sont particulièrement problématiques pour les organisations qui appartiennent à des domaines fortement réglementés comme les services financiers, la santé et le secteur public. Les auditeurs internes sont de plus en plus souvent investis de responsabilités en matière de conformité, et dans ce cas, il n'est pas rare qu'ils doivent rendre compte au chef du contentieux. L'augmentation du nombre de procédures liées au FCPA aux États-Unis, la loi britannique anti-corruption de 2010 et les mesures de lutte contre le blanchiment d'argent ont mis l'accent sur le respect des lois et règlements applicables. Néanmoins, il est important de savoir que les activités illégales, frauduleuses, ou contraires à la déontologie ou la morale, ne font pas toutes référence aux mêmes aspects.

Copyright © 2015 Eyrolles.

Questions de révision

1. D'après le rapport de l'ACFE, quel pourcentage de leur chiffre d'affaires la fraude fait-elle perdre aux organisations ? Sur la base du PIB mondial de 2011, combien la fraude a-t-elle coûté ?

2. Quelle est la définition de la fraude donnée par le *Fraud Guide* ?

3. Selon l'AICPA, quelles sont les trois méthodes permettant de réaliser un reporting financier financier ?

4. Selon l'ACFE, quels sont les quatre éléments qui caractérisent une fraude en entreprise ?

5. Quels sont les trois éléments que l'on peut qualifier de « causes à l'origine de la fraude » (qui sont toujours présents, quel que soit le type de fraude) ?

6. Quels sont les cinq grands principes de gestion du risque de fraude selon le *Fraud Guide* ?

7. Citez quelques exemples de pratiques de gouvernance pertinentes.

8. Dans un programme de gestion du risque de fraude, quels rôles et responsabilités devraient avoir chacun des groupes suivants ?
   a. Le Conseil.
   b. La direction générale.
   c. Les collaborateurs.
   d. La fonction d'audit interne.

9. Selon le *Fraud Guide*, quels sont les dix éléments que comporte généralement un programme efficace de gestion du risque de fraude ?

10. Quelles sont les trois principales étapes d'une évaluation du risque de fraude ?

11. Quels éléments convient-il de prendre en compte pour couvrir tous les cas de risques de fraude possibles ?

12. Quels sont les principaux éléments à prendre en compte lors de l'évaluation des risques de fraude ?

13. Quelles sont les modalités possibles de traitement du risque de fraude ?

14. Pourquoi les auditeurs internes doivent-ils connaître le FCPA ?

Copyright © 2015 Eyrolles.

Questions de révision



15. Selon le *Fraud Guide*, quelles méthodes une organisation emploie-t-elle pour :
    a. prévenir la fraude ?
    b. détecter la fraude ?

16. Quelles étapes comporte la phase finale d'un programme efficace de gestion du risque de fraude ?

17. D'après Thomas Golden, quels sont les deux profils de fraudeurs qui manipulent les informations financières ?

18. Quelles *Normes* de l'IIA donnent des orientations spécifiques à l'intention des auditeurs internes concernant leurs responsabilités en matière de fraude ?

19. Définissez le « scepticisme professionnel ».

20. Comment des spécialistes de la lutte contre la fraude, tels que les *Certified Fraud Examiners*, pourraient-ils aider la fonction d'audit interne à combattre la fraude ?

21. Quels éléments les auditeurs internes devraient-ils inclure dans leurs communications d'audit portant sur la fraude ? Quels éléments devraient-ils au contraire laisser de côté ?

Copyright © 2015 Eyrolles.

Questions à choix multiples

Sélectionnez la meilleure réponse pour chacune des questions suivantes.

1. La « suspicion de fraude » est un terme technique qui désigne :
   a. La capacité des auditeurs internes à anticiper la fraude.
   b. La capacité des auditeurs internes à lancer une enquête s'il existe des éléments indiquant l'existence d'une fraude et la probabilité qu'elle soit toujours en cours.
   c. Les activités des fraudeurs qui effacent leurs traces de manière à dissimuler leurs agissements et à ne pas être découverts.
   d. L'analyse par le management des risques de fraude afin qu'il puisse mettre en place des programmes et des contrôles antifraude.

2. Quelles sortes de fraude ont été les plus courantes en 2012 selon le rapport de l'ACFE ?
   a. La corruption.
   b. La fraude comptable.
   c. Le détournement de biens par les collaborateurs.
   d. La comptabilisation inappropriée du chiffre d'affaires dans les résultats financiers publiés.

3. Parmi les propositions suivantes, laquelle ne constitue pas une « justification » classiquement invoquée par un fraudeur ?
   a. C'est dans l'intérêt de l'organisation.
   b. L'organisation me doit de l'argent car je suis sous-payé.
   c. J'en veux à mon chef (désir de revanche).
   d. Je suis plus intelligent que les autres.

4. Laquelle des activités suivantes est réservée à des personnes dédiées dans l'organisation ?
   a. Comprendre le rôle qui leur est dévolu dans le cadre du contrôle interne.
   b. Comprendre les fondamentaux de la fraude et savoir reconnaître les signaux d'alerte.
   c. Faire part d'éventuels soupçons de fraude.
   d. Enquêter sur des activités suspectes dont ils pensent qu'elles sont frauduleuses.

Copyright © 2015 Eyrolles.

Questions à choix multiples

5. Une organisation qui fabrique et vend des ordinateurs souhaite augmenter son chiffre d'affaires d'ici la fin de l'année. Elle décide de verser à ses commerciaux une prime dépendant du nombre d'unités qu'ils vont vendre aux clients d'ici la fin de l'année. Le prix de tous les ordinateurs est déterminé par le directeur adjoint des ventes, et ne peut pas être modifié par les commerciaux. Parmi les opportunités suivantes, laquelle peut inciter un commercial à commettre une fraude ?
   a. Le commercial peut vendre des unités dont la marge est inférieure à celle d'autres unités.
   b. Les clients ont le droit de ramener leur ordinateur portable pendant les 90 jours qui suivent l'achat.
   c. Les unités vendues peuvent être défectueuses.
   d. Les clients peuvent ne pas payer leur ordinateur en temps opportun.

6. Comment une organisation doit-elle traiter une accusation anonyme émanant d'un collaborateur, qui affirme que l'un des superviseurs de l'organisation manipule les relevés du temps de travail ?
   a. Demander à un auditeur interne d'examiner tous les relevés du temps de travail des six derniers mois dans le secteur où travaille le superviseur en question.
   b. Prendre note de l'accusation mais ne rien faire, même si l'accusation est étayée par des preuves factuelles.
   c. Comparer les faits révélés par le collaborateur anonyme aux critères préétablis afin de déterminer si une enquête formelle est nécessaire.
   d. Transférer le dossier au service des ressources humaines car les accusations anonymes relèvent généralement des ressources humaines.

7. Parmi les propositions suivantes, laquelle constitue un détournement d'actifs ?
   a. Une petite somme en liquide est volée.
   b. Une entrée du journal des comptes est modifiée afin d'améliorer les résultats financiers publiés.
   c. Le directeur de l'exploitation soudoie un fonctionnaire étranger afin de faciliter l'autorisation de commercialisation d'un nouveau produit.
   d. Un double d'une facture est envoyé à un client dans l'espoir qu'il la paiera deux fois.

8. Parmi les exemples suivants, lequel n'entre pas dans le cadre d'un programme de prévention de la fraude ?
   a. Les enquêtes sur les antécédents des nouveaux collaborateurs.
   b. Les entretiens de départ des collaborateurs qui quittent l'organisation.
   c. L'établissement de limites d'autorisation pour les engagements d'achat.
   d. L'analyse des décaissements afin de déterminer si des paiements en double ont été effectués.

Copyright © 2015 Eyrolles.

9. Laquelle des organisations suivantes aurait le plus probablement besoin de contrôles antifraude renforcés ?
   a. Un fabricant de chaussures de sport populaires.
   b. Un supermarché.
   c. Une banque.
   d. Un vendeur de matériel électronique en ligne.

10. Un agent du service de la paye a augmenté le taux de salaire horaire d'un de ses amis et partagé avec celui-ci les sommes qui en résultent. Parmi les contrôles suivants, lequel serait le plus efficace pour prévenir cette fraude ?
    a. Exiger que tous les changements apportés aux registres de paye soient enregistrés sur un formulaire standard.
    b. Autoriser uniquement les superviseurs habilités du service des ressources humaines à procéder à des changements dans les informations portant sur le système de rémunération des collaborateurs.
    c. Rapprocher périodiquement les taux de rémunération des fichiers du personnel avec ceux du système de rémunération.
    d. Demander aux superviseurs des différents services d'effectuer une surveillance des coûts de rémunération sur une base mensuelle.

11. Les responsabilités de la fonction d'audit interne vis-à-vis de la fraude sont limitées :
    a. Aux seules activités opérationnelles et de conformité de l'organisation, car les questions relatives au reporting financier relèvent de l'auditeur externe.
    b. À la surveillance de tous les appels reçus *via* le dispositif d'alerte de l'organisation, mais pas nécessairement à la conduite d'une enquête de suivi.
    c. À la surveillance des indicateurs de fraude, y compris ceux qui sont liés à la fraude dans le reporting financier, mais sans posséder nécessairement l'expertise d'un spécialiste des enquêtes sur les fraudes.
    d. À l'assurance que tous les collaborateurs ont été suffisamment sensibilisés au problème de la fraude.

12. Du point de vue d'une organisation, étant donné que les auditeurs internes sont considérés comme des « experts du contrôle interne », ils sont également :
    a. La première et plus importante ligne de maîtrise contre le reporting financier frauduleux ou les détournements d'actifs.
    b. La meilleure ressource à consulter en interne par les comités d'audit, la direction générale et d'autres parties prenantes lorsqu'ils mettent en place des programmes et contrôles antifraude, même si les auditeurs n'ont aucune expérience en matière d'investigation des fraudes.
    c. Les personnes les mieux à même d'enquêter sur un cas de fraude impliquant une violation potentielle des lois et règlements.
    d. Le principal décideur lorsqu'il s'agit de déterminer la sanction ou d'autres conséquences pour les fraudeurs.

Copyright © 2015 Eyrolles.

Thèmes de discussion

1. Pourquoi la situation au sein de l'organisation, les compétences et l'objectivité de la fonction d'audit interne sont-elles particulièrement importantes en cas de fraude commise par la direction générale ? Pourquoi le rattachement hiérarchique direct du responsable de l'audit interne au directeur financier, au directeur général, au chef du contentieux ou au contrôleur de gestion peut-il se révéler plus problématique que le rattachement hiérarchique au comité d'audit (ou à son équivalent) ?

2. L'Open Compliance and Ethics Group (OCEG) a publié un guide à l'intention des auditeurs internes pour les aider à réaliser des audits de conformité et de respect de la déontologie (ce guide est disponible sur le site www.oceg.org). Comment l'exemplarité au plus haut niveau de l'organisation, une sensibilisation au contrôle et une culture d'intégrité et de déontologie au sein des organisations contribuent-elles à prévenir, dissuader et détecter la fraude ? Est-il suffisant que les organisations dissuadent effectivement les activités illégales, contraires à la déontologie ou la morale, et si ces activités sont constatées, qu'ils fassent en sorte que le dispositif d'alerte soit utilisé pour dénoncer ces conduites répréhensibles qui pourraient annoncer une fraude ?

3. La fraude revêt les formes les plus diverses, c'est pourquoi il existe autant de termes plus ou moins apparentés pour la décrire. Prenez soin d'examiner les termes suivants et expliquez-en la signification et en quoi ils se distinguent les uns des autres :
   - pots-de-vin et dessous-de-table ;
   - conflit d'intérêts ;
   - maquillage des comptes ;
   - opération pour le compte de son auteur et corruption ;
   - détournement de fonds ;
   - recettes ou charges fictives ;
   - usurpation d'identité ;
   - espionnage industriel ;
   - violation intentionnelle des principes comptables généralement reconnus ;
   - détournement par virement bancaire ;
   - fraude par report différé ;
   - vol qualifié ;
   - manquement à des obligations fiduciaires ;
   - présentation mensongère de faits matériels ;
   - blanchiment d'argent ;
   - conspiration ;
   - entités fictives ;
   - opérations circulaires ;
   - falsification ;

Copyright © 2015 Eyrolles.

- fausses notes de frais ;
- vol de secrets commerciaux ;
- écritures de journal directement effectuées sur le grand livre ;
- collusion des soumissionnaires ;
- fixation concertée des prix ;
- accords parallèles occultes ;
- collaborateurs fictifs ;
- modification de la date d'exercice des stock-options, attribution de stock-options pendant des périodes interdites (*spring loading* ou *bullet dodging*) ;
- transactions hors-bilan illégitimes ;
- fausses réclamations ;
- habillage du bilan ;
- remplissage des canaux de distribution (*channel stuffing*) ;
- délit d'initié.

4. Quels sont les indicateurs du risque de fraude que les auditeurs internes doivent surveiller en général ? Comment ces « signaux d'alerte » (facteurs de risque de fraude) sont-ils influencés par le secteur d'activité et l'implantation géographique d'une organisation ? Pourquoi certains domaines et actifs semblent-ils plus touchés par la fraude ? Quelles considérations de « risque relatif » doivent être prises en compte ? Élargissez ces considérations à l'importance relative (l'importance de réaliser des objectifs organisationnels) et au caractère approprié et suffisant des preuves.

5. Comment la fonction d'audit interne peut-elle aider le comité d'audit en l'alertant rapidement lorsque le management contourne le contrôle interne ?

6. Les auditeurs internes peuvent-ils participer aux enquêtes d'expertise et, si oui, comment ?

7. On peut demander aux auditeurs internes d'effectuer une enquête pour fraude impliquant une action en justice. Est-il important d'envisager de mener cette enquête dans le cadre du secret professionnel ? Expliquez votre réponse.

Copyright © 2015 Eyrolles.

CAS N° 1

« Fannie Mae Ex-Officials May Face Legal Action Over Accounting » (*The Wall Street Journal*, 24 mai 2006, pp. A1 et A11).

James B. Lockhart, directeur par interim de l'Office fédéral de vérification des constructeurs de logements (OFHEO), le principal régulateur de l'organisation Fannie Mae, a dénoncé ce qu'il appelait « une culture d'entreprise pleine d'arrogance et contraire à l'éthique » chez le deuxième plus grand prêteur américain après le gouvernement fédéral. Plus précisément, le rapport de 340 pages de l'OFHEO reprochait au Conseil et à la Direction générale d'avoir instauré une culture d'entreprise autorisant les managers à négliger les normes comptables lorsque celles-ci les empêchaient d'atteindre leurs objectifs de bénéfices. Selon le rapport, l'organisation récompensait par la suite les dirigeants pour avoir atteint ces objectifs, en leur versant des primes conséquentes.

Concernant l'audit interne, le rapport de l'OFHEO citait un discours de Sam Rogers*, ancien responsable du service d'audit de Fannie Mae, qui aurait déclaré aux auditeurs internes qu'ils avaient « l'obligation morale » de tout faire pour atteindre l'objectif fixé en 1999 par Frank Raines (alors PDG de Fannie Mae) de doubler le bénéfice par action et d'atteindre 6,46 par action en 2003. « À partir de maintenant, le chiffre de 6,46 doit rester gravé dans vos têtes, aurait-t-il déclaré. Vous devez brûler d'un feu intérieur qui consume tous les doutes. Vous devez vivre, respirer (*sic*), rêver 6,46… Après tout, grâce à Frank [Raines], il y a beaucoup d'argent à la clé [sous forme de primes] ». Compte tenu de la responsabilité qui incombait à M. Rogers en matière de conformité vis-à-vis des règles comptables, ces remarques étaient « inappropriées », estime l'OFHEO.

Quel(s) problème(s) cette situation pose-t-elle ? M. Rogers a-t-il potentiellement enfreint le Code de déontologie et les *Normes* de l'IIA en faisant de telles remarques ? Étoffez votre réponse en analysant son statut, son indépendance et son objectivité en tant que responsable de l'audit interne de Fannie Mae au moment des faits, et expliquez en quoi il peut exister un conflit lorsque les auditeurs internes reçoivent des stock-options et des primes liées aux performances financières.

*Le nom a été modifié.

Copyright © 2015 Eyrolles.

ÉTUDES DE CAS

CAS N° 2

Actuellement, plusieurs affaires de fraude sont instruites par les tribunaux et les enquêtes *a posteriori* se terminent. Vous en avez appris beaucoup sur l'identification du risque de fraude, sur les activités de contrôle qui permettent de maîtriser ce risque, ainsi que sur l'importance de la déontologie et de la conformité au sein de l'organisation. Vous devez à présent être en mesure de comprendre que l'incidence de la fraude est plus courante qu'on ne le pensait auparavant, et qu'il existe de nombreuses techniques, méthodes et motivations pour commettre une fraude. Vous devez également avoir compris que la découverte d'une fraude trahit peut-être d'autres problèmes (par exemple, lorsque le management ne fait pas preuve d'intégrité, un retraitement des états financiers peut indiquer que les commissaires aux comptes et/ou l'auditeur interne ont réussi à déjouer une tentative de fraude). C'est pourquoi la réglementation a été considérablement renforcée, comme cela s'est déjà produit lors de périodes similaires de l'histoire.

Votre projet de groupe est stratégique et traite de la manière dont les auditeurs internes peuvent aborder les cas de fraude, ainsi que des conséquences de certaines lois actuelles, comme le *Sarbanes-Oxley Act* de 2002 aux États-Unis. La première partie de cette étude de cas consiste à citer trois cas similaires. Votre tâche consiste à rechercher la cause à l'origine de chaque fraude et à identifier les techniques qui auraient pu en empêcher la survenue, ou au moins la déceler rapidement.

Faites une présentation PowerPoint en groupe. Cette présentation comportera deux ou trois diapositives pour chaque cas de fraude. Elles résumeront l'affaire, les pertes approximatives essuyées, les parties impliquées dans la fraude, la cause à l'origine de la fraude et les actions correctives qui ont été entreprises depuis. Veuillez aussi indiquer si les réglementations actuelles suffiront à éviter que des fraudes analogues ne soient perpétrées à l'avenir. De plus, décrivez les actions correctives que votre groupe recommanderait pour prévenir ou détecter rapidement ce type de fraude. Sur une diapositive distincte, comparez les causes des trois affaires que vous étudiez. Enfin, sur la dernière diapositive, résumez ce que votre groupe a appris en réalisant cette étude de cas.

Copyright © 2015 Eyrolles.

NOTES

Copyright © 2015 Eyrolles.



Copyright © 2015 Eyrolles.



CHAPITRE 9
LA GESTION DE L'AUDIT INTERNE

Objectifs pédagogiques

- Comprendre l'importance d'un positionnement adéquat de la fonction d'audit interne au sein de l'organisation.
- Déterminer les avantages de diverses structures organisationnelles pour l'audit interne.
- Déterminer les rôles et responsabilités des principaux postes au sein de l'audit interne.
- Comprendre les règles et procédures de l'audit interne et la manière dont elles guident la fonction d'audit interne.
- Comprendre les caractéristiques d'un modèle (processus) de gestion des risques bien exécuté et réfléchir au rôle que doit jouer l'audit interne dans les processus de gestion des risques de l'organisation.
- Comprendre l'assurance-qualité, son mode de fonctionnement et les raisons pour lesquelles elle est importante pour l'audit interne.
- Comprendre le rôle de l'informatique dans la gestion de l'audit interne.

Vous devez à présent être sensibilisé à l'importance et à la complexité d'une fonction d'audit interne, et être conscient du rôle critique qu'elle peut jouer dans la réussite de l'ensemble de l'organisation grâce aux activités d'assurance qu'elle réalise pour appuyer la structure de gouvernance de l'organisation. Dans ce chapitre, nous traitons les composantes du management de la fonction d'audit interne. Lorsque cela est possible, nous présentons l'éventail des méthodes utilisées par différentes fonctions d'audit interne, et les avantages de chacune. Nous commençons par décrire les différentes structures organisationnelles possibles pour une fonction d'audit interne, notamment sa place au sein de l'organisation. Nous identifions ensuite les postes clés au sein de cette fonction, notamment celui de responsable de l'audit interne, et mettons l'accent sur les rôles et responsabilités de chacun. Nous abordons les règles et procédures et la façon dont elles apportent l'orientation et la structure nécessaires à la fonction d'audit interne. Nous examinons différents modèles de gestion des risques et étudions le rôle que l'audit interne peut et doit jouer dans les processus de gestion des risques et de gouvernance mis en place par l'organisation. Nous expliquons ensuite la notion d'assurance-qualité et son importance pour l'audit interne. Nous terminons en mentionnant plusieurs outils technologiques auxquels peut recourir l'audit interne et la manière dont ils sont utilisés dans la gestion de la fonction.

Copyright © 2015 Eyrolles.

ENCADRÉ 9-1

DISPOSITIONS DU CRIPP PERTINENTES RELATIVES AU CHAPITRE 9

Norme 1000 – Mission, pouvoirs et responsabilités
Norme 1010 – Reconnaissance de la définition de l'audit interne, du Code de déontologie ainsi que des Normes dans la charte d'audit interne
Norme 1100 – Indépendance et objectivité
Norme 1110 – Indépendance dans l'organisation
Norme 1111 – Relation directe avec le Conseil
Norme 1120 – Objectivité individuelle
Norme 1130 – Atteinte à l'indépendance ou à l'objectivité
Norme 1200 – Compétence et conscience professionnelle
Norme 1210 – Compétence
Norme 1220 – Conscience professionnelle
Norme 1230 – Formation professionnelle continue
Norme 1300 – Programme d'assurance et d'amélioration qualité
Norme 1310 – Exigences du programme d'assurance et d'amélioration qualité
Norme 1311 – Évaluations internes
Norme 1312 – Évaluations externes
Norme 1320 – Rapports relatifs au programme d'assurance et d'amélioration qualité
Norme 1321 – Utilisation de la mention « conforme aux Normes internationales pour la pratique professionnelle de l'audit interne »
Norme 2000 – Gestion de l'audit interne
Norme 2010 – Planification
Norme 2020 – Communication et approbation
Norme 2030 – Gestion des ressources
Norme 2040 – Règles et procédures
Norme 2050 – Coordination
Norme 2060 – Rapports à la direction générale et au Conseil
Norme 2100 – Nature du travail
Norme 2110 – Gouvernement d'entreprise
Norme 2120 – Management des risques
Norme 2130 – Contrôle

Modalité Pratique d'Application 1000-1 : Charte d'audit interne
Modalité Pratique d'Application 1110-1 : Indépendance dans l'organisation
Modalité Pratique d'Application 1111-1 : Relation avec le Conseil
Modalité Pratique d'Application 1120-1 : Objectivité individuelle
Modalité Pratique d'Application 1130-1 : Atteintes à l'indépendance ou à l'objectivité
Modalité Pratique d'Application 1130.A1-1 : Audit des opérations dont les auditeurs internes ont été auparavant responsables
Modalité Pratique d'Application 1130.A2-1 : Responsabilités exercées par l'audit interne au titre d'autres fonctions
Modalité Pratique d'Application 1200-1 : Compétence et conscience professionnelle
Modalité Pratique d'Application 1210-1 : Compétence
Modalité Pratique d'Application 1210.A1-1 : Recours à des prestataires externes
Modalité Pratique d'Application 1220-1 : Conscience professionnelle
Modalité Pratique d'Application 1230-1 : Formation Professionnelle Continue
Modalité Pratique d'Application 1300-1 : Programme d'assurance et d'amélioration qualité

Copyright © 2015 Eyrolles.

Modalité Pratique d'Application 1310-1 :	Exigences du programme d'assurance et d'amélioration qualité
Modalité Pratique d'Application 1311-1 :	Évaluations internes
Modalité Pratique d'Application 1312-1 :	Évaluations externes
Modalité Pratique d'Application 1312-2 :	Évaluations externes : auto-évaluation avec validation indépendante
Modalité Pratique d'Application 1312-3 :	Indépendance de l'équipe d'évaluation externe dans le secteur privé
Modalité Pratique d'Application 1312-4 :	Indépendance de l'équipe d'évaluation externe dans le secteur public
Modalité Pratique d'Application 2010-1 :	La prise en compte des risques et des menaces pour l'élaboration du plan d'audit
Modalité Pratique d'Application 2020-1 :	Communication et approbation
Modalité Pratique d'Application 2030-1 :	Gestion des ressources
Modalité Pratique d'Application 2040-1 :	Règles et procédures
Modalité Pratique d'Application 2050-1 :	Coordination
Modalité Pratique d'Application 2050-2 :	Cartographie des services donnant une assurance sur les dispositifs de contrôle et de management des risques
Modalité Pratique d'Application 2050-3 :	S'appuyer sur les travaux d'autres prestataires de services d'assurance
Modalité Pratique d'Application 2060-1 :	Rapports à la direction générale et au Conseil

Prise de position : Prise de position de l'IIA sur les ressources de l'audit interne
Guide pratique : Élaborer le plan stratégique de l'audit interne
Guide pratique : *Integrated Auditing*
Guide pratique : Programme d'assurance et d'amélioration de la qualité
Guide pratique : *Coordinating Risk Management and Assurance*

Commentaire du traducteur

La profession de l'audit interne évolue continuellement. Le lecteur est donc invité à se référer au site Internet de l'IIA pour prendre connaissance des évolutions du Cadre de référence international des pratiques professionnelles de l'audit interne (CRIPP).

QUELLE PLACE POUR L'AUDIT INTERNE AU SEIN DE L'ORGANISATION ?

On trouve un large éventail d'opinions concernant la place que peut et doit occuper l'audit interne au sein d'une organisation pour satisfaire aux *Normes internationales pour la pratique professionnelle de l'audit interne* (les *Normes*) de l'IIA. À l'une des extrémités de cet éventail, l'audit interne est placé au niveau de la direction générale. Il a ainsi la visibilité, le pouvoir et le devoir :

- d'évaluer, de manière indépendante, le système de contrôle interne de l'organisation ;
- d'évaluer la capacité de cette dernière à atteindre ses objectifs et à gérer, piloter et maîtriser efficacement les risques associés à la réalisation de ses objectifs.

Responsable de l'audit interne

Désigne une personne, occupant un poste hiérarchique de haut niveau, qui a la responsabilité de gérer l'activité d'audit interne. Ce terme recouvre également des titres tels qu'auditeur général, chef de l'audit interne, directeur de l'audit interne ou inspecteur général.

Copyright © 2015 Eyrolles.

Outre les activités d'assurance, le management demande souvent à l'audit interne de réaliser des activités de conseil, sous la forme d'initiatives ou de projets, qui lui permettent d'utiliser les compétences professionnelles de l'audit interne (les activités de conseil sont traitées plus en détail dans le chapitre 15, *La mission de conseil*). À l'autre extrémité de l'éventail se trouvent les organisations qui ne possèdent pas de fonction d'audit interne ou bien qui le placent à un niveau nettement inférieur dans la hiérarchie organisationnelle. Elles lui demandent généralement d'effectuer quotidiennement des activités qui n'ont rien à voir avec l'audit, comme l'assurance-qualité, la conformité, des activités opérationnelles et/ou d'autres activités de traitement des transactions.

Pour se conformer à la définition de l'audit interne proposée par l'IIA, citée dans le chapitre 1, *Introduction à l'audit interne* – « une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée. Il aide cette organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle et de gouvernement d'entreprise, et en faisant des propositions pour renforcer leur efficacité » –, de nombreuses organisations positionnent leur fonction d'audit interne comme une activité relevant de la direction générale et rendant directement compte au Conseil. Les organisations qui continuent de demander à l'audit interne d'effectuer principalement des activités opérationnelles et des activités autres que l'audit, comme mentionné précédemment, l'empêchent de donner à la direction générale une évaluation de la conception et de l'efficacité

ENCADRÉ 9-2

RECOMMANDATIONS POUR L'ÉLABORATION D'UNE CHARTE D'AUDIT INTERNE

MPA 1000-1 – Charte d'audit interne

- L'existence d'une charte d'audit interne formalisée est essentielle pour la gestion du service d'audit interne. La charte est un document officiel soumis pour avis et acceptation à la direction générale, et approuvé par le comité d'audit ou le Conseil. Il précise le rôle du responsable d'audit interne et facilite ainsi l'évaluation périodique de la pertinence de sa mission, de ses pouvoirs et de ses responsabilités. Son approbation est consignée dans les procès-verbaux du Conseil. Il facilite en outre l'évaluation périodique de la pertinence de la mission, des pouvoirs et des responsabilités de l'audit interne, précisant ainsi le rôle de l'audit interne. En cas d'interrogation, la charte est la référence écrite officielle de l'accord passé avec la direction générale et le Conseil sur le rôle et les responsabilités du service d'audit interne de l'organisation.
- Le responsable de l'audit interne évalue périodiquement si la mission, les pouvoirs, et les responsabilités définis dans la charte permettent toujours au service d'audit interne d'atteindre ses objectifs. Il est également chargé de communiquer le résultat de cette évaluation périodique à la direction générale et au Conseil.

Copyright © 2015 Eyrolles.

de la gestion des risques, du contrôle et de la gouvernance, car il ne dispose pas de l'objectivité requise pour évaluer en toute indépendance les opérations de l'organisation et proposer des suggestions d'améliorations impartiales.

Les organisations qui ont compris qu'il était important de placer l'audit interne dans une position qui en maximise l'efficacité et la capacité à évaluer les performances des processus de gestion des risques, de contrôle et de gouvernance existants le font souvent en positionnant le responsable de l'audit interne à un niveau hiérarchique élevé. Selon la Norme 2000, Gestion de l'audit interne, « le responsable de l'audit interne doit gérer efficacement cette activité de façon à garantir qu'elle apporte une valeur ajoutée à l'organisation ». Reconnaissant que la présence d'un responsable de l'audit interne est cruciale pour l'efficacité de l'audit interne, l'interprétation de la Norme 2000 précise ensuite que « l'activité d'audit interne est gérée efficacement quand :

- les résultats des travaux de l'audit interne répondent aux objectifs et responsabilités définis dans la charte d'audit interne ;
- l'audit interne est exercé conformément à la définition de l'audit interne et aux *Normes* ;
- les membres de l'équipe d'audit agissent en respectant le Code de déontologie et les *Normes* ».

Pour que le responsable de l'audit interne puisse s'acquitter des responsabilités décrites ci-dessus, il est indispensable que soit mise en place une charte qui « défini[sse] la position de l'audit interne dans l'organisation y compris la nature de la relation fonctionnelle entre le responsable de l'audit interne et le Conseil ; autorise l'accès aux documents, aux personnes et aux biens, nécessaires à la réalisation des missions ; défini[sse] le champ des activités d'audit interne » (Interprétation de la Norme 1000, Mission, pouvoirs et responsabilités). La charte doit non seulement préciser la mission, les pouvoirs et les responsabilités de l'audit interne, mais aussi tenir compte des activités d'assurance et de conseil. Il est important de comprendre que l'audit interne et le comité d'audit obéissent à des chartes distinctes qui délimitent les obligations spécifiques qu'ils ont chacun vis-à-vis de l'organisation, tout en envisageant les interdépendances entre les deux et en en tenant compte. La charte d'audit interne est subordonnée à celle du comité d'audit. Elle doit l'étayer et non la contredire. L'audit interne complète souvent sa charte par l'exposé de ses conceptions, ainsi que par une stratégie à long terme détaillée pour l'audit interne. Ces informations complémentaires sont souvent incluses dans le plan annuel d'audit interne, aux côtés des budgets opérationnels et de la planification des ressources. Ce plan annuel d'audit est révisé et validé par le comité d'audit. Ces documents distincts et les règles et procédures opérationnelles de l'audit interne sont souvent regroupés dans un ensemble de principes directeurs (généralement appelé « manuel

Charte d'audit interne

Document officiel qui précise la mission, les pouvoirs et les responsabilités de cette activité. La charte d'audit interne est subordonnée à celle du comité d'audit.

Copyright © 2015 Eyrolles.

d'audit ») qui, avec les autres informations relatives à la procédure, guident l'audit interne. L'encadré 9-2 précise les recommandations de l'IIA pour la mise en place d'une charte d'audit interne.

Outre l'établissement d'une charte, l'exposé de conceptions et d'un plan d'audit interne, le responsable de l'audit interne doit établir et maintenir l'indépendance, l'objectivité, la compétence et la conscience professionnelle au sein de la fonction d'audit interne. Comme indiqué précédemment, la place de l'audit interne a une incidence sur sa capacité à conserver son objectivité. S'il est placé à un niveau équivalent à celui de membre de la direction générale et dispose d'un accès direct au comité d'audit, il bénéficiera d'une plus grande indépendance et, par conséquent, d'une plus grande objectivité. Le fait que le comité d'audit participe au choix, à l'évaluation et à la révocation du responsable de l'audit interne accroît encore la capacité de ce dernier à conserver son indépendance au sein de l'organisation et à éviter le plus possible que la direction générale n'exerce une influence indue, qui affecterait sa capacité à agir sans préjugés (objectivité individuelle). Dans l'idéal, le service d'audit interne sera placé assez haut dans la hiérarchie de l'organisation et doté d'un accès direct au comité d'audit, ce qui lui permettra de se conformer aux exigences et aux recommandations de l'IIA telles que détaillées ci-dessous.

Indépendance et objectivité

La Norme 1110, Indépendance dans l'organisation, indique que « le responsable de l'audit interne doit relever d'un niveau hiérarchique suffisant au sein de l'organisation pour permettre au service d'audit interne d'exercer ses responsabilités ». Plus précisément, la Norme 1110.A1 précise que « l'audit interne ne doit subir aucune ingérence lors de la définition de son champ d'intervention, de la réalisation du travail et de la communication des résultats ». La MPA 1110-1, Indépendance dans l'organisation, donne des indications plus détaillées, soulignant combien il est important que la direction générale et le Conseil soutiennent l'audit interne, ce qui l'aidera à obtenir la coopération des audités et à exercer son activité sans entrave.

La Norme 1120, Objectivité individuelle, énonce que « les auditeurs internes doivent avoir une attitude impartiale et dépourvue de préjugés, et éviter tout conflit d'intérêt ». L'IIA détaille ces exigences dans la MPA 1120-1, Objectivité individuelle.

- « L'objectivité individuelle nécessite que les auditeurs internes réalisent leurs missions de telle manière qu'ils aient sincèrement confiance dans le résultat de leur travail et dans le fait qu'aucune concession significative n'ait été faite en matière de qualité. Les auditeurs internes ne doivent pas se trouver placés dans des situations qui porteraient atteinte à leur capacité à porter des jugements professionnels objectifs.

Objectivité individuelle

Attitude impartiale qui permet aux auditeurs internes d'accomplir leurs missions de telle sorte qu'ils soient certains de la qualité de leurs travaux, menés sans compromis. L'objectivité implique que les auditeurs internes ne subordonnent pas leur propre jugement à celui d'autres personnes.

Indépendance dans l'organisation

Caractéristique du niveau hiérarchique dont relève le responsable de l'audit interne au sein de l'organisation, et qui permet à l'audit interne d'exercer ses responsabilités sans subir la moindre ingérence.

Copyright © 2015 Eyrolles.

- L'objectivité individuelle nécessite que le responsable de l'audit interne organise une affectation des auditeurs de manière à prévenir les conflits d'intérêts potentiels ou réels ainsi que les partis pris. Il s'informe périodiquement auprès des auditeurs à propos des conflits d'intérêts ou des partis pris et, le cas échéant, instaure une rotation régulière des auditeurs internes au sein de l'équipe.
- La revue des résultats de l'audit avant leur diffusion permet de fournir une assurance raisonnable que le travail a été réalisé avec objectivité.
- L'objectivité de l'auditeur interne n'est pas compromise lorsqu'il est amené à recommander la mise en place de normes de contrôle pour les systèmes d'information ou à examiner des procédures avant leur mise en application. Par contre, son objectivité est présumée altérée s'il conçoit, met en place, rédige les procédures y relatives ou exploite de tels systèmes.
- L'exécution ponctuelle par les auditeurs internes de travaux qui ne sont pas des travaux d'audit ne compromet pas nécessairement leur indépendance dans la mesure où ils sont clairement mentionnés dans le rapport d'audit. Toutefois, le management et les auditeurs internes doivent veiller attentivement à ce que ces travaux n'altèrent pas leur objectivité. »

Comme l'indique la Norme 1130, Atteinte à l'indépendance ou à l'objectivité :

> *« Si l'indépendance ou l'objectivité des auditeurs internes sont compromises dans les faits ou même en apparence, les parties concernées doivent en être informées de manière précise. La forme de cette communication dépendra de la nature de l'atteinte à l'indépendance. »*
>
> *Interprétation :*
>
> *« Parmi les atteintes à l'indépendance du service d'audit interne et à l'objectivité individuelle, peuvent figurer les conflits d'intérêts personnels, les limitations du champ d'un audit, les restrictions d'accès aux dossiers, aux personnes et aux biens, ainsi que les limitations de ressources telles que des limitations financières.*

L'identification des parties qui devraient être informées d'une atteinte à l'objectivité et à l'indépendance dépend d'une part des attentes de la direction générale et du Conseil, telles que décrites dans la charte d'audit interne, en termes de responsabilités de l'audit interne et du responsable d'audit interne, et d'autre part de la nature de cette atteinte. »

Si une atteinte à l'indépendance ou à l'objectivité est identifiée, l'auditeur interne doit faire état de cette atteinte (réelle ou perçue)

Copyright © 2015 Eyrolles.

ENCADRÉ 9-3

ATTEINTES À L'INDÉPENDANCE ET À L'OBJECTIVITÉ : LES EXIGENCES DE L'IIA

Norme 1130.A1

Les auditeurs internes doivent s'abstenir d'auditer des opérations particulières dont ils étaient auparavant responsables. L'objectivité d'un auditeur interne est présumée altérée lorsqu'il réalise une mission d'assurance pour une activité dont il a eu la responsabilité au cours de l'année précédente.

Norme 1130.A2

Les missions d'assurance concernant des fonctions dont le responsable de l'audit a la charge doivent être supervisées par une personne ne relevant pas de l'audit interne.

Norme 1130.C1

Les auditeurs internes peuvent être amenés à réaliser des missions de conseil liées à des opérations dont ils ont été auparavant responsables.

Norme 1130.C2

Si l'indépendance ou l'objectivité des auditeurs internes sont susceptibles d'être compromises lors des missions de conseil qui leur sont proposées, ils doivent en informer le client donneur d'ordre avant de les accepter.

au responsable de l'audit interne, à qui il revient de décider s'il faut réaffecter l'auditeur interne. Lorsque cette atteinte résulte d'une limitation du champ d'intervention, définie dans la MPA 1130-1, Atteintes à l'indépendance ou à l'objectivité, comme « une restriction imposée à l'audit interne l'empêchant de réaliser ses objectifs et son planning », le responsable de l'audit interne doit communiquer au Conseil, de préférence par écrit, l'existence d'une limitation du champ d'intervention et ses répercussions possibles. En outre, afin d'éviter toute possibilité d'atteinte (réelle ou perçue), « les auditeurs internes ne doivent pas accepter une rémunération, des cadeaux ou des invitations de la part d'un salarié, d'un client, d'un fournisseur ou d'un partenaire » (MPA 1130-1).

L'encadré 9-3 présente d'autres exigences de l'IIA concernant les atteintes à l'indépendance ou à l'objectivité.

L'audit interne coordonne souvent ses travaux avec d'autres services de l'organisation qui ont des objectifs et des responsabilités analogues en matière de maîtrise des risques, comme les services de conformité et de gestion des risques. Tant que l'on ne demande pas à l'audit interne d'effectuer des activités opérationnelles ou de concevoir des processus et procédures qu'il devra ensuite évaluer dans le cadre de ses missions d'audit interne, son indépendance et son objectivité ne sont pas menacées. Ce type de coordination peut apporter une valeur ajoutée significative à l'organisation et promouvoir une utilisation efficiente des ressources dans les efforts de maîtrise des risques déployés par l'organisation. De même, l'audit interne peut identifier les possibilités de coordination des travaux d'assurance entre les différents services de l'organisation, sans que

Copyright © 2015 Eyrolles.

son indépendance et son objectivité ne soient menacées. La coordination des travaux d'assurance est détaillée plus loin dans ce chapitre.

Compétence et conscience professionnelle

La Norme 1200, Compétence et conscience professionnelle, énonce simplement que « les missions doivent être conduites avec compétence et conscience professionnelle ». La Norme 1210, Compétence, va plus dans le détail et précise que « les auditeurs internes doivent posséder les connaissances, le savoir-faire et les autres compétences nécessaires à l'exercice de leurs responsabilités individuelles. L'équipe d'audit interne doit collectivement posséder ou acquérir les connaissances, le savoir-faire et les autres compétences nécessaires à l'exercice de ses responsabilités ». En outre, la Norme 1220, Conscience professionnelle, indique que « les auditeurs internes doivent apporter à leur travail la diligence et le savoir-faire que l'on peut attendre d'un auditeur interne raisonnablement averti et compétent. La conscience professionnelle n'implique pas l'infaillibilité ».

Il importe de noter que l'interprétation de la Norme 1200 définit « les connaissances, le savoir-faire et les autres compétences [comme] une expression générique utilisée pour décrire la capacité professionnelle dont les auditeurs internes doivent disposer pour pouvoir exercer efficacement leurs responsabilités professionnelles ». Cette interprétation encourage en outre les auditeurs internes à « démontrer leurs compétences en obtenant des certifications et qualifications professionnelles appropriées telles que le CIA (*Certified Internal Auditor*) et tout autre diplôme promu par l'IIA [par l'un de ces chapitres nationaux] ou par d'autres organisations professionnelles appropriées ».

PLANIFICATION

Comme mentionné précédemment, le responsable de l'audit interne est chargé d'élaborer un budget opérationnel et d'allouer les ressources de façon à réaliser le plan annuel d'audit interne. Ce dernier est élaboré par l'audit interne *via* un processus qui identifie et hiérarchise les entités sur lesquelles peut porter l'audit (la définition de ces unités opérationnelles ou processus métier renvoie à la notion d'« univers d'audit »), afin de ramener les principaux risques, qu'ils soient stratégiques, opérationnels, de reporting ou de conformité, à un niveau acceptable aux yeux du Conseil et de la direction générale de l'organisation. Les principaux risques sont ceux qui doivent faire l'objet d'un contrôle et d'une surveillance, pour que l'organisation puisse atteindre les objectifs qu'elle s'est fixés. Ces risques, tels qu'identifiés par la direction générale, doivent être

Compétence

Les connaissances, le savoir-faire et les autres compétences que les auditeurs doivent posséder et qui sont nécessaires à l'exercice de leurs responsabilités individuelles.

Conscience professionnelle

La diligence et le savoir-faire que l'on peut attendre d'un auditeur interne raisonnablement averti et compétent ; la conscience professionnelle n'implique pas l'infaillibilité.

Univers d'audit

Ensemble des filiales, unités opérationnelles, services, groupes, processus ou autres subdivisions en place dans une organisation qui gèrent un ou plusieurs risques opérationnels.

Plan d'audit interne

Description des missions d'assurance et de conseil programmées sur une certaine période (généralement un an) sur la base d'une évaluation des risques de l'organisation.

Copyright © 2015 Eyrolles.

corroborés par l'audit interne en toute indépendance. Une fois ces risques identifiés par consensus, le responsable de l'audit interne détermine quels unités opérationnelles et processus métier doivent s'attacher à maîtriser ces risques. L'information qui en résulte est alors soumise à un processus qui hiérarchise les risques et les unités opérationnelles ou processus métier qui y sont associés. Le responsable de l'audit interne prend en compte toutes ces informations et détermine les ressources humaines et financières nécessaires pour une couverture appropriée de l'univers d'audit, par ordre de priorité. Il en résulte un plan d'audit interne complet qui comprend à la fois les activités d'assurance et de conseil nécessaires pour évaluer si, dans les faits, l'organisation gère efficacement les risques qui menacent ses objectifs, et pour identifier les opportunités d'amélioration de la gestion des risques. Le plan d'audit peut alors être mis en œuvre. Des collaborateurs spécifiques sont ainsi affectés à chacune des missions qui composent le plan d'audit pour l'exercice à venir. L'audit interne mettra en œuvre et allouera les ressources à l'exécution du plan d'audit interne pendant tout l'exercice. Il arrive fréquemment qu'il actualise et refonde ce plan plus souvent qu'une fois par an (par exemple tous les trimestres ou tous les mois).

Il existe beaucoup de théories concernant l'élaboration d'un plan d'audit interne. De nombreuses fonctions d'audit interne ont opté pour un processus global dans lequel la direction générale et l'audit interne travaillent ensemble pour élaborer une évaluation formelle complète des risques dans toute l'organisation, afin de dresser une liste des priorités que l'organisation doit traiter pour atteindre ses principaux objectifs face aux scénarios des principaux risques. Il est toutefois beaucoup plus courant que le processus soit informel et nettement moins collaboratif. Quel que soit le processus retenu, l'efficacité sera maximale si l'évaluation des risques est effectuée sur une base annuelle en début d'exercice ou avant. Le responsable de l'audit interne peut ainsi déterminer les ressources d'audit pour l'année à venir en fonction des conclusions tirées de cette évaluation des risques par le management. Lorsque le responsable de l'audit interne dispose d'une liste définitive des entités à auditer liées aux risques figurant sur la liste des priorités, il peut élaborer un plan d'audit interne selon une approche descendante et fondée sur les risques. Cependant, de nombreuses organisations et leur fonction d'audit interne n'utilisent toujours pas cette approche. Ils continuent de définir des plans d'audit interne qui abordent de manière cyclique chaque service de l'organisation en prévoyant des audits plus fréquents pour les unités opérationnelles ou les processus métier classés comme prioritaires, et moins fréquents pour les autres.

L'IIA explique les différences entre les activités d'assurance et de conseil relatives à la Norme 2010, Planification, au moyen des Normes 2010.A1 et 2010.C1.

Copyright © 2015 Eyrolles.

- **Activités d'assurance.** Le plan d'audit interne doit s'appuyer sur une évaluation des risques documentée et réalisée au moins une fois par an. Les points de vue de la direction générale et du Conseil doivent être pris en compte dans ce processus (Norme 2010.A1).
- **Activités de conseil.** Lorsqu'on lui propose une mission de conseil, le responsable de l'audit interne, avant de l'accepter, devrait considérer dans quelle mesure elle est susceptible de créer de la valeur ajoutée, d'améliorer le management des risques et le fonctionnement de l'organisation. Les missions de conseil qui ont été acceptées doivent être intégrées dans le plan d'audit (Norme 2010.C1).

Le processus de planification doit porter sur la définition des objectifs, le calendrier des missions, les prévisions d'effectifs et les budgets financiers. En outre, une planification efficace doit se faire l'écho de la charte d'audit interne et rester dans la lignée des objectifs de l'organisation.

COMMUNICATION ET APPROBATION

Une fois le plan d'audit interne défini, le responsable de l'audit interne doit le présenter à la direction générale et au Conseil (en général le comité d'audit) pour approbation. Il doit également signaler ses besoins, tout changement important susceptible d'intervenir en cours d'exercice ainsi que l'impact de toute limitation de ses ressources (Norme 2020, Communication et approbation).

La MPA 2020-1, Communication et approbation, donne des recommandations précises concernant le respect de cette exigence.

- Le responsable de l'audit interne soumet, annuellement, pour examen et approbation, à la direction générale et au Conseil, une synthèse du plan annuel d'audit interne, du planning des travaux, des prévisions d'effectifs et le budget financier. Cette synthèse signalera à la direction générale et au Conseil l'étendue des missions d'audit et, le cas échéant, les limitations qui y sont apportées. Le responsable de l'audit interne signalera également, pour information et approbation, tout changement ultérieur significatif.
- Le planning des travaux, les prévisions d'effectifs et le budget financier approuvés, ainsi que tous les changements importants survenus en cours d'exercice, doivent contenir suffisamment d'informations pour permettre à la direction générale et au Conseil de déterminer si les objectifs et les plans de l'audit interne correspondent à ceux de l'organisation et du Conseil et sont cohérents avec la charte d'audit interne.

Copyright © 2015 Eyrolles.

L'*Internal Auditor Competency Framework*

Ouvrage publié par l'IIA qui décrit le niveau minimum de connaissances et de compétences requis de la part des auditeurs internes à différents moments de leur carrière, en les décomposant selon les quatre éléments suivants :
- qualités relationnelles ;
- outils et techniques ;
- normes d'audit interne ;
- domaines de compétence.

Commentaire du traducteur

*L'*Internal Auditor Competency Framework *est régulièrement actualisé. Ainsi, en 2013, le référentiel de compétences des auditeurs internes, des managers et des responsables de l'audit a été décliné en 10 domaines (déontologie ; gestion du service d'audit interne ; CRIPP ; gouvernance ; gestion des risques et dispositifs de contrôle ; connaissance de l'organisation et de son environnement ; communication ; persuasion et collaboration ; esprit critique ; planification et réalisation des missions d'audit interne ; amélioration et innovation). Ces domaines correspondent à ceux qui sont développés dans cet ouvrage.*

GESTION DES RESSOURCES

L'allocation des ressources constitue un paramètre important dans la mise en œuvre du plan d'audit interne. Il appartient au responsable de l'audit interne de « veiller à ce que les ressources affectées à cette activité soient adéquates, suffisantes et mises en œuvre de manière efficace pour réaliser le plan d'audit approuvé » (Norme 2030, Gestion des ressources). Il convient pour ce faire de gérer de manière pertinente un certain nombre de paramètres.

Structure organisationnelle et stratégie relative aux collaborateurs

L'audit interne doit être structuré de façon cohérente par rapport aux besoins et à la culture de son organisation. Le responsable de l'audit interne peut opter pour une structure horizontale dans laquelle la plupart des auditeurs internes présentent plus ou moins le même niveau de compétences, d'expérience et d'ancienneté. Généralement, avec ce type d'organisation, l'audit interne est stable, très compétent et les auditeurs travaillent en collaboration. Il n'est pas nécessaire que la supervision soit importante, et les travaux réalisés sont cohérents et fiables. Cependant, une structure horizontale alourdit généralement les coûts en raison du niveau de salaire élevé nécessaire pour retenir les auditeurs qui possèdent l'expérience et l'expertise nécessaires. D'autres fonctions d'audit interne suivent, par nature, une structure nettement plus hiérarchique ; les auditeurs de terrain rendent compte aux auditeurs seniors et apprennent de ces derniers. Les auditeurs seniors quant à eux rendent compte aux managers et aux directeurs d'audit, qui guident leurs subalternes et épaulent le responsable de l'audit interne placé au-dessus d'eux.

Les fonctions d'audit interne à structure hiérarchique sont en principe plus dynamiques, car la rotation des effectifs est fréquente. Lorsque les individus proches du sommet de la structure organisationnelle gravissent des échelons et que certains quittent le service,

Copyright © 2015 Eyrolles.

ceux qui se trouvaient à des postes subalternes viennent pourvoir les postes ainsi libérés. Cette méthode permet aux individus de progresser au sein du service, mais aussi de cultiver diverses compétences et de découvrir de nouvelles perspectives, pour un coût moindre. Ces deux types d'organisations s'appuient toutefois sur des collaborateurs qui continuent de suivre des formations et d'élargir leur base de compétences.

L'audit interne classique à structure hiérarchique se compose de membres, qui occupent diverses positions, en fonction de leur rôle précis au sein de la fonction.

- **Les auditeurs internes.** Les collaborateurs de l'équipe d'audit sont chargés d'effectuer le travail sur le terrain pour les missions financières, opérationnelles, de conformité et sur les systèmes d'information en respectant le calendrier d'audit établi, afin de juger de l'exactitude des documents financiers, de l'efficacité des pratiques de l'organisation et de la conformité aux règles, procédures, lois et règlements.
- **L'auditeur interne senior (ou chef de mission).** Outre les responsabilités énoncées ci-dessus, les auditeurs seniors sont chargés de planifier les étapes d'une mission, de guider les collaborateurs de l'équipe d'audit dans leur travail de terrain, de veiller au respect du calendrier de la mission, de réviser les papiers de travail préparés par les collaborateurs d'audit, de contribuer à l'élaboration de la communication des résultats de la mission, d'effectuer les étapes finales de la mission et d'évaluer les performances des auditeurs de l'équipe.
- **Le superviseur.** Le superviseur supervise et administre les missions conformément au calendrier d'audit établi. En outre, il aide à élaborer et à mettre à jour le plan annuel d'audit interne ainsi que le modèle de risque pour certains services, à communiquer les résultats de la mission et à superviser les auditeurs seniors.
- **Le directeur de mission.** Le poste de directeur de mission se trouve dans les fonctions d'audit interne de grande taille. Outre les responsabilités énoncées ci-dessus, le directeur de mission participe à l'élaboration de la stratégie et de la planification générales d'audit interne, et notamment à la présentation et à l'examen de la stratégie, de la mission, de la charte et du plan d'audit interne, et procède à la planification avec le comité d'audit et la direction générale. Le directeur de mission supervise également les superviseurs et est chargé de recruter et de licencier les membres du service d'audit interne.
- **Le responsable de l'audit interne.** Le responsable de l'audit interne élabore, oriente, organise, surveille, planifie et administre le plan et le budget de l'audit interne tels qu'approuvés par le comité d'audit, afin de juger notamment de l'exactitude des documents financiers, de l'efficacité des pratiques de

Copyright © 2015 Eyrolles.

l'organisation et de la conformité aux règles, procédures, lois et règlements. De plus, le responsable de l'audit interne supervise directement l'équipe de management de l'audit interne (directeurs de mission et superviseurs), surveille l'ensemble de la fonction d'audit interne et donne son approbation à l'embauche et au licenciement des auditeurs internes.

Outre les fonctions traditionnelles précitées, de nombreux services d'audit interne créent également des fonctions spécialisées en vue d'offrir un ensemble rare ou unique de compétences, d'expériences et de connaissances, telles que celles que possèdent des ingénieurs, des actuaires, des rédacteurs, des analystes de données, etc. Ces fonctions varient sensiblement selon la philosophie, la structure et le mandat de l'audit interne, et selon le secteur, l'environnement réglementaire et la structure de gouvernance de l'organisation. Selon la complexité de l'expertise requise, l'expérience souhaitée et les besoins particuliers du service d'audit interne, ces fonctions spécialisées peuvent être exécutées à tous les niveaux (du membre de l'équipe au responsable de l'audit interne).

L'*Internal Auditor Competency Framework*, publié par l'IIA, donne des informations détaillées sur le niveau minimum de connaissances et de compétences requis de la part des auditeurs internes à différents moments de leur carrière, en les décomposant selon les quatre éléments suivants : qualités relationnelles, outils et techniques, normes d'audit interne et domaines de compétence. L'*Internal Auditor Competency Framework* est étudié dans le chapitre 1, *Introduction à l'audit interne* ; il est disponible sur le site Internet de l'IIA dans la section « Professional Guidance ».

Ajustement des effectifs

L'ajustement des effectifs représente un concept important pour la dotation en personnel et la planification d'un service d'audit interne. Il est important de trouver et de conserver des collaborateurs compétents et qualifiés, afin de pouvoir exécuter le plan d'audit interne sans faire peser une pression inutile sur les collaborateurs en raison d'une charge de travail excessive, tout en conservant un budget raisonnable. Cette affirmation est valable que la structure du service d'audit soit horizontale ou hiérarchique, et c'est souvent un facteur à prendre en compte lorsque l'on détermine le type de structure qui convient à une organisation. Le responsable de l'audit interne s'appuie sur diverses sources afin de valider les décisions en la matière, notamment le travail en réseau, les études comparatives, les études de marché et autres sources de conseil.

Copyright © 2015 Eyrolles.

Prévisions d'effectifs/ressources humaines

Si certains aspects de la gestion des ressources humaines sont délégués à d'autres collaborateurs seniors de l'audit interne (par exemple, les directeurs et superviseurs interviennent parfois largement dans la sélection et le recrutement des candidats), c'est le responsable de l'audit interne qui « s'assure de l'adéquation et de la gestion des ressources nécessaires à l'exercice des responsabilités de l'audit interne, telles que définies dans la charte. Cela suppose l'existence d'une réelle communication avec la direction générale et le Conseil sur les besoins et le profil des ressources de l'audit interne » (MPA 2030-1, Gestion des ressources). De plus, le responsable de l'audit interne doit veiller à ce que le service d'audit interne dispose des compétences et du savoir nécessaires pour mener à bien le plan d'audit interne et « permettre l'accomplissement de ses activités avec toute la justesse, la précision et la ponctualité attendues par la direction générale et le Conseil, comme prévu dans la charte d'audit interne » (MPA 2030-1).

Le responsable de l'audit interne doit également procéder à une affectation efficace des ressources humaines, ce qui signifie que les auditeurs internes sont affectés à des missions pour lesquelles ils sont qualifiés et à même d'obtenir des résultats. Dans certains cas, les personnes ayant une connaissance et/ou des compétences spécialisées, au sein de l'organisation (ou en dehors de l'organisation), peuvent participer à une mission d'audit interne, lorsque les compétences nécessaires ne sont pas disponibles au sein de la fonction d'audit interne.

Plus généralement, le responsable de l'audit interne tient compte du plan de succession et veille à ce que soit en place une solide évaluation des collaborateurs et des programmes de développement des compétences. Pour ce qui est des autres aspects de la gestion de l'audit interne, le responsable de l'audit interne doit discuter ouvertement avec la direction générale et le Conseil des sujets relatifs aux ressources humaines. Classiquement, cette communication prend la forme d'actualisations régulières au cours de réunions trimestrielles du Conseil. Ces actualisations se composent d'une « synthèse précisant le profil et l'adéquation des ressources », mais aussi d'« indicateurs appropriés, [de] buts et [d']objectifs pour contrôler l'adéquation générale des ressources. Il peut s'agir de la comparaison des ressources avec le plan annuel d'audit, de l'impact d'une absence temporaire de ressources ou d'une vacance de poste, des formations et apprentissages, de nouveaux besoins ou exigences spécifiques résultant des changements intervenus dans les activités commerciales, le fonctionnement, les programmes, les systèmes et les contrôles de l'organisation » (MPA 2030-1).

Copyright © 2015 Eyrolles.

Pratiques d'embauche

Le responsable de l'audit interne doit embaucher des collaborateurs pour doter la structure organisationnelle de la fonction de manière à en maximiser l'efficience, à obtenir la base de compétences nécessaires et à faire bon usage du budget. Pour ce faire, il cherche généralement à recruter des personnes possédant une formation et un savoir-faire dans un certain nombre de domaines, notamment la comptabilité et la communication financière, les systèmes d'information, les activités opérationnelles, les lois et règlements applicables et diverses connaissances propres au secteur d'activité.

Externalisation (ou co-traitance)

Externalisation (ou co-traitance)

Complément apporté à la fonction d'audit interne de l'organisation par le recours aux services de prestataires tiers afin de se doter d'une expertise dans un domaine précis et pour une mission spécifique ou de combler une lacune dans les ressources nécessaires pour mener à bien le plan d'audit interne.

L'externalisation (*outsourcing*) ou co-traitance (*cosourcing*) permet au responsable de l'audit interne d'optimiser la base de compétences de ses collaborateurs et les aspects financiers y afférents. L'audit interne peut ainsi rester efficient, car il recrute des collaborateurs permanents dotés d'une vaste base de compétences générales, tout en se réservant la possibilité de faire appel aux experts nécessaires pour des projets ou des audits spécifiques, mais qu'il serait trop coûteux de maintenir de façon permanente au sein de l'équipe. L'externalisation ou co-traitance sert également à la planification, lorsque le nombre d'heures prévues pour la réalisation du plan d'audit dépasse celui que peuvent effectuer les collaborateurs permanents, et que l'embauche d'un collaborateur supplémentaire serait inefficiente, présenterait un coût prohibitif ou se révélerait impossible dans les conditions actuelles du marché.

Formation et tutorat

Le développement des ressources humaines revêt une importance particulière pour une fonction d'audit interne en raison du niveau de compétence et de conscience professionnelle qu'on attend d'elle, comme indiqué précédemment dans ce chapitre. Si la Norme 1220, Conscience professionnelle, souligne spécifiquement qu'on n'attend pas qu'ils soient infaillibles, les collaborateurs doivent, en tout état de cause, actualiser leur connaissance du secteur et leurs compétences en matière d'audit. Cela passe principalement par une formation et un tutorat, ainsi que par la formation continue. Chaque fonction d'audit interne doit définir un minimum de formation et de développement professionnel, ce qui englobe généralement les certifications professionnelles (par exemple, *Certified Internal Auditor* [CIA], *Certified Information Systems Auditor* [CISA] et *Certified Fraud Examiner* [CFE]), ainsi que le minimum de formation continue permettant de conserver ces certifications.

Copyright © 2015 Eyrolles.

Gestion des carrières et développement professionnel

Outre la formation et le tutorat requis pour satisfaire aux exigences de compétence et de conscience professionnelle, une bonne fonction d'audit interne doit se doter d'un plan de gestion des carrières et d'un plan de succession, qui permettent à chaque collaborateur d'atteindre ses objectifs de carrière à long terme tout en continuant à participer aux activités de l'audit interne. Grâce à une gestion des carrières et à un processus de développement professionnel solides, l'audit interne possédera toujours des collaborateurs qualifiés et compétents pour exécuter le plan d'audit approuvé et s'acquitter de ses missions, pouvoirs et responsabilités tels que définis dans la charte d'audit interne.

Planification

Une fois que l'équilibre est trouvé entre collaborateurs permanents et intervenants extérieurs au sein de l'audit interne, le responsable de l'audit interne peut commencer à planifier ou à assigner des audits et des projets spécifiques aux collaborateurs qui sont les mieux à même de les réaliser. C'est là que les avantages de bonnes pratiques d'embauche et d'ajustement des effectifs prennent tout leur sens. Le responsable de l'audit interne tire pleinement parti de son budget en formant des équipes qui, en fonction de leurs compétences et de leur place dans la structure organisationnelle, atteindront avec le plus d'efficience et d'efficacité les objectifs d'une mission donnée. Dans le même temps, le responsable de l'audit interne prend en considération les besoins de développement de ses collaborateurs et s'efforce d'arbitrer entre les opportunités de développement que peut offrir une mission donnée et la nécessité d'achever les missions dans les temps.

Budget

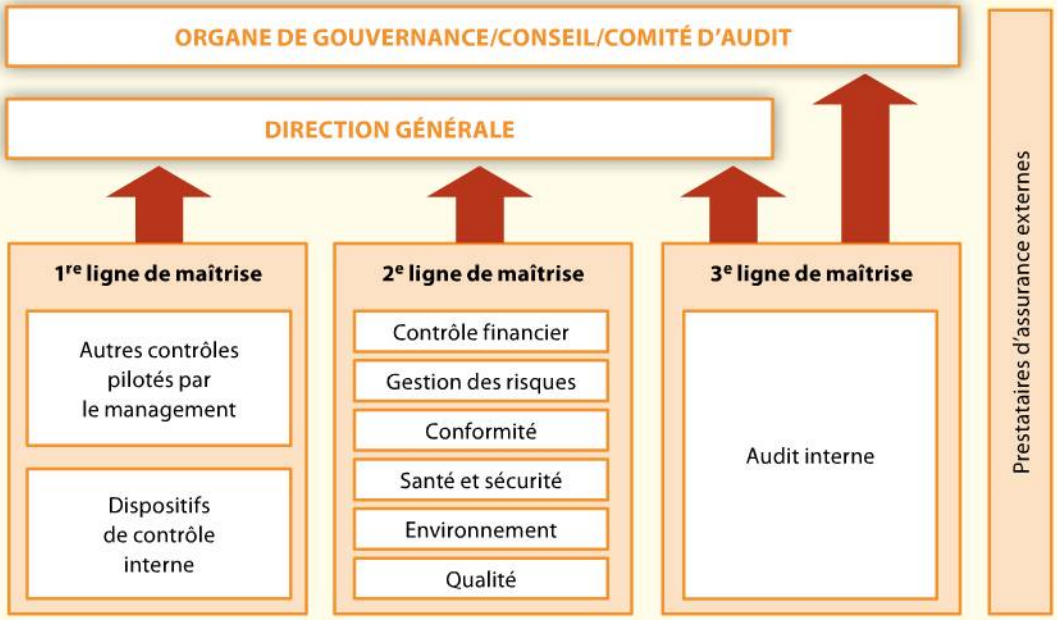
Comme déjà indiqué dans ce chapitre, le budget dépend en premier lieu du plan d'audit interne, de la structure organisationnelle et de la stratégie relative aux effectifs. Le responsable de l'audit interne doit soigneusement évaluer les ressources financières requises pour atteindre les objectifs fixés. Il apparaît à ce stade que le budget influence et est influencé par chacune des tâches effectuées par le responsable de l'audit interne, qui sont décrites ci-dessus.

RÈGLES ET PROCÉDURES

La norme relative à la mise en œuvre de règles et de procédures énonce simplement que « le responsable de l'audit interne doit établir des règles et procédures fournissant un cadre à l'activité d'audit

Copyright © 2015 Eyrolles.

ATTEINTES À L'INDÉPENDANCE ET À L'OBJECTIVITÉ : LES EXIGENCES DE L'IIA



Global Advocacy Platform (Altamonte Springs, Floride: The Institute of Internal Auditors Global, 2012), p. 9.

ENCADRÉ 9-4

interne » (Norme 2040, Règles et procédures). La MPA 2040-1, Règles et procédures, recommande des règles et procédures adaptées à la taille de la fonction d'audit interne : « Le responsable de l'audit interne établit des règles et des procédures. Des manuels administratifs et techniques peuvent ne pas être nécessaires pour toutes les entités d'audit interne. Un petit service d'audit interne peut être dirigé d'une manière informelle. Son personnel peut être dirigé et contrôlé au jour le jour par une supervision étroite et des notes de service qui définissent les règles et les procédures à suivre. Par contre, dans un service d'audit interne important, il est essentiel de disposer de règles et procédures plus formalisées et complètes pour guider les auditeurs dans la réalisation du plan annuel d'audit. »

Auditeur externe

Cabinet d'experts-comptables agréé, chargé par le Conseil ou la direction générale de l'organisation de procéder à un audit des états financiers.

COORDINATION DES TRAVAUX D'ASSURANCE

Selon la MPA 2050-1 (*cf.* p. 9-3), Coordination, « afin d'assurer une couverture adéquate et d'éviter les doubles emplois, le responsable de l'audit interne devrait partager des informations et coordonner les activités avec les autres prestataires internes et externes d'assurance et de conseil ». Il est important de coordonner les travaux de l'audit interne et ceux des autres prestataires de services d'assurance et de conseil à l'intérieur et à l'extérieur de l'organisation en raison des gains d'efficience et d'efficacité qui peuvent en découler.

Copyright © 2015 Eyrolles.

Nombre d'organisations disposent de divers moyens pour s'assurer qu'elles opèrent dans les limites de leur appétence pour le risque. Celles qui opèrent dans un environnement hautement réglementé doivent notamment démontrer qu'elles ont su ramener à un niveau raisonnable les nombreux risques auxquels elles sont exposées. Elles mettent donc en place différents niveaux d'assurance pour maîtriser les risques tel que requis ou souhaité. Le « modèle des trois lignes de maîtrise » est un exemple classique.

Ce modèle permet aux organisations d'articuler en plusieurs niveaux les moyens par lesquels elles obtiennent l'assurance que les risques auxquels elles sont exposées sont maîtrisés dans les limites de leur appétence pour le risque. En dépit de son nom, ce modèle peut inclure plus de trois lignes (niveaux) d'assurance en fonction de l'organisation et de la manière dont elle est structurée.

L'encadré 9-4 est une représentation traditionnelle du modèle des trois lignes de maîtrise, dans laquelle les prestataires d'assurance externes et indépendants sont placés à l'extérieur du modèle. Comme indiqué plus haut, les organisations peuvent adapter ce modèle de manière à ce qu'il représente leur approche ou leur philosophie particulière.

Les différentes lignes de maîtrise illustrées dans l'encadré sont décrites ci-après.

- **Première ligne de maîtrise.** Le management est responsable de l'évaluation et de la maîtrise des risques, et doit maintenir des dispositifs de contrôle interne efficaces. Cette ligne de maîtrise interne n'est pas indépendante du management opérationnel.
- **Deuxième ligne de maîtrise.** Au sein de l'organisation, différents services collaborent pour contribuer à la maîtrise des risques en facilitant et en pilotant les efforts de gestion des risques de l'organisation. Ces services participent également à la communication d'informations adéquates en matière de risques. Cette ligne de maîtrise interne n'est pas indépendante du management opérationnel. L'audit interne collabore avec ces services en contribuant aux évaluations des risques, en demandant et en apportant un retour d'information sur les domaines de l'organisation qui évoluent, etc. Cette coordination ne compromet ni l'indépendance ni l'objectivité de l'audit interne.
- **Troisième ligne de maîtrise.** L'audit interne constitue la troisième ligne de maîtrise interne. Contrairement aux deux premières, cette ligne de maîtrise est indépendante de l'ensemble du management opérationnel.

Le degré de coordination entre ces trois lignes de maîtrise peut sensiblement varier selon l'organisation. Dans les organisations de taille plus restreinte et moins réglementées, les efforts de coordination déployés pour dégager les gains d'efficience souhaités peuvent

Copyright © 2015 Eyrolles.

être moins formels. Dans les organisations de taille plus importante soumises à une forte réglementation, la coordination peut être très formelle et complexe. Ces organisations commencent généralement par élaborer une cartographie des services donnant une assurance. Cette cartographie permet de déterminer où il existe une maîtrise des risques au sein de l'organisation, qui opère cette couverture, quelles sont les normes professionnelles auxquelles les différents prestataires d'assurance se conforment, et quels sont la fréquence et le calendrier des activités d'assurance. Si ce processus exige beaucoup de temps au début, les gains d'efficience réalisés par la suite en valent souvent la peine.

- **Autres lignes de maîtrise.** Outre les lignes de maîtrise internes précitées, les organisations s'appuient également sur des sources externes pour s'assurer que les risques auxquels elles sont confrontées sont maîtrisés de manière appropriée. Ces sources incluent notamment les auditeurs externes de l'organisation et les régulateurs compétents. Que l'organisation les intègre formellement à son modèle de lignes de maîtrise ou non, ils lui apportent un niveau supplémentaire d'assurance externe et indépendante.

S'il est essentiel de capitaliser les travaux des autres activités d'assurance et de conseil, réalisées en interne ou en externe, la forme la plus courante de collaboration est celle qui existe avec les auditeurs externes. La MPA 2050-1, Coordination, précise dans quel contexte l'audit interne peut recourir aux travaux d'auditeurs externes. Plus exactement, elle indique qu'alors « le responsable de l'audit interne prend les mesures nécessaires pour comprendre le travail réalisé par les auditeurs externes, notamment :

- l'étendue, la nature du travail et l'échéancier prévus par les auditeurs externes et s'assurer que le travail des auditeurs internes et externes répond aux exigences de la Norme 2100 [Nature du travail] ;
- l'évaluation des risques et le seuil de matérialité utilisés par les auditeurs externes ;
- les techniques, les méthodes et la terminologie employées par les auditeurs externes, afin de permettre au responsable de l'audit interne de (1) coordonner le travail des auditeurs internes et externes, (2) évaluer le travail des auditeurs externes pour s'y appuyer, (3) communiquer efficacement avec les auditeurs externes ;
- l'accès aux programmes et aux documents de travail des auditeurs externes pour s'assurer que leur travail peut être utilisé pour atteindre les objectifs de l'audit interne. Les auditeurs internes respectent la confidentialité de ces programmes et documents de travail ».

Conseil

Organe de gouvernance d'une organisation. Il peut s'agir d'un Conseil d'administration, d'un Conseil de surveillance, de l'organe délibérant d'un organisme public ou d'une association ou de tout autre organe y compris le Comité d'audit auquel le responsable de l'audit interne peut être rattaché sur le plan fonctionnel.

Copyright © 2015 Eyrolles.

Pour mettre encore davantage à profit les synergies entre les auditeurs internes et les auditeurs externes, le responsable de l'audit interne doit offrir les mêmes opportunités aux auditeurs externes afin qu'ils puissent, à leur tour, s'appuyer sur les travaux accomplis par l'audit interne. Pour réussir cette coordination dans les deux sens, il est intéressant qu'auditeurs internes et auditeurs externes utilisent des « techniques, méthodes et terminologie similaires » (MPA 2050-1). Pour ce faire, on recommande des réunions régulières au cours desquelles ils discutent des activités d'audit planifiées, du calendrier de réalisation et de l'impact éventuel des observations et recommandations sur la portée des travaux planifiés. En outre, l'audit interne doit mettre à la disposition de l'auditeur externe tous les rapports définitifs de l'audit interne, les commentaires du management à propos de ces rapports, et les analyses complémentaires qui en découlent. Ces rapports aident les auditeurs externes à déterminer et à ajuster l'étendue et le calendrier de leur travail. De même, l'audit interne doit pouvoir accéder aux supports de présentation et communications des auditeurs externes, de sorte que le responsable de l'audit interne puisse s'assurer de « l'existence d'un suivi approprié et de la mise en œuvre des actions correctives » (MPA 2050-1).

Si le responsable de l'audit interne est chargé de la coordination entre auditeurs internes et auditeurs externes, le Conseil (directement ou à travers le comité d'audit) est responsable de la surveillance de cette coordination, ainsi que des travaux des auditeurs externes. Le responsable de l'audit interne doit donc obtenir le soutien du Conseil pour coordonner efficacement les travaux de l'audit interne et ceux des auditeurs externes. Grâce à des communications régulières, le responsable de l'audit interne informe le Conseil des résultats de l'évaluation continue de ses activités de coordination et plus particulièrement de celles qui concernent les auditeurs externes

RAPPORTS AU CONSEIL ET À LA DIRECTION GÉNÉRALE

« Le responsable de l'audit interne doit rendre compte périodiquement à la direction générale et au Conseil des missions, des pouvoirs et des responsabilités de l'audit interne, ainsi que du degré de réalisation du plan d'audit. Il doit plus particulièrement rendre compte de l'exposition aux risques significatifs (y compris des risques de fraude) et des contrôles correspondants ; des sujets relatifs au gouvernement d'entreprise ; et de tout autre problème répondant à un besoin ou à une demande de la direction générale ou du Conseil » (Norme 2060, Rapports à la direction générale et au Conseil). Le responsable de l'audit interne atteste que ces responsabilités professionnelles ont été satisfaites en présentant régulièrement un rapport sur les résultats des activités d'audit interne en cours à la direction générale et au comité d'audit lors des réunions régulières

Copyright © 2015 Eyrolles.

prévues durant l'année. Ces rapports permettent également d'informer la direction générale et le Conseil sur « les écarts significatifs par rapport au plan d'audit, aux prévisions de dotation en personnel et aux budgets financiers approuvés ; les raisons de ces écarts ; et les mesures prises ou à prendre » (MPA 2060-1, Rapports à la direction générale et au Conseil). Dans le cas où la direction générale et/ou le Conseil ont accepté le risque de ne pas entreprendre d'actions correctives après des observations d'audit significatives, le responsable de l'audit interne juge s'il convient d'informer le Conseil de ces observations d'audit significatives en fonction des circonstances présentes, notamment lorsque des changements sont récemment intervenus dans le management ou le profil de risque de l'organisation.

En outre, le management et le responsable de l'audit interne coordonnent leurs efforts pour présenter régulièrement un rapport sur diverses activités de contrôle et de réduction des risques effectuées par l'une et l'autre, conformément aux rôles et responsabilités fixées par le Conseil et le comité d'audit. Ces rapports traitent généralement des aspects suivants :

- pilotage des risques par les unités opérationnelles et reporting y afférent ;
- activités des auditeurs externes ;
- activités financières clés ;
- activités de gestion des risques ;
- respect de la législation et conformité aux règles.

Outre ces informations, la direction générale ou le responsable de l'audit interne soumet généralement un rapport au comité d'audit qui énonce les résultats de l'auto-évaluation du management quant à l'adéquation de la conception et au fonctionnement effectif du dispositif de contrôle interne de l'organisation. Au minimum, l'audit interne doit évaluer de façon indépendante le processus adopté par le management pour aboutir à ses conclusions. Cependant, de nombreux responsables de l'audit interne donnent également leur opinion, en toute indépendance, sur le système de contrôle interne de l'organisation relatif au reporting financier. Cette opinion est communiquée au comité d'audit en même temps que les critères de qualité retenus par le management sur le système de contrôle interne. Dans un nombre de cas plus limité, l'opinion des responsables de l'audit interne porte sur le contrôle interne relatif aux objectifs liés aux opérations, à la conformité et au reporting extrafinanciers.

Commentaire du traducteur

Notons que la version 2013 de la Norme IIA 2130.A1 étend le rôle de l'audit interne à l'évaluation de l'efficacité des dispositifs relatifs à l'atteinte des objectifs stratégiques de l'organisation.

Copyright © 2015 Eyrolles.

Ils considèrent cette activité comme le prolongement naturel du plan annuel d'audit interne au titre duquel l'audit interne a déjà procédé à une évaluation indépendante du système de contrôle interne de l'organisation, comme le prévoit le plan d'audit interne. Certains responsables de l'audit interne ne sont pas d'accord avec cette approche et affirment qu'elle contredit directement leur devoir, qui consiste à évaluer de façon indépendante et objective l'auto-évaluation des systèmes de contrôle interne par le management. L'approche retenue par une organisation dépend en grande partie de sa culture.

Cependant, étant donné que le responsable de l'audit interne est chargé de maintenir des relations avec des instances dont les attentes peuvent être conflictuelles, notamment le comité d'audit, la direction générale, la ligne managériale et diverses parties extérieures (régulateurs et auditeurs externes, en particulier), cela n'est pas toujours aussi simple qu'il n'y paraît. Si un rapport d'audit ne renferme aucune observation et qu'on estime que les contrôles internes sont conçus de manière adéquate et fonctionnent de manière effective, il n'y a normalement pas désaccord entre les parties. Toutefois, si l'audit interne estime que les contrôles internes sont conçus de manière inadéquate et/ou ne fonctionnent pas de manière effective, il peut y avoir désaccord entre le management et une ou plusieurs des parties. La situation se complique fortement. Le responsable de l'audit interne ne doit pas se contenter de signaler ce désaccord au Conseil et à la direction générale. Il doit également recommander une solution destinée à remédier à l'observation en question et faire remonter au Conseil et à la direction générale quelles mesures le management souhaite mettre en œuvre pour la rectifier. Ce n'est que dans de très rares cas, lorsque le responsable de l'audit interne et le management ne parviennent pas à s'entendre sur l'observation et/ou sa solution, que le responsable de l'audit rapportera une observation qui ne sera pas accompagnée de sa solution. Les obligations de communication sont détaillées au chapitre 14, *La communication des résultats d'une mission d'assurance et les procédures de suivi*, et au chapitre 15, *La mission de conseil*.

LA GOUVERNANCE

Comme le définit le chapitre 1, *Introduction à l'audit interne*, puis à nouveau le chapitre 3, *La gouvernance*, la gouvernance est un processus piloté par le Conseil qui consiste à autoriser, diriger et surveiller les activités de la direction générale en vue de réaliser les objectifs de l'organisation. Le chapitre 3 donne des détails sur le processus de gouvernance, ainsi que sur les rôles et responsabilités de toutes les parties impliquées. Toutefois, dans le présent chapitre, nous n'examinerons la gouvernance que sous l'angle des responsabilités spécifiques de l'audit interne.

Gouvernance (ou gouvernement d'entreprise)

Dispositif comprenant les processus et les structures mis en place par le Conseil afin d'informer, de diriger, de gérer et de piloter les activités de l'organisation en vue de réaliser ses objectifs.

Copyright © 2015 Eyrolles.

Selon la Norme 2110, Gouvernement d'entreprise, l'audit interne doit « évaluer le processus de gouvernement d'entreprise et formuler des recommandations appropriées en vue de son amélioration. À cet effet, il détermine si le processus répond aux objectifs suivants :

- promouvoir des règles d'éthique et des valeurs appropriées au sein de l'organisation ;
- garantir une gestion efficace des performances de l'organisation, assortie d'une obligation de rendre compte ;
- communiquer aux services concernés de l'organisation les informations relatives aux risques et aux contrôles ;
- fournir une information adéquate au Conseil, aux auditeurs internes et externes et au management, et assurer une coordination de leurs activités ».

Ce sont les missions d'assurance réalisées par l'audit interne qui permettent en grande partie de s'acquitter de ces responsabilités. La charte d'audit interne définit le rôle qu'a l'audit interne dans la fourniture d'une assurance relative au processus de gouvernance et elle doit refléter les attentes du Conseil. Le chapitre 3 donne les exemples suivants de responsabilité de l'audit interne vis-à-vis de la gouvernance :

- déterminer si les diverses activités de gestion des risques sont conçues de manière à permettre une gestion correcte des risques susceptibles de générer des événements inacceptables ;
- vérifier que les diverses activités de gestion des risques fonctionnent comme prévu ;
- vérifier si les déclarations faites par les propriétaires de risques à la direction générale au sujet de l'efficacité des activités de gestion des risques donnent une image exacte de l'efficacité actuelle de la gestion des risques ;
- vérifier si les déclarations faites par la direction générale au Conseil au sujet de l'efficacité des activités de gestion des risques lui apportent les informations qu'il désire concernant l'efficacité actuelle de la gestion des risques ;
- déterminer si les informations relatives à la tolérance au risque sont communiquées efficacement et rapidement à la fois par le Conseil à la direction générale et par la direction générale aux propriétaires de risques ;
- déterminer s'il existe des domaines de risques qui ne sont pas couverts actuellement par le processus de gouvernance, alors qu'ils le devraient (par exemple, un risque pour lequel la tolérance et les attentes de reporting n'ont pas été déléguées à un propriétaire de risques précis).

Copyright © 2015 Eyrolles.

Pour pouvoir s'acquitter de ces responsabilités, l'audit interne doit clairement comprendre l'orientation et les attentes du Conseil vis-à-vis de la gouvernance, notamment les seuils de tolérance au risque et les attentes en termes de communication. Le plan d'audit interne doit s'en faire l'écho en intégrant des activités adéquates d'assurance sur la gouvernance et en offrant des opportunités régulières de communication à la direction générale et au Conseil en ce qui concerne l'efficacité des activités de gestion des risques. Reportez-vous au chapitre 3, *La gouvernance,* qui traite ce sujet de manière plus approfondie.

LA GESTION DES RISQUES

Gestion des risques

Processus piloté par le management qui consiste à appréhender et à traiter les incertitudes (risques et opportunités) susceptibles d'affecter la capacité de l'organisation à atteindre ses objectifs.

Selon une définition communément admise, la gestion des risques est un processus participatif destiné à identifier, documenter, évaluer, communiquer et piloter les incertitudes les plus significatives auxquelles une organisation peut être confrontée et nécessitant des mesures de maîtrise des risques ou d'exploitation des opportunités pour que l'organisation puisse atteindre ses objectifs. En d'autres termes, la gestion des risques est un processus piloté par le management qui consiste à appréhender et à traiter les incertitudes (risques et opportunités) susceptibles d'affecter la capacité de l'organisation à atteindre ses objectifs. Le traitement des risques est une mesure ou un ensemble de mesures prises par le management, afin d'accomplir la stratégie de gestion des risques désirée. La mise en œuvre efficace des stratégies de gestion des risques permet au management de réaliser les objectifs de l'organisation en réduisant l'impact potentiel ou la probabilité d'occurrence (ou les deux) d'un risque ou, à l'inverse, en exploitant une opportunité perçue. La maîtrise des risques consiste à atténuer la sévérité ou l'impact potentiel des risques en recourant à des modalités de traitement des risques, sujet qui est étudié au chapitre 4, *La gestion des risques*.

La maîtrise des risques est plus efficace lorsqu'elle est décentralisée aux secteurs les plus affectés par les risques en question. En revanche, l'efficacité de la gestion des risques est la plus grande lorsque cette fonction est centralisée. La gestion des risques est plus efficace lorsque la direction générale est activement engagée dans le processus, de façon à ce que les participants sortent de leur secteur/service et considèrent les risques qui pèsent sur l'organisation dans son ensemble. Malheureusement, de nombreuses organisations commettent l'erreur de laisser la gestion des risques, ainsi que les mesures de maîtrise des risques, se disperser au sein de l'organisation. Par conséquent, les différents responsables de la maîtrise des risques deviennent également responsables des activités de gestion des risques décrites ci-dessus. On aboutit à une situation dans laquelle des risques similaires sont gérés différemment. On débouche sur une incohérence des modalités de traitement des

Copyright © 2015 Eyrolles.

risques et des inefficiences résultant d'une appétence pour le risque différente et de mesures de maîtrise différentes selon les secteurs.

Historiquement, la gestion des risques a pour but de concentrer les efforts sur l'évitement d'un danger potentiel et d'empêcher des actions dommageables d'avoir un impact délétère sur une organisation. Au fil du temps, les modèles de gestion des risques des organisations ont évolué et concentrent désormais leurs efforts non plus seulement sur l'identification des risques susceptibles d'avoir une incidence négative sur l'organisation, mais aussi sur les opportunités pouvant être exploitées. Dans ces modèles, les efforts de gestion des risques visent à faciliter la gestion de ces risques et opportunités dans les limites d'une appétence pour le risque prédéterminée, définie par le Conseil et la direction générale. Une gestion des risques bien exécutée aide le Conseil et la direction générale à mettre en œuvre des modalités de traitement des risques appropriées (évitement, réduction, partage et/ou acceptation des risques, ou exploitation des opportunités) en augmentant la probabilité d'atteindre le résultat escompté (maîtriser un risque ou tirer parti d'une opportunité). Une gestion efficace des risques procure aussi une assurance raisonnable (non absolue) que les objectifs d'une organisation seront atteints.

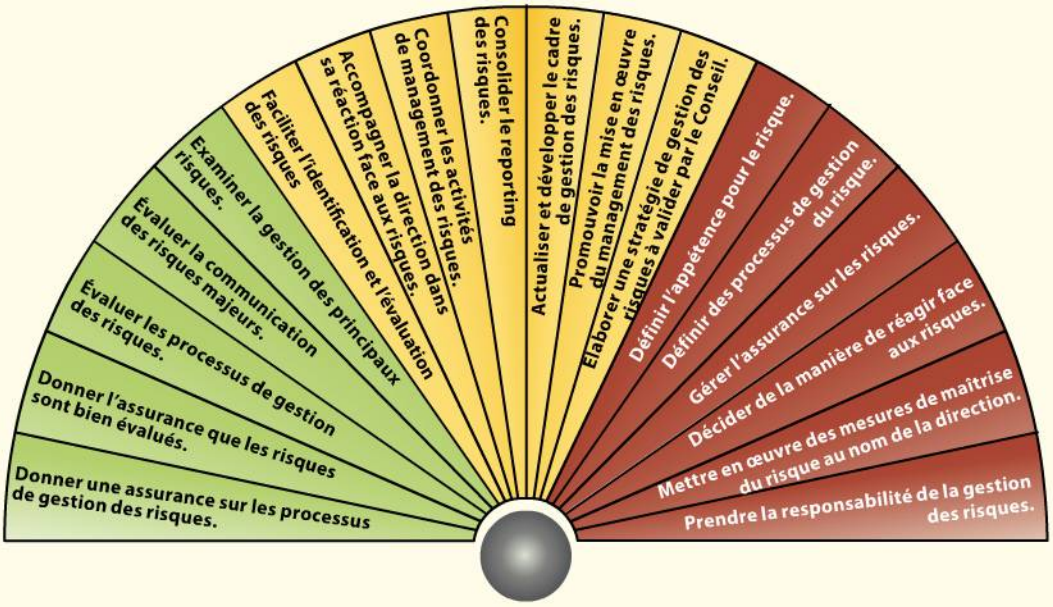
Contrôle

Toute mesure prise par le management, le Conseil et d'autres parties afin de gérer les risques et d'accroître la probabilité que les buts et objectifs fixés seront atteints. Les managers planifient, organisent et dirigent la mise en œuvre de mesures suffisantes pour donner une assurance raisonnable que les buts et objectifs seront atteints.

Comme indiqué plus haut dans le présent chapitre, les résultats d'un processus (modèle) de gestion des risques bien exécuté peuvent aussi constituer une source essentielle permettant d'identifier les facteurs de risque et d'apporter une contribution inestimable pour l'élaboration de l'univers d'audit et du plan d'audit par la fonction d'audit interne. Par conséquent, la gestion des risques est un domaine dans lequel l'audit interne peut et doit jouer un rôle critique. Le degré d'implication de l'audit interne dans le processus de gestion des risques de l'organisation suscite néanmoins de nombreux débats. Même si beaucoup d'organisations sont aujourd'hui dotées d'un service officiellement chargé de la gestion des risques, dont la tâche consiste à piloter et à faciliter les efforts de maîtrise des risques dans toute l'organisation, le rôle de l'audit interne varie fortement et dépend de la division des responsabilités de gestion des risques et de la culture de l'organisation. Au minimum, l'audit interne doit évaluer l'adéquation de la conception et le fonctionnement effectif des processus de gestion des risques de l'organisation en apportant une contribution et un retour d'information *via* une revue (un audit) périodique. L'audit interne doit aussi faciliter l'identification et l'évaluation des risques et opportunités, accompagner le management pour déterminer comment réagir aux risques et opportunités et aider l'organisation à coordonner les activités de gestion des risques. L'audit interne collabore de plus en plus activement avec les autres structures de gestion des risques, non seulement en tant que troisième ligne de maîtrise, mais également en vue de dégager des gains d'efficience pour l'organisation. Il tire ainsi parti des synergies de planification et met à profit les travaux

Copyright © 2015 Eyrolles.

LE RÔLE DE L'AUDIT INTERNE DANS LE MANAGEMENT DES RISQUES DE L'ENTREPRISE



Ce diagramme est extrait de la prise de position intitulée « Le rôle de l'audit interne dans le management des risques de l'entreprise », traduite par l'IFACI, et reproduit avec l'autorisation de l'*Institute of Internal Auditors – United Kingdom and Ireland*. Pour consulter l'intégralité du texte de cette prise de position en anglais, vous pouvez consulter le site www.iia.org.uk. © *The Institute of Internal Auditors – UK and Ireland Ltd.*, juillet 2004.

ENCADRÉ 9-5

d'assurance dans la mesure du possible. Cependant, comme indiqué plus haut, il ne doit pas définir l'appétence pour le risque de l'organisation, prendre des décisions sur les modalités de traitement des risques ni assumer la propriété des processus de gestion des risques (ou avoir à rendre des comptes à son propos). Seul le management doit endosser ces rôles.

D'après la Norme 2120, Management des risques, « l'audit interne doit évaluer l'efficacité des processus de management des risques et contribuer à leur amélioration ». L'interprétation de cette Norme précise :

« Afin de déterminer si les processus de management des risques sont efficaces, les auditeurs internes doivent s'assurer que :

- les objectifs de l'organisation sont cohérents avec sa mission et y contribuent ;
- les risques significatifs sont identifiés et évalués ;

Copyright © 2015 Eyrolles.

- les modalités de traitement des risques retenues sont appropriées et en adéquation avec l'appétence pour le risque de l'organisation ;
- les informations relatives aux risques sont recensées et communiquées en temps opportun au sein de l'organisation pour permettre aux collaborateurs, à leur hiérarchie et au Conseil d'exercer leurs responsabilités.

Les processus de management des risques sont surveillés par des activités de gestion permanente, par des évaluations spécifiques ou par ces deux moyens ».

Concrètement, l'audit interne doit renforcer la gestion et la maîtrise des risques, en apportant un niveau de protection supplémentaire. L'encadré 9-5 présente un éventail d'activités qui sont susceptibles d'être demandées à une fonction d'audit interne, et précise celles qu'elle peut accepter et celles qu'elle doit éviter. Cet encadré a déjà été introduit dans le chapitre 4, *La gestion des risques* (encadré 4-4), où il est examiné plus en détail. Pour plus de précisions sur les responsabilités de l'audit interne concernant la gestion des risques, reportez-vous à la MPA 2120-1, Évaluer la pertinence des processus de management des risques.

Assurance qualité

Processus consistant à donner l'assurance que l'audit interne opère conformément à un ensemble de normes qui définissent les éléments spécifiques qui doivent être présents pour garantir que les constats de l'audit interne sont légitimes.

CONTRÔLE

Selon la Norme 2130, Contrôle : « L'audit interne doit aider l'organisation à maintenir un dispositif de contrôle approprié en évaluant son efficacité et son efficience et en encourageant son amélioration continue. »

S'agissant d'effectuer des activités d'assurance, l'information issue de l'évaluation des risques doit guider l'audit interne lorsqu'il évalue « la pertinence et l'efficacité du dispositif de contrôle choisi pour faire face aux risques relatifs au gouvernement d'entreprise, aux opérations et systèmes d'information de l'organisation. Cette évaluation doit porter sur les aspects suivants :

- l'atteinte des objectifs stratégiques de l'organisation ;
- la fiabilité et l'intégrité des informations financières et opérationnelles [extrafinancières] ;
- l'efficacité et l'efficience des opérations et des programmes ;
- la protection des actifs ;
- le respect des lois, règlements procédures et contrats » (Norme 2130.A1).

Copyright © 2015 Eyrolles.

Par ailleurs, l'audit interne devrait identifier les objectifs du domaine audité et évaluer dans quelle mesure ils sont alignés avec les objectifs de l'organisation. Les missions d'assurance devraient permettre d'évaluer si les dispositifs de contrôle en place contribuent efficacement à la réalisation de ces objectifs.

En outre, la Norme 2130.C1 indique que : « Les auditeurs internes doivent utiliser leurs connaissances des dispositifs de contrôle acquises lors de missions de conseil lorsqu'ils évaluent les processus de contrôle de l'organisation. »

Le contrôle est traité en détail au chapitre 6, intitulé *Le contrôle interne*.

ASSURANCE QUALITÉ ET PROGRAMMES D'AMÉLIORATION

Dans l'environnement actuel de gouvernance, il est devenu impératif que l'audit interne dispose des outils appropriés pour s'autoréglementer et vérifier que les normes professionnelles sont bien respectées. Afin de maintenir des normes cohérentes que devront respecter les fonctions d'audit interne aux fins de l'autoréglementation, l'IIA a défini des normes d'assurance qualité officielles qui doivent être suivies par les fonctions d'audit interne si elles veulent être considérées comme conformes aux *Normes* de l'IIA.

L'assurance qualité est le processus qui consiste à donner l'assurance que l'audit interne respecte un ensemble de normes qui définissent les éléments spécifiques qui doivent être présents pour garantir que le service fonctionne correctement. Plus précisément, selon la Norme 1300, Programme d'assurance et d'amélioration qualité, « le responsable de l'audit interne doit élaborer et tenir à jour un programme d'assurance et d'amélioration qualité portant sur tous les aspects de l'audit interne ». L'interprétation de cette Norme explique que : « un programme d'assurance et d'amélioration qualité est conçu de façon à évaluer la conformité de l'audit interne avec la définition de l'audit interne et les *Normes*, le respect du Code de déontologie par les auditeurs internes. Ce programme permet également de s'assurer de l'efficacité et de l'efficience de l'activité d'audit interne et d'identifier toutes opportunités d'amélioration ».

La Norme 1310, Exigences du programme d'assurance et d'amélioration qualité, la Norme 1311, Évaluations internes – et la Norme 1312, Évaluations externes – détaillent les critères à respecter énoncés dans la Norme 1300 : elles précisent que l'audit interne doit définir des procédures d'évaluation internes et externes. Dans la pratique, les procédures d'évaluation internes sont les mesures d'assurance qualité prises quotidiennement et normalement précisées dans les procédures opérationnelles de l'audit interne (manuel d'audit) qui veillent à ce que les *Normes* soient respectées. Les

Copyright © 2015 Eyrolles.

ENCADRÉ 9-6

LES PROCÉDURES D'ASSURANCE QUALITÉ DE L'AUDIT INTERNE, TELLES QUE DÉCRITES PAR L'IIA

MPA 1311-1 – Évaluations internes

1. Les processus et outils utilisés dans les évaluations internes permanentes sont notamment les suivants :
   - supervision des missions ;
   - utilisation de listes de contrôle et de procédures (par exemple dans un manuel d'audit et de procédures) ;
   - informations fournies, en retour, par les clients et les parties prenantes de l'audit interne ;
   - revues de dossiers de mission effectuées par des auditeurs qui n'ont pas participé aux missions concernées ;
   - budgets par projet, systèmes de suivi des temps passés, réalisation du plan d'audit, recouvrement des coûts ;
   - analyse d'autres indicateurs de performance (par ex. durée des missions et taux de recommandations acceptées).
2. Il convient de conclure sur la qualité des prestations et d'en effectuer un suivi afin de s'assurer que les améliorations appropriées sont mises en œuvre.
3. Le manuel de l'IIA relatif à l'évaluation de la qualité (*Quality Assessment Manual*), ou un ensemble comparable de lignes directrices et d'outils, pourront servir de base aux évaluations internes périodiques.
4. Les évaluations internes périodiques peuvent :
   - comporter des enquêtes et des entretiens plus approfondis avec les parties prenantes de l'audit interne ;
   - être réalisées par les membres de l'audit interne (auto-évaluation) ;
   - être réalisées par des auditeurs internes certifiés CIA ou par d'autres professionnels de l'audit, intervenant dans d'autres départements de l'organisation ;
   - combiner auto-évaluation et préparation de documents revues ultérieurement par des auditeurs internes certifiés CIA ou par d'autres professionnels de l'audit ;
   - inclure une étude comparative des pratiques et des indicateurs de performance de l'audit interne et des meilleures pratiques de la profession.
5. Une évaluation interne périodique, réalisée peu de temps avant une évaluation externe, peut faciliter cette dernière et en réduire le coût. Même si l'évaluation périodique interne est effectuée par des évaluateurs externes qualifiés et indépendants, les résultats de l'évaluation ne devraient pas présumer les résultats de la revue qualité externe à venir. Le rapport peut contenir des suggestions et des recommandations d'amélioration des pratiques d'audit. Si l'évaluation externe prend la forme d'une auto-évaluation suivie d'une validation indépendante, l'évaluation interne périodique peut tenir lieu d'auto-évaluation dans le cadre de ce processus.
6. Il convient de conclure sur la qualité des prestations et prendre toute mesure appropriée pour, en tant que de besoin, mettre en œuvre les améliorations et assurer la conformité aux *Normes*.
7. Le responsable de l'audit interne met en place un système de diffusion des résultats des évaluations internes permettant de préserver la crédibilité du service et de garantir son objectivité. En règle générale, les personnes chargées des évaluations continues et périodiques rendent compte au responsable de l'audit interne au cours de leurs revues et lui adressent directement leurs résultats.
8. Le responsable de l'audit interne rend compte, au moins annuellement, à la direction générale et au Conseil des résultats des évaluations internes, des plans d'action à mettre en œuvre et de leur mise en œuvre effective.

Copyright © 2015 Eyrolles.

PROCÉDURES D'ASSURANCE QUALITÉ PAR AUTO-ÉVALUATION DE L'AUDIT INTERNE POUR LES FONCTIONS DE TAILLE RESTREINTE, TELLES QUE DÉCRITES PAR L'IIA

MPA 1312-2 – Évaluations externes : auto-évaluation avec validation indépendante

1. Une évaluation externe périodique, réalisée par un évaluateur ou une équipe d'évaluateurs compétents et indépendants, peut être problématique pour les services d'audit interne de taille modeste ou considérée comme n'étant pas vraiment appropriée ou nécessaire dans d'autres organisations. Par exemple, le service d'audit interne peut (a) appartenir à un secteur extrêmement régulé, (b) faire par ailleurs l'objet d'une supervision externe importante en matière de gouvernance et de contrôle interne, (c) avoir récemment fait l'objet d'évaluations externes et/ou de services de conseil aux cours desquels il y a eu un benchmark approfondi avec les meilleures pratiques, ou (d) du point de vue du responsable d'audit interne, l'intérêt pour le développement des auditeurs et le renforcement du programme d'assurance et d'amélioration qualité surpasse actuellement l'intérêt d'une revue qualité par une équipe externe.
2. Une auto-évaluation avec validation (externe) indépendante comporte les éléments suivants :
   - un processus détaillé et parfaitement documenté d'auto-évaluation, comparable au processus d'évaluation externe, du moins en ce qui concerne l'évaluation du respect de la définition de l'audit interne, du Code de déontologie et des *Normes* ;
   - une validation sur site indépendante réalisée par un évaluateur qualifié ;
   - des modalités économiques en termes de temps et de ressources, l'accent étant mis, par exemple, sur le respect des *Normes* ;
   - les autres points, tels que l'analyse comparative, l'examen et les consultations relatifs à l'emploi des meilleures pratiques, les entretiens avec la direction générale et les cadres opérationnels peuvent faire l'objet d'une attention réduite. Cependant, les informations obtenues par ces points sont parmi les plus bénéfiques lors d'une évaluation externe.
3. Les conditions et critères décrits dans la MPA 1312-1 s'appliquent en ce qui concerne :
   - les considérations d'ordre général ;
   - les qualifications de l'évaluateur ou de l'équipe d'évaluateurs externes ;
   - l'indépendance, l'intégrité et l'objectivité, la compétence, l'approbation du choix de l'intervenant par la direction générale et le Conseil, l'étendue de la mission (sauf pour des domaines comme les outils et techniques utilisés, les autres meilleures pratiques, l'évolution de carrière et les activités à valeur ajoutée) ;
   - la communication des résultats (y compris des actions correctrices et de leur mise en œuvre).
4. Le processus d'auto-évaluation est mis en œuvre et parfaitement documenté par une équipe dirigée par le responsable de l'audit interne. Un projet de rapport similaire à celui concernant l'évaluation externe est établi avec l'opinion du responsable du service d'audit concernant le respect des *Normes*.
5. L'évaluateur ou l'équipe d'évaluateurs compétent(s) et indépendant(s) chargé(s) de la validation procèdent à des tests sur l'auto-évaluation, de façon à en valider les résultats et à formuler une opinion sur le respect de la définition de l'audit interne, du Code de déontologie et des *Normes*. La validation indépendante suit le processus décrit dans le Manuel d'évaluation qualité (*Quality Assessment Manual*) de l'IIA ou un processus comparable détaillé.
6. Au cours de la validation indépendante, qui inclut un examen rigoureux de l'évaluation du respect de la définition de l'audit interne, du Code de déontologie et des *Normes*, l'évaluateur externe indépendant :
   - examine le projet de rapport et s'efforce, le cas échéant, de résoudre les points en suspens ;
   - en cas d'accord avec l'opinion concernant le respect de la définition de l'audit interne, du Code de déontologie et des *Normes*, il complète le rapport (s'il y a lieu), afin d'approuver le processus d'auto-évaluation et l'opinion exprimée par le responsable de l'audit, ainsi que les constatations, conclusions et recommandations (s'il le juge opportun) ;
   - en cas de désaccord avec cette évaluation, il fait part de son désaccord dans le rapport en précisant les points de divergence avec ce dernier et, s'il le juge opportun, avec les constatations, conclusions et recommandations significatives qu'il contient ;
   - peut également établir un rapport de validation indépendante séparé, mentionnant son accord ou son désaccord comme indiqué ci-dessus, à joindre au rapport d'auto-évaluation.
7. Le(s) rapport(s) final(s) de l'auto-évaluation avec validation indépendante sont ensuite signé(s) par l'équipe chargée de l'auto-évaluation et la personne compétente responsable de la validation indépendante, puis diffusé(s) à la direction générale et au Conseil par le responsable de l'audit interne.
8. Dans le but d'assurer la crédibilité et la transparence, le responsable de l'audit interne communique aux différentes parties prenantes de l'audit interne, telles que la direction générale, le Conseil et les auditeurs externes, les résultats de l'évaluation, y compris les actions correctrices prévues sur les points significatifs, puis des informations concernant leur mise en œuvre.

Copyright © 2015 Eyrolles.

procédures d'évaluation externes sont les mesures d'assurance qualité qu'un tiers compétent et indépendant a prises ou que l'audit interne a prises et fait vérifier par un tiers compétent et indépendant. Ce processus est généralement connu sous le nom d'« examen par des pairs indépendants ». L'audit interne doit faire réaliser une évaluation externe périodique (au moins une fois tous les cinq ans) visant à confirmer qu'il respecte les *Normes*. Les procédures d'évaluation interne et externe doivent avoir été mises en place et être respectées pour que l'audit interne puisse affirmer que ses missions d'assurance et de conseil sont « conduites conformément aux *Normes internationales pour la pratique professionnelle de l'audit interne* » (Norme 1321, Utilisation de la mention « conforme aux *Normes internationales pour la pratique professionnelle de l'audit interne* »). L'encadré 9-6 présente les procédures d'assurance qualité d'une fonction d'audit interne, telles que suggérées dans la Modalité Pratique d'Application 1311-1, Évaluations internes.

Tandis que les Normes 1300, 1310, 1311 et 1312 génèrent peu d'ambiguïté, en particulier lorsqu'elles sont explicitées par les Modalités Pratiques d'Application requises, les questions concernant la mise en œuvre de ces normes font débat chez les professionnels de l'audit interne. Les fonctions d'audit interne de taille importante disposent généralement des moyens nécessaires pour faire appel à des sources externes qui réalisent l'évaluation externe requise pour se conformer à la Norme 1312. Lors du processus de sélection, il convient toutefois de veiller à ce que l'indépendance de l'équipe d'évaluation externe ne soit pas compromise. Les MPA 1312-3 et 1312-4 apportent des précisions quant à la manière dont les organisations du secteur privé ou public peuvent s'assurer que l'équipe d'évaluation externe demeure indépendante. Par ailleurs, l'application de la Norme 1312 peut se révéler très onéreuse, en particulier pour les fonctions d'audit interne de taille restreinte. Si la MPA 1312-2, Évaluations externes : auto-évaluation avec validation indépendante, tente de répondre à cette préoccupation, en prévoyant la possibilité de réaliser une auto-évaluation avec validation indépendante, et s'il est généralement possible d'atteindre un consensus sur le plan des principes, les problèmes apparaissent lorsque les professionnels tentent de définir ce qu'est une fonction d'audit interne de taille restreinte : ce terme devient relatif suivant la taille de la fonction qui le définit. L'encadré 9-7 présente une autre possibilité pour les fonctions d'audit interne de taille restreinte qui estiment que les procédures d'évaluation externe de l'assurance qualité sont trop onéreuses.

Étant donné que ni les *Normes* ni les Modalités Pratiques d'Application n'opèrent de distinction entre les fonctions qui sont principalement exécutées par des ressources internes et celles qui proviennent principalement de l'extérieur (externalisation ou co-traitance), le débat se poursuit sur l'applicabilité des *Normes* et sur la meilleure manière de s'y conformer lorsque la fonction est largement externalisée.

Copyright © 2015 Eyrolles.

Les impératifs associés à un programme d'assurance et d'amélioration qualité bien conçu sont expliqués dans l'encadré 9-8.

ENCADRÉ 9-8

EXIGENCES DU PROGRAMME D'ASSURANCE ET D'AMÉLIORATION QUALITÉ

MPA 1310-1 – Exigences du programme d'assurance et d'amélioration qualité

1. Un programme d'assurance et d'amélioration qualité consiste en des évaluations permanentes ou périodiques de l'ensemble des prestations d'audit et de conseil effectuées par l'audit interne. Ces évaluations permanentes ou périodiques reposent sur des processus rigoureux et détaillés, une supervision continue et la vérification des prestations d'audit et de conseil, ainsi que des validations périodiques du respect de la définition de l'audit interne, du Code de déontologie et des *Normes*. Ce suivi comporte une évaluation et une analyse continues d'indicateurs de performances (réalisation du plan d'audit interne, durée des missions, recommandations acceptées et satisfaction des clients, par exemple). Si, suite à ces évaluations, il apparaît que des améliorations sont à apporter par l'audit interne, le responsable de l'audit interne les mettra en œuvre dans le cadre du programme d'assurance et d'amélioration qualité.
2. Les évaluations donnent une opinion sur la qualité des travaux d'audit interne et aboutissent à des recommandations en vue de leur amélioration. Les programmes qualité comportent notamment une évaluation des points suivants :
   - respect de la définition de l'audit interne, du Code de déontologie et des *Normes*, et notamment mise en œuvre, dans des délais appropriés, d'actions correctrices visant à remédier à toute non-conformité significative ;
   - caractère adéquat de la charte d'audit interne, des objectifs, des règles et des procédures de l'audit interne ;
   - contribution aux processus de gouvernement d'entreprise, de management des risques et de contrôle de l'organisation ;
   - respect des lois, réglementations, normes administratives ou sectorielles en vigueur ;
   - efficacité des processus d'amélioration continue et adoption des meilleures pratiques ;
   - contribution de l'audit interne à la création de valeur et à l'amélioration du fonctionnement de l'organisation.
3. Le programme d'assurance et d'amélioration qualité inclut également le suivi des recommandations relatives à la modification appropriée et opportune des ressources, des technologies, des processus et des procédures.
4. Par souci de transparence, le responsable de l'audit interne communique les résultats des évaluations externes et, si nécessaire, des évaluations internes du programme qualité, aux diverses parties prenantes de l'audit interne, telles que la direction générale, le Conseil et les auditeurs externes. Au moins une fois par an, le responsable de l'audit interne rend compte à la direction générale et au Conseil de l'état d'avancement et des résultats du programme qualité.

Indication de non-conformité

Si l'on constate que l'audit interne est suffisamment déficient, au point d'avoir « une incidence sur le champ d'intervention ou sur le fonctionnement de l'audit interne », la Norme 1322, Indication de non-conformité, précise que « le responsable de l'audit interne doit informer la direction générale et le Conseil de cette non-conformité

Non-conformité aux *Normes*

Situation qui survient lorsque l'on constate que l'audit interne est déficient, au point d'avoir une incidence sur le champ d'intervention ou sur le fonctionnement de l'audit interne. Il est impératif de signaler la non-conformité.

Copyright © 2015 Eyrolles.

Programme d'assurance et d'amélioration qualité

Évaluations permanentes ou périodiques de l'ensemble des prestations d'audit et de conseil effectuées par l'audit interne.

et de ses conséquences ». À ce moment-là, on détermine généralement si la non-conformité est intentionnelle ou involontaire, si une action corrective est prévue, et si oui laquelle. Si la direction générale et le Conseil décident de ne pas entreprendre d'action corrective et que l'audit interne reste non conforme, celui-ci ne pourra plus affirmer que ses activités d'assurance et de conseil sont « conduites conformément aux *Normes internationales pour la pratique professionnelle de l'audit interne* » (Norme 1321). S'il continue de proposer des activités d'assurance et de conseil qui ne sont pas réalisées conformément aux *Normes*, cela pourrait avoir des conséquences étendues, susceptibles de gêner considérablement la relation de l'audit interne avec les tiers intéressés comme les autorités de régulation et de supervision et les autres tiers (aux États-Unis, la *Securities and Exchange Commission* [SEC], le cabinet d'audit externe auquel fait appel l'organisation, par exemple).

Commentaire du traducteur

Toutes les grandes places financières ont un « gendarme de la bourse ». Par exemple, l'Autorité des marchés financiers (AMF) en France ou les Autorités canadiennes en valeurs mobilières (ACVM). Il existe également des superviseurs sectoriels tels que la Banque centrale européenne (dans le cadre du mécanisme de surveillance unique) et l'Autorité de contrôle prudentiel et de résolution pour la banque et l'assurance en France.

Auto-évaluation des contrôles

Processus par lequel les propriétaires des contrôles effectuent une auto-évaluation de l'adéquation de la conception et du fonctionnement effectif des contrôles dont ils sont responsables.

LES INDICATEURS DE PERFORMANCE POUR L'AUDIT INTERNE

Les indicateurs de performance font partie intégrante de l'obligation d'évaluation interne décrite par la Norme 1311, Évaluations internes (voir précédemment). En plus de fournir les critères sur la base desquels l'audit interne évalue ses performances dans les principaux domaines, ils permettent de juger de l'efficacité avec laquelle l'audit interne remplit sa mission/ses objectifs. Le responsable de l'audit interne doit tenir compte de nombreux facteurs lorsqu'il définit des indicateurs de performance (taille de la fonction d'audit interne, services proposés, normes sectorielles, environnement dans lequel opère l'organisation et culture de cette dernière). Les indicateurs de performance doivent correspondre à la charte d'audit interne, et toutes les fonctions importantes mentionnées dans la charte doivent être prises en compte lors de la définition des indicateurs de performance. Le processus de mesure doit décrire les activités qui contribuent à la réalisation des objectifs définis dans la charte.

Copyright © 2015 Eyrolles.

LA PLACE DE LA TECHNOLOGIE DANS LE PROCESSUS D'AUDIT INTERNE

La technologie tient une place de plus en plus importante dans le processus d'audit interne. De plus en plus d'outils technologiques permettent aux auditeurs internes d'accroître leur productivité et leur efficience, et de passer moins de temps à des tâches administratives, pour se consacrer davantage aux activités d'assurance et de conseil réalisées pour le compte des audités et des clients. Compte tenu des progrès technologiques actuels, il peut être difficile de ne pas se laisser détourner de ses objectifs par la course au progrès, et il est important de garder à l'esprit que la technologie doit améliorer la productivité de l'audit interne, et de ne pas perdre l'audit de vue.

Outre la réduction du temps consacré aux tâches administratives, les outils technologiques doivent également accroître la productivité des missions d'audit interne, car ils réduisent le temps passé à rassembler des documents, à les classer, à les archiver et à y accéder. Trois de ces outils ont été intégrés dans le présent manuel. TeamMate est un outil de documentation et de gestion de l'audit. Il peut être utilisé dans le cadre d'exercices et d'études de cas présentés dans les chapitres concernés de ce manuel. ACL et IDEA sont des outils classiques d'analyse de données. Ils ont été intégrés dans ce manuel afin que les étudiants puissent se familiariser avec les outils utilisés dans la pratique de l'audit interne.

Auto-évaluation des risques et des contrôles

Il doit être clair, à ce stade, que l'audit interne aide l'organisation à évaluer et à maîtriser les risques de plusieurs manières, notamment en mettant en place des équipes et des procédures d'auto-évaluation. En général, ces équipes travaillent avec le management, afin d'effectuer les recherches et les entretiens préliminaires permettant de repérer les risques ou les scénarios potentiels pour une organisation. Elles réunissent les représentants de la direction générale, afin de discuter de ces risques potentiels et de les hiérarchiser. On recourt de plus en plus souvent à des outils de vote qui peuvent s'avérer utiles pour hiérarchiser les risques en offrant au management la possibilité de faire part de son avis sur l'impact et la probabilité d'un risque donné tout en restant anonyme. Il s'ensuit généralement des réponses plus honnêtes, puisque les différents participants à la réunion ne sont pas influencés les uns par les autres. Une fois les risques identifiés et hiérarchisés, l'audit interne continue d'aider le management à définir, documenter, évaluer, communiquer et réduire la gravité (c'est-à-dire l'impact et la probabilité) potentielle des risques associés aux principaux facteurs de risques qui ont été identifiés. L'utilisation de la technologie (base de données et outils de suivi) peut être utile aux équipes, qui peuvent ainsi attribuer les différents scénarios aux personnes

Audit continu

Recours à des techniques informatisées qui permettent d'auditer en permanence le traitement des transactions d'une organisation.

Copyright © 2015 Eyrolles.

qui sont les mieux armées pour gérer et maîtriser les risques qui préoccupent le management. La base de données peut alors servir à documenter et à suivre les efforts d'établissement du plan d'action et de maîtrise des risques convenus avec le management. Sans la technologie moderne, les efforts d'auto-évaluation seraient lourds, inefficients et très difficiles à gérer. L'auto-évaluation peut servir de manière autonome pour évaluer le risque dans divers domaines ou processus d'une organisation, ou comme un outil efficace pour appuyer l'évaluation des risques dans toute l'organisation.

Au niveau administratif, les outils automatisés d'évaluation des risques peuvent doter l'audit interne d'une base de données qui permet d'identifier les risques, de les documenter et de les hiérarchiser, de déterminer quels services de l'organisation sont concernés par ces risques, et de concevoir des contrôles clés, afin de gérer ou de maîtriser ces risques. Ces outils documentent également l'univers d'audit et rassemblent des informations sur les différents services qui interviennent dans cet univers. Ils sont utilisés pour évaluer les risques spécifiques liés à ces services. Ces outils permettent en outre de hiérarchiser les risques liés à chaque service et ainsi de fixer la fréquence de l'audit y afférent. La hiérarchisation de l'univers d'audit qui en découle détermine donc le budget, la planification, le plan d'audit et les ressources nécessaires, comme indiqué plus haut dans ce chapitre.

De nombreuses organisations appliquent les techniques décrites ci-dessus aux contrôles d'auto-évaluation. Dans ces situations, les propriétaires des processus et des contrôles mettent en œuvre des techniques qui les aident à évaluer l'adéquation de la conception et le fonctionnement effectif des contrôles dont ils sont responsables. Ces techniques, qui peuvent être facilitées par l'audit interne, incluent notamment l'utilisation de la technologie, comme indiqué plus haut.

Analyse des données

L'auditeur interne a souvent à examiner d'importants volumes de données. Cette tâche peut se révéler très difficile, prendre beaucoup de temps et nécessiter des compétences spécialisées si l'on n'utilise pas l'informatique. De nombreux services d'audit interne ont créé des fonctions spécialisées qui contribuent à ces efforts. Ces fonctions ont été analysées plus en détail précédemment dans ce chapitre. De même, l'échantillonnage risque de ne pas être efficace, pratique et peut parfois être écarté. Il peut également limiter la capacité de l'auditeur interne à tirer des conclusions définitives. Dans ces cas, les outils et les techniques d'analyse des données peuvent se révéler incontournables, car ils permettent de tout vérifier et d'aboutir à des résultats et des conclusions définitifs. De plus, ces outils et ces techniques peuvent également contribuer aux efforts d'audit continu, de pilotage continu et/ou de détection et de

Copyright © 2015 Eyrolles.

prévention de la fraude. Pour de plus amples détails sur les techniques d'audit informatisées et l'échantillonnage, il est possible de se reporter aux chapitres 10, *Les preuves d'audit et les papiers de travail*, et 11, *L'échantillonnage en audit*.

ENCADRÉ 9-9

APPORTER SON POINT DE VUE GRÂCE À UNE GESTION EFFICACE DE SON SERVICE OPPORTUNITÉS POUR L'AUDIT INTERNE

- Élaborer une charte qui apporte à l'organisation un retour d'information indépendant et objectif qui lui permette d'améliorer ses opérations en optimisant l'efficacité et l'efficience des processus de gestion des risques, de contrôle et de gouvernance.
- Coordonner les activités d'assurance avec les autres prestataires internes et externes afin d'assurer une couverture adéquate, d'éviter les doubles emplois et de minimiser les coûts.
- Aider l'organisation à développer et à mettre en œuvre des stratégies efficaces de gestion des risques, qui permettent au management de réaliser les objectifs en réduisant l'impact ou la probabilité d'occurrence des risques.
- Aider l'organisation à mettre en place et à maintenir un dispositif de contrôle approprié en évaluant son efficacité et son efficience et en encourageant son amélioration continue.
- Collaborer avec le management afin de mettre en place des activités d'auto-évaluation conçues pour contribuer aux efforts de gestion des risques de l'organisation.

Le pilotage automatisé

De même que les outils d'interrogation des données, les outils de pilotage automatisés permettent à l'audit interne d'effectuer plus efficacement ses missions d'audit continu en donnant aux auditeurs internes la possibilité d'évaluer de gros volumes de données (informations), ce qui ne serait pas possible ou aisé autrement. Contrairement aux audits périodiques, l'audit continu « désigne toute méthode utilisée par [les auditeurs] pour accomplir leurs activités d'audit de manière plus continue ou continuelle. »[1] L'audit continu vient souvent soutenir ou compléter les processus périodiques d'audit, d'évaluation des contrôles et d'évaluation des risques. Les outils de pilotage automatisés peuvent également faciliter les efforts de communication de l'audit interne en procurant des informations en « quasi » temps réel à propos de l'efficacité des activités de pilotage continu déployées par le management. La disponibilité d'informations actualisées sur l'adéquation de la conception et le fonctionnement effectif des contrôles peut aider l'audit interne à réévaluer ses priorités pour les activités d'assurance et de conseil, et ainsi maximiser la couverture de l'univers d'audit interne. Grâce à ces outils, l'audit interne est mieux à même d'apporter des services à valeur ajoutée, tout en gérant ses ressources humaines et ses moyens financiers de la manière la plus efficiente possible.

Copyright © 2015 Eyrolles.

Papiers de travail automatisés

Les papiers de travail automatisés améliorent la productivité de l'audit interne, car ils procurent un support plus efficient pour documenter, examiner, archiver et accéder aux informations qui étayent les travaux d'audit réalisés (activités d'assurance et de conseil). L'amélioration de la productivité permet de consacrer davantage de temps aux travaux d'audit plutôt qu'à la documentation, au stockage et à la recherche des informations. Les papiers de travail automatisés sont également utilisés comme bases de données où trouver les documents attestant de la conformité aux normes professionnelles et de la conscience professionnelle.

Administration et gestion du service

La plupart des activités nécessaires pour gérer l'audit interne, y compris les évaluations des collaborateurs, le suivi du temps et des charges et la planification des missions, peuvent désormais être effectuées électroniquement. En réalité, nombre de ces activités, si ce n'est toutes, peuvent être réalisées avec les outils qui permettent d'élaborer les procédures d'évaluation des risques et les papiers de travail automatisés. L'audit interne peut ainsi être géré de façon bien plus efficiente. En général, plus le nombre d'activités possibles avec un outil est élevé, plus il est efficient et rentable d'employer cet outil. Lorsqu'il n'est pas possible de choisir un outil qui accomplit toutes ces activités, il est judicieux de choisir des outils qui peuvent interagir (communiquer) facilement. Nombre des outils disponibles aujourd'hui présentent un rapport coût/efficacité suffisant pour être utilisables par des organisations de toutes tailles.

Internet

Outre les outils d'audit précités, Internet peut être un outil efficace s'il est utilisé correctement. Internet permet d'effectuer des recherches et d'accéder plus rapidement aux informations qu'il fallait auparavant localiser sur papier. Un nombre croissant de fonctions d'audit interne utilisent Internet et Intranet pour améliorer la planification et la prestation de services et accéder aux programmes de travail, aux papiers de travail, aux règles, aux procédures et à d'autres outils et ressources d'audit, ce qui accroît leur efficience et leur productivité.

Copyright © 2015 Eyrolles.

OPPORTUNITÉS POUR UN POINT DE VUE DE L'AUDIT INTERNE

Il est crucial que l'audit interne soit géré de manière efficace pour aider la direction générale à atteindre les objectifs de l'entité. L'encadré 9-9 décrit les opportunités de l'audit interne pour apporter son point de vue grâce à une gestion efficace de son service.

RÉSUMÉ

Ce chapitre a présenté les différentes visions de la place de l'audit interne au sein d'une organisation, ainsi que les avantages et les inconvénients de chaque solution. Il a défini et étudié les rôles et responsabilités des principales fonctions de l'audit interne. Il a également décrit les règles et les procédures de l'audit interne, ainsi que la façon dont elles orientent l'audit interne. Il a examiné différents modèles de gestion des risques, ainsi que le rôle que doit tenir l'audit interne dans les processus de gestion des risques de l'organisation. Il a aussi traité des responsabilités de l'audit interne en matière de gouvernance, proposant des exemples qui montrent comment ces responsabilités peuvent être assumées. Il a expliqué les exigences d'assurance qualité, telles que définies par l'IIA, ainsi que leur importance pour l'audit interne. Il a enfin exposé en détail les avantages à tirer de l'informatique, en particulier pour la gestion de l'audit interne. Il doit être clair que la gestion d'une fonction d'audit interne est une activité complexe, qui requiert une bonne dose de jugement de la part du responsable de l'audit interne. C'est pourquoi il est impératif que celui-ci fasse usage des outils à sa disposition, en particulier des orientations formulées par l'IIA, et que l'audit interne soit doté, à tous les niveaux, de collaborateurs compétents et avertis, à même d'aider le responsable de l'audit interne à effectuer, pour l'organisation, des activités d'assurance et de conseil créatrices de valeur ajoutée et qui soutiennent la direction générale dans la réalisation des objectifs de l'organisation.

Copyright © 2015 Eyrolles.

Questions de révision

1. Quels avantages y a-t-il à positionner le responsable de l'audit interne au niveau de la direction générale d'une organisation ?

2. Quelles informations devraient être contenues dans la charte d'audit interne ?

3. D'après l'interprétation de la Norme 2000, le responsable de l'audit interne a trois grandes responsabilités de gestion. Quelles sont-elles ?

4. Quelles sont les différences entre l'indépendance dans l'organisation et l'objectivité individuelle ?

5. Dans quelles circonstances l'indépendance de l'audit interne et l'objectivité de l'auditeur interne pourraient-elles être menacées ? Comment une telle atteinte à l'indépendance ou à l'objectivité devrait-elle être traitée ?

6. Les missions d'audit interne doivent être conduites avec compétence et conscience professionnelle. Que signifient les termes « compétence » et « conscience professionnelle » ?

7. Le responsable de l'audit interne peut recourir à de multiples approches pour élaborer un plan annuel d'audit interne. Comment une approche descendante fondée sur les risques est-elle mise en œuvre ?

8. Le responsable de l'audit interne est tenu de soumettre le plan d'audit interne à l'approbation de la direction générale et du Conseil. Quelles informations spécifiques devraient leur être communiquées ?

9. Quels éléments clés doivent être pris en compte pour déterminer la façon de gérer les ressources dans une fonction d'audit interne ?

10. Quelle est la différence entre une fonction d'audit interne à structure horizontale et une fonction à structure hiérarchique, et quels sont les avantages et les inconvénients de chacune ?

11. Quels sont les différents postes au sein d'une fonction d'audit interne à structure hiérarchique, et quelles sont les principales responsabilités de chacun ?

12. Quelles sont les lignes de maîtrise de la stratégie d'assurance par niveaux qui constituent le « modèle des trois lignes de maîtrise » ?

13. Quels sont les sujets abordés lors des sessions de coordination réunissant les auditeurs externes et l'audit interne ?

Copyright © 2015 Eyrolles.

Questions de révision

14. Quelles sont les responsabilités du responsable de l'audit interne lorsqu'il rend compte au comité d'audit ?

15. Quelles sont les responsabilités du responsable de l'audit interne et de la fonction d'audit interne en matière de gouvernance de l'organisation ?

16. Quelle est la différence entre maîtrise des risques et gestion des risques ?

17. Selon l'IIA, comment une fonction d'audit interne détermine-t-elle l'efficacité des processus de gestion des risques ?

18. Comment l'audit interne aide-t-il l'organisation à maintenir des contrôles efficaces ?

19. Pourquoi est-il important qu'une fonction d'audit interne dispose d'un programme d'assurance et d'amélioration qualité efficace ? Quels aspects de l'audit interne une évaluation du programme qualité devrait-elle couvrir ?

20. Comment la technologie peut-elle permettre d'accroître la productivité et l'efficacité du processus d'audit interne ?

Copyright © 2015 Eyrolles.

Questions à choix multiples

Sélectionnez la meilleure réponse pour chacune des questions suivantes.

1. Conformément aux *Normes* de l'IIA, les fonctions d'audit interne :
   a. Doivent établir des évaluations internes du programme d'assurance et d'amélioration qualité.
   b. Doivent établir des évaluations externes du programme d'assurance et d'amélioration qualité.
   c. Doivent établir des évaluations à la fois internes et externes du programme d'assurance et d'amélioration qualité.
   d. Ne doivent établir aucune évaluation interne ou externe du programme d'assurance et d'amélioration qualité.

2. La direction générale a demandé à l'audit interne de réaliser un examen opérationnel des opérations de télémarketing d'une grande division et de recommander des procédures et des mesures destinées à améliorer le contrôle exercé par le management. L'audit interne doit :
   a. Accepter la mission d'audit, car son indépendance ne sera pas menacée.
   b. Accepter la mission, mais indiquer au management que le fait de recommander des contrôles compromettrait l'indépendance de l'audit, afin que le management sache que les audits futurs de ce domaine seront compromis.
   c. Refuser la mission parce que l'audit interne est censé posséder une expertise des contrôles comptables et non des contrôles du marketing.
   d. Refuser la mission parce que le fait de recommander des contrôles compromettrait l'objectivité future du service vis-à-vis du service client.

3. Qui doit, en fin de compte, déterminer que les objectifs d'une mission d'audit interne ont bien été atteints ?
   a. Un membre du service d'audit interne.
   b. Le responsable de l'audit interne.
   c. Le comité d'audit.
   d. Le superviseur de la mission d'audit interne.

4. Parmi les raisons suivantes, laquelle justifie le plus que le responsable de l'audit interne tienne compte du plan stratégique de l'organisation lorsqu'il élabore son plan annuel d'audit interne ? La volonté…
   a. de souligner l'importance de l'audit interne pour l'organisation.
   b. d'énoncer des recommandations visant à améliorer le plan stratégique.
   c. de s'assurer que le plan d'audit interne soutient les objectifs globaux.
   d. de donner l'assurance que le plan stratégique correspond aux valeurs de l'organisation.

Copyright © 2015 Eyrolles.

Questions à choix multiples

5. Selon les *Normes*, des règles et des procédures doivent guider les collaborateurs du service d'audit interne. Parmi les affirmations suivantes, laquelle est fausse à cet égard ?
   a. Une fonction d'audit interne de taille restreinte peut être gérée de manière informelle *via* une supervision étroite et des notes de service.
   b. Toutes les fonctions d'audit interne n'ont pas besoin de manuels d'audit technique et administratif.
   c. Le responsable de l'audit interne doit définir les règles et les procédures du service.
   d. Toutes les fonctions d'audit interne doivent posséder un manuel détaillé de règles et de procédures.

6. Alors qu'elle mène une mission de conseil afin d'améliorer l'efficience et la qualité d'un processus de production, l'équipe d'audit se heurte à une limite de l'étendue de l'examen car plusieurs mois de données de production ont été perdus ou sont incomplets. Dans une telle situation, que doit faire le responsable de l'audit interne ?
   a. Renoncer à sa mission de conseil et mener un audit afin de déterminer les raisons pour lesquelles plusieurs mois de données ne sont pas disponibles.
   b. Discuter du problème avec le client et évaluer ensemble si la mission doit être poursuivie.
   c. Accroître la fréquence des audits portant sur l'activité en question.
   d. Signaler les effets potentiels de la limite de l'étendue de l'examen au comité d'audit.

7. Parmi les propositions suivantes, laquelle n'est pas une obligation incombant au responsable de l'audit interne ?
   a. Communiquer à la direction générale et au Conseil, en vue de leur examen et de leur approbation, les plans et les ressources nécessaires à l'audit interne.
   b. Superviser l'établissement, l'administration et l'évaluation du système de contrôle interne et les processus de gestion des risques de l'organisation.
   c. Vérifier que le management a pris les bonnes mesures concernant les risques significatifs signalés dans les rapports d'audit interne.
   d. Définir un plan axé sur les risques afin de réaliser les objectifs de l'audit interne conformément aux objectifs de l'organisation.

Copyright © 2015 Eyrolles.

8. Selon les *Normes*, le responsable de l'audit interne doit communiquer des informations et coordonner des activités avec d'autres prestataires de services d'assurance internes et externes. Concernant l'auditeur externe, laquelle des propositions suivantes ne constitue pas une manière appropriée de remplir cette obligation pour le responsable de l'audit interne ?
   a. Organiser une réunion entre le responsable de l'audit interne et le cabinet d'audit externe afin de discuter du prochain audit des états financiers.
   b. Donner à l'auditeur externe accès aux papiers de travail pour un audit des fournisseurs extérieurs.
   c. Demander que l'auditeur externe obtienne l'aval du responsable de l'audit interne concernant son plan annuel d'audit relatif à l'audit des états financiers.
   d. Demander à ce que l'audit interne reçoive une copie de la lettre de recommandation de l'auditeur externe.

Copyright © 2015 Eyrolles.

Thèmes de discussion

1. Comment les normes professionnelles de l'IIA sur les programmes d'assurance et d'amélioration qualité (Norme 1300) s'appliquent-elles à une fonction d'audit interne intégralement externalisée ? Développez en particulier le caractère applicable et les obligations de conformité aux procédures d'évaluation externe (Norme 1312).

2. Présentez les diverses possibilités permettant de positionner correctement une fonction d'audit interne au sein d'une organisation, ainsi que les avantages et les inconvénients de chacune. Quels sont les principaux facteurs qu'une organisation doit prendre en compte lorsqu'elle met en place une fonction d'audit interne ? Où cette fonction doit-elle se positionner au sein d'une organisation ?

3. Le responsable de l'audit interne doit-il donner son assentiment sur l'adéquation de la conception et/ou le fonctionnement effectif du système de contrôle interne relatif :
   a. à la fiabilité du reporting financier ? Pourquoi ?
   b. à l'efficacité et à l'efficience des opérations ? Pourquoi ?
   c. à la conformité aux lois et règlements applicables ? Pourquoi ?

4. De nombreuses organisations ont mis en œuvre des stratégies de niveaux d'assurance pour ramener les risques auxquels elles sont confrontées à un niveau acceptable. Le modèle des trois lignes de maîtrise est l'une de ces stratégies.
   a. Décrivez les première et deuxième lignes de maîtrise incluses dans ce modèle.
   b. Indiquez ce qui distingue la troisième ligne de maîtrise des deux premières.
   c. Expliquez comment les trois lignes de maîtrise sont coordonnées.
   d. Citez les sources externes d'assurance que les organisations utilisent pour renforcer leurs lignes de maîtrise internes.

5. Conformément aux *Normes* de l'IIA, les fonctions d'audit interne doivent évaluer et contribuer à l'amélioration des processus de gouvernance, de gestion des risques et de contrôle de l'organisation.
   a. Citez plusieurs exemples de responsabilités relatives au processus de gouvernance qu'une fonction d'audit interne peut assumer.
   b. Décrivez :
   - les activités de gestion des risques qu'une fonction d'audit interne peut réaliser ;
   - celles qu'elle devrait éviter.

   c. Les fonctions d'audit interne sont tenues d'évaluer l'adéquation de la conception et le fonctionnement effectif des contrôles. Indiquez les domaines de contrôle qui entrent dans le périmètre d'évaluation des auditeurs internes.

Copyright © 2015 Eyrolles.

ÉTUDE DE CAS

Pat Goodly a accepté un poste de responsable de l'audit interne dans une grande multinationale disposant d'un service d'audit interne bien établi. On considère que cette organisation est un leader de son secteur et applique des pratiques de gouvernance très solides. Le Conseil se compose essentiellement d'administrateurs externes et indépendants. Le comité d'audit se compose également d'administrateurs externes et indépendants, tous qualifiés. Le président du comité d'audit est considéré comme l'« expert financier » du comité d'audit.

La fin de l'exercice est dans à peine un peu plus d'un mois. Après deux mois seulement à son nouveau poste, Pat prépare la prochaine réunion du comité d'audit. C'est normalement la réunion au cours de laquelle le plan d'audit interne et le budget pour l'année suivante sont présentés pour approbation par le comité d'audit, ainsi que tous les documents nécessaires relatifs à la communication de fin de l'exercice.

Pat a récemment reçu un appel de « bienvenue » de la part du président du comité d'audit, qui l'a assurée de son soutien « plein et entier » envers elle et le service d'audit interne. Le président du comité d'audit lui a fait savoir qu'il souhaitait la rencontrer et connaître la conception et l'orientation qu'elle entend donner à l'audit interne à l'avenir. Il a indiqué qu'il était important qu'ils communiquent périodiquement et ferait en sorte qu'ils puissent avoir un dialogue ouvert et franc à l'avenir.

Pat a été recrutée par le directeur financier et c'est à lui qu'elle rend compte. Traditionnellement, c'est le directeur financier qui est chargé de l'ordre du jour des réunions du comité d'audit et de la sélection des sujets y afférents. C'est également lui qui préside jusqu'alors les réunions.

La direction générale, y compris le directeur général et le directeur financier, ont fait part de leur soutien envers l'audit interne et la façon dont Pat conçoit cette fonction, à la fois lors du recrutement et après que Pat a rejoint l'organisation. Cependant, lors d'une réunion récente, le directeur financier a fermement déclaré : « Je sais que tout le monde est très occupé et que le rythme va s'intensifier à l'approche de la fin de l'exercice. Je pense qu'il est dans l'intérêt de chacun de ne pas opérer de changement « radical » dans la structure de reporting de notre organisation jusqu'à la fin de l'exercice. Si nous restons le nez dans le guidon et travaillons dur, nous devrions terminer l'exercice sans encombre. »

Alors qu'elle prépare la prochaine réunion du comité d'audit, Pat réfléchit aux propos du directeur financier et à la manière dont les normes professionnelles de l'IIA traitent les obligations de reporting du responsable de l'audit interne vis-à-vis de la direction générale et du Conseil. Mettez-vous à la place de Pat et réfléchissez aux points suivants.

Copyright © 2015 Eyrolles.

ÉTUDE DE CAS

1. Quelle conduite Pat doit-elle tenir à l'égard du président du comité d'audit ? A-t-elle des obligations vis-à-vis du président du comité d'audit, et si oui, quelles sont-elles ? En tant que responsable de l'audit interne, quels sont les responsabilités et le rôle de Pat vis-à-vis du comité d'audit et du président du comité d'audit ?

2. Discutez des principaux points à maîtriser et à traiter (et avec qui) pour s'acquitter correctement des obligations de reporting.

Copyright © 2015 Eyrolles.



Copyright © 2015 Eyrolles.



CHAPITRE 10
LES PREUVES D'AUDIT ET LES PAPIERS DE TRAVAIL

Objectifs pédagogiques

- Comprendre en quoi consistent la collecte et l'évaluation de preuves d'audit suffisantes et adéquates.
- Connaître les procédures manuelles utilisées par les auditeurs internes pour rassembler des preuves.
- Se familiariser avec les techniques d'audit informatisées (ou techniques d'audit assistées par ordinateur), et notamment avec les logiciels d'audit généralisés.
- Comprendre l'importance de papiers de travail bien préparés.

Dans ce chapitre, nous nous concentrons tout d'abord sur la collecte et la documentation des preuves d'audit, qui constituent un volet important de toutes les missions d'audit interne. La qualité des conclusions et des avis rendus par les auditeurs internes dépend de la capacité de ces intervenants à rassembler des preuves suffisantes et adéquates, et à les évaluer correctement. L'audit recourt à une succession de procédures pour collecter les preuves nécessaires à la réalisation des objectifs de la mission. Ces objectifs sont décrits et illustrés dans les chapitres 12 à 15, que nous qualifierons collectivement de chapitres relatifs aux processus d'audit interne.

Nous traiterons ensuite des papiers de travail qui constituent le principal moyen de consigner les procédures exécutées, les preuves obtenues, les conclusions rendues et les recommandations formulées par les auditeurs internes auxquels une mission a été confiée. Ce sont essentiellement les papiers de travail, en tant que documents de base (« *primary support* »), qui étayent les communications adressées par cette équipe à l'audité, à la direction générale, au Conseil et aux autres parties prenantes.

PREUVES D'AUDIT

Rappelons (chapitre 1, *Introduction à l'audit interne*) que l'audit interne repose sur la logique, donc sur un raisonnement et des déductions. Lorsque les auditeurs internes rendent des conclusions et des avis fondés sur les preuves qu'ils ont réunies et évaluées, ils s'appuient largement sur leur jugement de professionnels

Copyright © 2015 Eyrolles.

expérimentés. La qualité de leurs conclusions et avis dépend de leur capacité à rassembler et à évaluer correctement des preuves suffisantes et adéquates.

La collecte de preuves suffisantes et adéquates passe par un degré élevé d'interaction et de communication avec les collaborateurs de l'entité auditée, tout au long de la mission. Cette interaction et cette communication sont essentielles à l'efficacité et à l'efficience de la mission. Il importe, par conséquent, que les auditeurs internes se montrent ouverts et qu'ils sachent communiquer et travailler en équipe. Néanmoins, l'auditeur interne doit toujours être conscient du fait que les managers et collaborateurs, auprès desquels il recueille des preuves, ne comprennent pas forcément la finalité, les objectifs et le périmètre de sa mission, ni la façon dont celle-ci est conduite. De plus, il arrive que certains managers ou collaborateurs perçoivent la mission d'audit comme une menace pour eux, c'est-à-dire qu'ils pensent que l'auditeur interne recherche uniquement la faute. Une erreur ou une fraude commise par le management et/ou par un collaborateur n'est malheureusement jamais exclue.

ENCADRÉ 10-1

DISPOSITIONS DU CRIPP PERTINENTES RELATIVES AU CHAPITRE 10

Norme 1220 – Conscience professionnelle
Norme 2200 – Planification de la mission
Norme 2240 – Programme de travail de la mission
Norme 2300 – Accomplissement de la mission
Norme 2310 – Identification des informations
Norme 2320 – Analyse et évaluation
Norme 2330 – Documentation des informations

Modalité Pratique d'Application 2240-1 : Programme de travail de la mission
Modalité Pratique d'Application 2330-1 : Documentation des informations
Modalité Pratique d'Application 2330.A1-1 : Contrôle des dossiers d'audit
Modalité Pratique d'Application 2330.A2-1 : Conservation des dossiers

Scepticisme professionnel
État d'esprit consistant à ne rien tenir pour acquis. Les auditeurs internes remettent constamment en question ce qu'ils entendent et voient, et portent un regard critique sur les preuves d'audit.

Assurance raisonnable
Niveau d'assurance étayé par des procédures et des jugements d'audit généralement acceptés.

Scepticisme professionnel et assurance raisonnable

L'auditeur interne doit toujours évaluer les preuves d'audit avec un certain niveau de scepticisme professionnel. Le scepticisme professionnel désigne l'état d'esprit qui consiste à ne rien tenir pour acquis. Les auditeurs internes remettent constamment en question ce qu'ils entendent et voient, et portent un regard critique sur les preuves d'audit. Ils ne présupposent pas que les collaborateurs de l'entité auditée sont honnêtes ou malhonnêtes. En exerçant son scepticisme professionnel tout au long de sa mission, l'auditeur interne reste impartial et garde un esprit ouvert pour formuler des

Copyright © 2015 Eyrolles.

jugements qui reposent sur la prépondérance des preuves réunies au cours de sa mission, et non pas uniquement sur des éléments d'information. Le chapitre 8, *Les risques de fraude et d'actes illégaux*, traite du scepticisme professionnel dans le contexte de la fraude.

Les auditeurs internes sont rarement, voire jamais, en mesure de donner une assurance absolue concernant la véracité des critères de qualité retenus par le management pour l'évaluation du système de contrôle interne et des performances. En raison de la nature et de l'étendue des preuves qu'ils rassemblent et des décisions qu'ils prennent, il est rare que les auditeurs internes, même expérimentés, n'aient aucun doute. Souvent, ils doivent se fonder sur des preuves convaincantes, plutôt que totalement concluantes, et leurs décisions sont rarement soit positives soit totalement négatives. De surcroît, les auditeurs internes doivent rendre des conclusions et des avis à un coût et dans un délai raisonnables, afin de créer de la valeur ajoutée. Ils s'attachent donc à obtenir des preuves suffisantes et adéquates pour justifier leurs conclusions et avis. C'est ce que les auditeurs internes appellent une « *assurance raisonnable* ».

Commentaire du traducteur

Finalement, le risque d'audit est le risque résiduel après le passage des auditeurs internes du fait d'oublis ou de négligences volontaires ou involontaires. De même que le risque de contrôle interne est le risque résiduel après la mise en place du contrôle interne… et que traquent les auditeurs.

Caractère convaincant des preuves d'audit

Les preuves d'audit sont convaincantes si elles permettent à l'auditeur interne de formuler, en toute confiance, des conclusions et des avis justifiés (bien fondés). Une preuve convaincante est :

- **pertinente :** La preuve considérée est-elle pertinente vis-à-vis de l'objectif d'audit ? Étaye-t-elle logiquement la conclusion ou l'avis de l'auditeur interne ?
- **fiable :** La preuve considérée vient-elle d'une source crédible ? A-t-elle été directement obtenue par l'auditeur interne ?
- **suffisante :** L'auditeur interne a-t-il obtenu suffisamment de preuves ? Des éléments de preuve différents mais connexes se corroborent-ils mutuellement ?

Selon l'*American Institute of Certified Public Accountants* (AICPA), « l'*adéquation* indique la qualité des preuves d'audit, c'est-à-dire leur pertinence et leur fiabilité […], et le *caractère suffisant* rend compte du volume des preuves d'audit […] »[1].

Preuve d'audit convaincante

Preuve qui permet à l'audit interne de formuler, en toute confiance, des conclusions et des avis justifiés (bien fondés).

Risque d'audit

Risque d'aboutir à une conclusion d'audit non valide et/ou d'apporter un conseil inadéquat sur la base des travaux d'audit menés.

Copyright © 2015 Eyrolles.

Commentaire du traducteur

Les Normes d'Exercice Professionnel (NEP) de la CNCC, traduction des International Standards of Auditing, *donnent également des définitions relatives à la qualité des preuves d'audit (notamment NEP 330, 500, 706…). Ces normes sont accessibles sur le site www.cncc.fr.*

Pourquoi les preuves d'audit doivent-elles être pertinentes pour être convaincantes ? Parce que le fait de se fonder sur des preuves peu ou non pertinentes pour un objectif d'audit accroît nettement le *risque d'audit*, c'est-à-dire le risque d'aboutir à une conclusion d'audit non valide et/ou d'apporter un conseil inadéquat sur la base des travaux d'audit menés.

> **Exemple.** Supposons qu'un auditeur interne cherche à déterminer si un véhicule comptabilisé dans les immobilisations corporelles de l'organisation existe bien et si cette dernière en est propriétaire. L'auditeur interne localise ce véhicule dans le parking de l'organisation. Peut-il raisonnablement conclure, à la simple vue du véhicule, que celui-ci existe ? Oui. Peut-il raisonnablement conclure, à la simple vue du véhicule, que celui-ci appartient à l'organisation ? Non. Il lui faudrait pour cela examiner les documents probants pertinents, tels qu'un titre de propriété.

S'il n'existe pas de principes clairs concernant la fiabilité et le caractère suffisant des preuves, il existe des règles que les auditeurs internes peuvent suivre à condition de ne pas oublier qu'elles s'accompagnent généralement d'exceptions. Ces règles sont les suivantes :

- les preuves obtenues auprès de tiers indépendants sont *plus fiables* que celles émanant des collaborateurs de l'entité auditée ;
- les preuves produites par un processus ou un système auquel sont appliqués des contrôles efficaces sont *plus fiables* que celles produites par un processus ou un système faisant l'objet de contrôles inefficaces ;
- les preuves obtenues directement par l'auditeur interne sont *plus fiables* que celles obtenues indirectement ;
- les preuves documentées sont *plus fiables* que les preuves non documentées ;
- les preuves obtenues rapidement sont *plus fiables* que les preuves obtenues après un long délai ;
- les preuves corroborées sont *plus suffisantes* que les preuves non corroborées ou que les preuves contradictoires ;
- un grand échantillon produit, toutes choses égales par ailleurs, une présomption de preuves *plus suffisantes* qu'un petit échantillon.

Copyright © 2015 Eyrolles.

Commentaire du traducteur

La Norme 2310 définit les caractéristiques des informations nécessaires pour atteindre les objectifs d'une mission d'audit. Ainsi, « une information suffisante est factuelle, adéquate et probante, de sorte qu'une personne prudente et informée pourrait parvenir aux mêmes conclusions que l'auditeur ».

Les documents probants constituent une part significative des preuves réunies au cours de la plupart des missions d'audit interne. Leur fiabilité dépend, dans une large mesure, de leur source et du chemin qu'ils parcourent avant d'être examinés par l'auditeur interne. L'encadré 10-2 illustre ce point.

ENCADRÉ 10-2

FIABILITÉ DES DOCUMENTS PROBANTS

Degré de fiabilité	Descriptions	Exemples de documents
Élevé	Documents élaborés par l'auditeur interne. Documents envoyés directement par un tiers à l'auditeur interne.	Comptage des stocks par sondage. Cartographies des processus. Matrices de risques et de contrôles. Confirmations. Relevés bancaires de contrôle. Courriers de conseils juridiques extérieurs.
Moyen	Documents produits par un tiers, envoyés à l'organisation et demandés par l'auditeur interne à celle-ci. Documents produits par l'organisation, envoyés à un tiers, renvoyés à l'organisation et demandés par l'auditeur interne à celle-ci.	Factures fournisseurs. Bons de commande émanant de clients. Relevés bancaires. Avis de règlement. Opposition sur chèque. Bordereaux de dépôt.
Faible	Documents produits par l'organisation et demandés par l'auditeur interne à celle-ci.	Déclaration de principes par écrit. Bordereaux de réception. Listing ou fiches de pointage.

LES PROCÉDURES D'AUDIT

Procédures d'audit

Tâches spécifiques effectuées par l'auditeur interne afin de recueillir les preuves nécessaires à la réalisation des objectifs de l'audit.

Les *procédures d'audit* sont les tâches spécifiques effectuées par l'auditeur interne afin de recueillir les preuves nécessaires à la réalisation des objectifs de l'audit. Elles sont mises en œuvre durant le processus d'audit pour :

- acquérir une connaissance approfondie de l'audité, notamment de ses objectifs, risques et contrôles ;
- vérifier l'adéquation de la conception et le fonctionnement effectif du système de contrôle interne du domaine ciblé ;

Copyright © 2015 Eyrolles.

- analyser les relations plausibles entre les différentes données ;
- vérifier directement les données financières et extrafinancières, à la recherche d'erreurs et de fraudes.

Pour obtenir les preuves suffisantes et adéquates qui permettront d'atteindre les objectifs d'audit définis, il faut déterminer la nature, l'étendue et le calendrier d'application des procédures d'audit.

Nature des procédures d'audit. Il s'agit du type de tests que l'auditeur interne doit effectuer pour atteindre ses objectifs. Il existe rarement une relation biunivoque entre les objectifs et les procédures d'audit. Les procédures d'audit individuelles apportent souvent des preuves pertinentes pour plus d'un objectif d'audit et, souvent, plusieurs procédures sont nécessaires pour atteindre un objectif d'audit. En fonction de leur nature, les différents tests donnent un degré d'assurance variable, sont plus ou moins longs et plus ou moins coûteux. L'auditeur interne doit comparer les coûts et avantages associés aux différents types de procédures. Selon la nature de la mission, il pourra recourir à des procédures d'audit manuelles, à des techniques d'audit informatisées, ou à une combinaison des deux, pour rassembler des preuves suffisantes et adéquates. Les procédures d'audit manuelles et les techniques d'audit assistées par ordinateur sont analysées plus loin dans ce chapitre.

Étendue des procédures d'audit. Il s'agit du volume de preuves d'audit que l'auditeur interne doit obtenir pour atteindre ses objectifs. L'auditeur interne doit, par exemple, déterminer la combinaison appropriée de procédures à mettre en œuvre, ainsi que l'ampleur des tests à effectuer. L'auditeur interne peut notamment décider de tester certains types de transactions dans leur intégralité, et d'autres par échantillonnage. L'échantillonnage en audit est analysé en détail dans le chapitre 11, *L'échantillonnage en audit*. Enfin, l'auditeur interne doit réunir et évaluer suffisamment de preuves pour rendre des conclusions et des avis justifiés.

Calendrier d'application des procédures d'audit. Le calendrier d'application des procédures d'audit définit à quel moment les tests sont effectués et la période qui est couverte. Quelques exemples sont donnés ci-après :

- un auditeur interne qui, au moyen d'un échantillon, teste le fonctionnement effectif d'un contrôle manuel, sur une période donnée, doit prendre des mesures appropriées afin d'obtenir l'assurance que l'échantillon sélectionné est représentatif de l'ensemble de la période ;
- un auditeur interne qui vérifie que des transactions sont comptabilisées sur le bon exercice fiscal se concentrera sur celles qui précèdent et qui suivent immédiatement la clôture de l'exercice ;

Copyright © 2015 Eyrolles.

- un auditeur interne vérifie le fonctionnement d'un contrôle d'application informatisé à un moment donné, pour déterminer si ce contrôle fonctionne de manière effective à cette date. Afin d'obtenir l'assurance que le contrôle a été efficace sur cette période, il réalise différents tests, portant notamment sur l'accès aux programmes applicatifs et sur la modification de ces programmes pendant une période donnée.

Les procédures d'audit manuelles

Les procédures d'audit manuelles courantes consistent en des demandes de renseignements, observations, inspections, pistes d'audit descendantes et ascendantes, vérifications de calculs, procédures analytiques et confirmations. Chacune est définie et analysée ci-dessous. L'encadré 10-3 propose des exemples d'applications.

Demande de renseignements. Cela consiste à poser aux collaborateurs de l'entité auditée ou à des tiers des questions auxquelles ils répondent par oral ou par écrit. Une demande de renseignements permet d'obtenir des preuves indirectes qui, par nature, sont rarement convaincantes. C'est tout particulièrement le cas lorsque les demandes de renseignements sont adressées aux collaborateurs de l'entité auditée, dont l'auditeur interne ne peut pas attendre de réponses impartiales. Certaines demandes de renseignements sont plus formelles, telles que les entretiens, les enquêtes et les questionnaires. L'encadré 10-4 répertorie les principaux éléments d'un entretien efficace.

Observation. Cela consiste à observer des personnes, des procédures ou des processus (y compris les documents ou les biens les concernant). L'observation est habituellement considérée comme plus convaincante qu'une demande de renseignements, dans le sens où elle permet à l'auditeur interne d'obtenir des preuves directes. Ainsi, en observant personnellement et directement un collaborateur qui met en œuvre un contrôle, l'auditeur interne obtient généralement un degré d'assurance plus grand que s'il se contentait d'interroger ce collaborateur sur l'application du contrôle en question. L'observation comporte néanmoins une limite importante : elle apporte des preuves à un instant donné. L'auditeur interne ne peut donc pas conclure que ce qui est observé est représentatif des événements qui se sont déroulés au cours de l'année. Il faut tenir compte de la possibilité que les gens se comportent différemment lorsqu'ils se sentent observés.

Inspection. Il s'agit d'étudier des documents et des pièces, et d'examiner physiquement des actifs corporels. L'inspection apporte des preuves directes quant au contenu des documents et pièces. De même, l'examen physique d'actifs corporels (tels qu'un immeuble ou un équipement) permet à l'auditeur interne de s'assurer directement et personnellement que ces ressources existent, ainsi que de leur état physique. Cependant, les auditeurs internes doivent

Copyright © 2015 Eyrolles.

EXEMPLES D'APPLICATIONS DES PROCÉDURES D'AUDIT MANUELLES

Procédures	Exemples d'applications
Demande de renseignements	• Diffuser auprès des cadres supérieurs un questionnaire leur demandant d'identifier les « 10 principaux risques » qui font peser une menace sur l'organisation. • Demander au conseil juridique extérieur de l'organisation de donner des informations sur tout litige, toute réclamation et/ou toute évaluation à l'encontre de l'organisation. • Demander aux managers et aux collaborateurs chargés des décaissements d'identifier les contrôles clés.
Observation	• Visiter le site de l'audité pour avoir une vue d'ensemble de ses opérations quotidiennes. • Observer quel soin les collaborateurs portent à l'inventaire du stock physique de clôture. • Observer les collaborateurs chargés de réaliser et de comptabiliser les décaissements, afin de déterminer s'ils exercent les responsabilités qui leur ont été assignées et *uniquement* celles-ci.
Inspection	• Examiner les procès-verbaux des réunions du Conseil pour y rechercher les autorisations données à des opérations importantes (telles que l'acquisition d'une autre organisation). • Inspecter quelques éléments du stock pour déterminer leur état et s'ils sont vendables. • Prendre connaissance des règles et procédures de décaissement, de façon à comprendre les composantes essentielles du processus (par exemple les rôles et responsabilités assignés).
Piste d'audit ascendante (*vouching*)	• Vérifier un échantillon d'articles du stock issu des documents comptables en le comparant aux documents de l'entrepôt, afin de vérifier que ces éléments existent bien. • Comparer un échantillon de factures clients aux documents d'expédition correspondants, afin de vérifier que ces expéditions ont bien eu lieu. • Comparer un échantillon de copies de chèques aux pièces justificatives correspondantes, afin de vérifier la validité de ces chèques.
Piste d'audit descendante (*tracing*)	• Retrouver les comptages du stock effectués par sondage par l'auditeur interne, en les comparant aux enregistrements de l'inventaire du stock effectués par l'audité, afin de vérifier que les comptages sont correctement inclus dans les enregistrements des stocks. • Rapprocher les bordereaux de réception des articles reçus aux pièces justificatives correspondantes, puis au journal des achats, afin de vérifier que les réceptions de marchandises sont effectivement comptabilisées au passif. • Retrouver les chèques établis sur une période de plusieurs jours, avant et après la clôture de l'exercice, en les comparant avec les pièces comptables correspondantes, afin de vérifier leur comptabilisation sur le bon exercice.
Réexécution de contrôles, d'autres procédures, ou de calculs	• Recalculer les amortissements cumulés et la dotation aux amortissements, afin de vérifier qu'ils ont été correctement calculés. • Estimer de manière indépendante la provision pour créances douteuses, afin de vérifier la vraisemblance de l'estimation effectuée par le service comptable. • Refaire les rapprochements bancaires effectués par l'audité, afin de vérifier s'ils ont été réalisés correctement.
Procédures analytiques	• Établir les états financiers en données relatives pour l'exercice en cours et les deux exercices précédents ; rechercher d'éventuels écarts ou des tendances anormales. • Comparer les états financiers établis par l'organisation avec les informations sectorielles publiées sous la même forme (en données relatives), afin de rechercher des incohérences. • Calculer la rotation des comptes fournisseurs pour l'exercice en cours et les deux exercices précédents, à titre de preuve des périodes de règlement des factures fournisseurs.
Confirmation ou circularisation	• Faire confirmer, directement par les clients de l'audité, un échantillon de solde de la balance auxiliaire client. • Faire confirmer par les organismes prêteurs le solde principal de sommes dues et le taux d'intérêt. • Faire confirmer les soldes de trésorerie auprès des établissements financiers.

ENCADRÉ 10-3

Copyright © 2015 Eyrolles.

PRINCIPAUX ÉLÉMENTS D'UN ENTRETIEN EFFICACE

Objectifs de l'entretien :

- Rassembler des informations (à savoir des preuves d'audit) pertinentes pour la mission.
- Élaborer un rapport favorisant des relations de travail positives tout au long de la mission.

Processus :

Préparer l'entretien :

- Définir la finalité de l'entretien.
- Identifier la personne à interroger.
- Rassembler des informations de base sur le domaine à auditer et sur la personne à interroger.
- Formuler l'ensemble adéquat de questions (quoi, pourquoi, comment, où, quand, qui).
- Déterminer les attentes vis-à-vis de la personne à interroger et identifier les besoins d'information.
- S'occuper de la logistique (date, heure, lieu, durée de l'entretien).
- Préparer les grandes lignes de l'entretien.

Conduire l'entretien :

- Établir la communication et créer un climat de confiance propice à la transparence.
- Exposer la finalité de l'entretien, les aspects à traiter et le temps nécessaire estimé.
- Poser des questions directes et des questions complémentaires pertinentes.
- Éviter tout jargon technique.
- Savoir utiliser les temps de silence.
- Écouter.
- Résumer et reformuler les points clés pour confirmation.
- Discuter des étapes suivantes.
- Prendre rendez-vous pour un suivi.
- Remercier la personne interrogée.

Documenter les résultats de l'entretien (le plus tôt possible après l'entretien) :

- Se remémorer l'entretien et relire les notes prises.
- Consigner les résultats de l'entretien en bonne et due forme.

Qualités des personnes qui mènent des entretiens efficacement :

- Professionnalisme (par exemple, préparer l'entretien, se montrer respectueux, courtois et ponctuel).
- Grand sens des relations humaines, excellentes compétences en communication orale, et notamment capacités d'écoute.
- Capacité à inspirer confiance et respect, sans arrogance.
- Curiosité innée.
- Objectivité (c'est-à-dire rester impartial et s'abstenir d'exprimer des opinions personnelles).

Obstacles fréquents à l'efficacité des entretiens :

- Entraves dues à l'audité, par exemple plusieurs impératifs à satisfaire au même moment, préjugés à l'égard des auditeurs internes, peur des représailles.
- Failles dans le processus d'entretien.
- Absence de certaines compétences requises de la part de l'auditeur interne.

Facteurs clés de réussite :

- Préparer l'entretien.
- Connaître et respecter la personne interrogée.
- Instaurer de la crédibilité et de la confiance.
- Utiliser le même langage que la personne interrogée.
- S'attendre au plus inattendu.

Copyright © 2015 Eyrolles.

connaître leur propre niveau de compétences (c'est-à-dire leur capacité à comprendre ce qu'ils lisent et voient) et en tenir compte. Par exemple, la formulation, sur la base d'une inspection, de conclusions valides portant sur la valeur de pierres précieuses peut dépasser le champ de compétences d'un auditeur interne. Dans ce cas, celui-ci doit faire appel à un expert en gemmologie, qui l'aidera à valider la valeur de ces pierres.

Piste d'audit ascendante (*vouching*)

À partir d'un document ou d'une pièce, il s'agit de *rechercher* un document, une pièce établi(e) préalablement, ou l'actif corporel correspondant.

Piste d'audit ascendante (vouching). À partir d'un document ou d'une pièce, il s'agit de *rechercher* un document, une pièce établi(e) préalablement, ou l'actif corporel correspondant. Une piste d'audit ascendante sert spécifiquement à vérifier la *validité* d'informations contenues dans un document ou dans une pièce. Ainsi, une vente de marchandises ne doit généralement pas être comptabilisée tant que les marchandises n'ont pas été expédiées (sorties des stocks). En appliquant une piste d'audit ascendante pour rechercher le bordereau d'expédition à partir d'une facture, on obtient la preuve que l'expédition sur laquelle se fonde la facture a bien eu lieu. De même, en appliquant une piste d'audit ascendante pour rechercher le véhicule réel correspondant à l'écriture comptable dans le grand livre des immobilisations corporelles, on obtient la preuve que ce dernier existe bien. Dans le cadre des audits financiers, les pistes d'audit ascendantes permettent de repérer notamment des éléments surévalués dans des sommes comptabilisées.

Piste d'audit descendante (*tracing*)

À partir d'un document, d'une pièce ou d'un actif corporel, il s'agit de *retrouver* le document final ou l'écriture comptable finale.

Piste d'audit descendante (tracing). À partir d'un document, d'une pièce ou d'un actif corporel, il s'agit de *retrouver* le document final ou l'écriture comptable finale. Une piste d'audit descendante sert spécifiquement à vérifier l'*exhaustivité* des informations contenues dans un document ou dans une pièce. Ainsi, les achats de marchandises doivent généralement être comptabilisés à réception des marchandises (entrées des stocks). En appliquant une piste d'audit descendante, à partir d'un avis de réception de marchandises reçues à la fin d'un exercice, en retrouvant (retraçant) les écritures comptables correspondantes, on obtient la preuve que les éléments d'actif et de passif ont tous les deux été comptabilisés sur le même exercice que celui pendant lequel les marchandises ont été reçues. Dans le cadre des audits financiers, les pistes d'audit descendantes permettent de repérer notamment des éléments sous-évalués dans des sommes comptabilisées.

Réexécution de contrôles, d'autres procédures, ou de calculs. Il s'agit de refaire des contrôles, d'autres procédures, ou des calculs, ce qui apporte des preuves directes quant au fonctionnement effectif d'un contrôle. La réexécution apporte également des preuves directes permettant de déterminer si les calculs de l'audité sont corrects. En effectuant une estimation comptable indépendante portant, par exemple, sur les provisions pour créances douteuses, et en la comparant à l'estimation de l'audité, la vraisemblance de cette dernière est directement démontrée.

Copyright © 2015 Eyrolles.

Procédures analytiques. Les procédures d'audit analytiques servent à évaluer des informations obtenues au cours d'une mission en les comparant aux résultats attendus ou définis par l'auditeur interne. L'utilisation de procédures analytiques repose sur une condition préalable : l'auditeur interne peut raisonnablement présumer que certaines relations, entre différents éléments d'information, existent en l'absence d'éléments contraires identifiés. Il importe que les auditeurs internes expriment des attentes, en toute indépendance, fondées sur leur connaissance de l'audité, du secteur d'activité de l'organisation et de l'économie, avant d'accumuler et d'analyser des informations, ce qui permettra des comparaisons impartiales.

Procédures analytiques

Évaluation des informations obtenues au cours d'une mission en les comparant aux résultats attendus ou définis par l'auditeur interne.

Les auditeurs internes mettent en œuvre des procédures analytiques lors de la planification et de l'exécution d'une mission, de façon à déceler d'éventuelles anomalies au niveau de l'information, telles que l'existence de fluctuations, différences ou corrélations inattendues, ou au contraire l'absence de fluctuations, différences ou corrélations attendues. Ces anomalies peuvent être le signe d'opérations ou d'événements inhabituels ou non récurrents, d'erreurs ou d'activités frauduleuses, qui justifient une attention plus poussée et la collecte d'éléments de corroboration. Voici les procédures analytiques couramment appliquées par les auditeurs internes.

- **Analyse de tableaux en données relatives.** L'auditeur interne exprime les postes des états financiers, en pourcentage des totaux pertinents (par exemple, les postes du compte de résultat en pourcentage du chiffre d'affaires et les postes du bilan en pourcentage du total de l'actif).
- **Analyse de ratios.** L'auditeur interne calcule les ratios financiers pertinents (par exemple : ratio de liquidités, taux de marge brute, taux de rotation des stocks, coût des matières premières achetées par rapport au coût des produits finis) ainsi que des ratios extrafinanciers (chiffre d'affaires divisé par la superficie des espaces de vente, charges de personnel divisées par le nombre moyen de collaborateurs et pourcentage d'unités défectueuses produites, etc.). L'encadré 10-5 donne des exemples de ratios de performance. Il faut toutefois savoir que les seules véritables limites à l'analyse de ratios sont la disponibilité des informations nécessaires à leur calcul et le caractère inventif de l'auditeur interne.
- **Analyse de tendance.** L'auditeur interne compare les données relatives aux performances (montants, pourcentages et/ou ratios) concernant l'exercice en cours avec les mêmes informations concernant un ou plusieurs exercices précédents.
- **Analyse d'informations prospectives.** L'auditeur interne compare les informations relatives à l'exercice en cours aux budgets ou aux prévisions.

Copyright © 2015 Eyrolles.

- **Analyse comparative (*benchmarking*) externe.** L'auditeur interne compare les données relatives aux performances de l'organisation avec les mêmes informations concernant d'autres organisations ou le secteur d'activité dans lequel opère l'organisation. À des fins de comparaison, des données sectorielles publiées peuvent être obtenues auprès de sources comme Dun & Bradstreet, Standard & Poor's, les instituts de statistiques nationaux, etc.
- **Analyse comparative (*benchmarking*) interne.** L'auditeur interne compare les données relatives aux performances d'une unité opérationnelle avec les mêmes informations concernant d'autres unités opérationnelles.

Analyse comparative (*benchmarking*) externe

Comparaison des données relatives aux performances de l'organisation avec les mêmes informations concernant d'autres organisations ou le secteur d'activité dans lequel opère l'organisation.

Analyse comparative (*benchmarking*) interne

Comparaison des données relatives aux performances d'une unité opérationnelle avec les mêmes informations concernant d'autres unités opérationnelles.

La *confirmation (ou circularisation)* consiste à vérifier directement, par écrit, auprès de tiers indépendants, l'exactitude d'une information. Les preuves obtenues par confirmation sont généralement considérées comme très fiables, car elles sont apportées directement à l'auditeur interne par des sources indépendantes. Il existe deux principaux types de demandes de confirmations : la *confirmation positive (expresse),* qui consiste à demander aux destinataires de répondre indépendamment du fait qu'ils pensent ou non que l'information qui leur a été donnée est correcte, et la *confirmation négative (tacite),* par laquelle il est demandé aux destinataires de répondre qu'ils pensent que l'information qui leur a été donnée est incorrecte. Une confirmation positive peut consister à demander au destinataire d'apporter l'information recherchée (on parle alors de « confirmation ouverte ») ou à inclure cette information et à demander au destinataire d'indiquer s'il est d'accord ou non avec l'information en question (on parle alors de « confirmation fermée »).

Techniques d'audit informatisées

« Pour remplir ses fonctions avec conscience professionnelle, l'auditeur interne doit envisager l'utilisation de techniques informatiques d'audit et d'analyse des données » (Norme 1220.A2).

L'ISACA (*Information Systems Audit and Control Association*, www.isaca.org) définit les techniques d'audit informatisées, ou les techniques d'audit assistées par ordinateur (CAAT), comme « tout outil d'audit automatisé, tel que les logiciels d'audit généralisés, les générateurs de données de test, les programmes d'audit informatisés et les utilitaires d'audit spécialisés ». Certaines de ces techniques les plus courantes, sont définies ci-après par l'ISACA.

- *Logiciels d'audit généralisés.* Logiciels polyvalents, qui peuvent être utilisés à des fins [générales], par exemple pour la sélection d'écritures, le rapprochement, la vérification de calculs et le reporting.

Logiciel d'audit généralisé

Logiciel polyvalent, qui peut être utilisé à des fins d'audit, par exemple pour la sélection d'écritures, le rapprochement, la vérification de calculs et le reporting.

Copyright © 2015 Eyrolles.

EXEMPLES DE RATIOS DE PERFORMANCE

ENCADRÉ 10-5

Chiffre d'affaires, comptes clients et encaissements :

- Chiffre d'affaires net (Toutes taxes comprises) ÷ comptes clients en valeur nette, moyenne ou à la clôture de l'exercice (rotation des comptes clients)
- 365 ÷ rotation des comptes clients (délai moyen de recouvrement)
- Chiffre d'affaires net ÷ superficie des espaces de vente
- Livraisons aux clients dans les délais ÷ total des livraisons aux clients
- Créances douteuses ÷ chiffre d'affaires net (Toutes taxes comprises)
- Provision pour créances douteuses à la clôture de l'exercice ÷ comptes clients à la clôture de l'exercice

Achats, comptes fournisseurs et décaissements :

- Coût des matières premières ÷ coût des produits finis
- Livraisons des fournisseurs dans les délais ÷ total des livraisons des fournisseurs
- Retours sur achats ÷ total des achats ou coût des produits vendus
- Coût des produits vendus (Toutes taxes comprises) ou achats nets (Toutes taxes comprises) ÷ comptes fournisseurs, moyen ou à la clôture de l'exercice (rotation des comptes fournisseurs)

Stock et coût des produits vendus :

- Coût des produits vendus ÷ stock moyen ou à la clôture de l'exercice (rotation des stocks)
- 365 ÷ rotation des stocks (délai moyen de vente)
- Nombre d'unités défectueuses produites ÷ total des unités produites
- Coût des rebuts/gaspillages/rejets de production ÷ chiffre d'affaires net ou coût des marchandises vendues
- Marge brute ÷ chiffre d'affaires net (ratio de la marge brute)

Ressources humaines et masse salariale :

- Nombre de départs volontaires et/ou non au cours de l'exercice ÷ nombre de collaborateurs moyen ou à la clôture de l'exercice (rotation du personnel)
- Jours/homme perdus en raison de l'absentéisme ÷ total des jours/homme
- Nombre d'heures supplémentaires travaillées ÷ total des heures travaillées
- Charges de personnel ÷ nombre de collaborateurs moyen ou à la clôture de l'exercice

- *Logiciels utilitaires.* Logiciels constitués de plusieurs programmes informatiques fournis par un fabricant de matériel informatique ou un vendeur de logiciels et servant à faire fonctionner le système d'exploitation. Cette technique peut être utilisée pour examiner le déroulement d'un traitement, tester des programmes, des interventions système et des procédures opérationnelles, évaluer les activités sur les fichiers de données et analyser les données afférentes à la comptabilisation des travaux.
- *Données de test.* Simulation de transactions pouvant servir à tester la logique du traitement, les calculs et les contrôles réellement programmés dans les applications informatiques. Les tests peuvent porter sur des programmes individuels ou sur un système entier. Cette technique englobe les mécanismes de test intégrés et les évaluations de systèmes sur la base d'un scénario de référence.

Copyright © 2015 Eyrolles.

- *Outils de traçage logique et de cartographie des logiciels d'application.* Outils spécialisés qui peuvent être utilisés pour analyser le flux de données à travers la logique de traitement des logiciels d'application et pour documenter cette logique, les chemins, les conditions de contrôle et les séquences de traitement. L'analyse peut porter, d'une part, sur le langage de commande ou sur l'ordre de contrôle des travaux et, d'autre part, sur le langage de programmation. Cette technique inclut la cartographie du programme/système, le traçage logique, les points de contrôle instantanés, les simulations parallèles et la comparaison des codes.
- *Systèmes experts d'audit.* Systèmes experts ou systèmes d'aide à la décision qui peuvent être utilisés pour assister les systèmes d'information (SI) au cours du processus décisionnel en automatisant les connaissances de spécialistes dans le domaine examiné. Cette technique inclut l'analyse automatisée des risques, les logiciels système et les progiciels fondés sur des objectifs de contrôle (cas des outils d'aide à la décision dans les salles de marché).
- *Audit continu.* Il permet aux auditeurs des SI de surveiller en continu la fiabilité des systèmes et de recueillir des preuves d'audit sélectives *via* un ordinateur[2].

Audit continu

Recours à des techniques informatisées qui permettent d'auditer en permanence le traitement des transactions d'une organisation.

Ces définitions indiquent que les auditeurs internes peuvent recourir à des techniques informatisées d'aide à l'audit pour tester directement (1) les contrôles intégrés dans les systèmes d'information informatisés et (2) les données contenues dans les fichiers informatiques. Il convient de noter que, dans ce second cas, les auditeurs internes obtiennent des preuves indirectes concernant l'efficacité des contrôles au niveau de l'application qui a traité les données.

> **Exemple.** Un auditeur interne utilise un logiciel d'audit généralisé pour déterminer directement si le journal des décaissements de l'organisation contient des paiements en double. Il découvre plusieurs paiements en double, effectués pendant l'exercice. Cet auditeur interne peut en déduire, à juste titre, que des contrôles destinés à prévenir et/ou à détecter rapidement de tels paiements ne sont pas en place, qu'ils sont conçus de manière inadéquate ou ne fonctionnent pas de manière effective.

Une analyse approfondie de chacune des techniques informatisées d'aide à l'audit définies plus haut sortirait du cadre du présent manuel. Cependant, les logiciels d'audit généralisés et le type d'analyses des données que les auditeurs internes peuvent effectuer avec ces logiciels méritent un peu plus d'attention.

Certains auditeurs internes continuent de penser que les logiciels d'audit généralisés sont des outils réservés à l'usage exclusif des spécialistes de l'audit des SI. Toutefois, comme l'indique la citation

Copyright © 2015 Eyrolles.

suivante extraite du *GTAG 16, Data Analysis Technologies* (Techniques informatisées d'analyse de données), qui figure parmi les guides pratiques d'audit des technologies de l'information de l'IIA, ce n'est plus vrai aujourd'hui.

> *« Dans le monde fortement automatisé d'aujourd'hui, presque tous les auditeurs doivent savoir analyser les données. Ce qui était autrefois considéré comme une expertise particulière, propre aux auditeurs des systèmes d'information, ou comme une tâche largement externalisée auprès d'autres services de l'organisation, est devenu une compétence clé de la profession d'audit interne. »*[3]

Heureusement, ces logiciels sont désormais relativement simples à utiliser, même par des auditeurs internes peu formés aux systèmes d'information. Ils combinent une interface conviviale et des fonctions d'analyse de données puissantes, notamment :

- examen des fichiers et enregistrements pour vérifier leur validité, leur exhaustivité et leur exactitude ;
- vérification du calcul des valeurs enregistrées et calcul d'autres valeurs clés qui intéressent l'audit ;
- sélection et impression d'échantillons, calcul des résultats d'échantillonnage ;
- comparaison des informations contenues dans différents fichiers ;
- synthèse, reséquençage et reformatage de données ;
- création de tableaux croisés dynamiques pour des analyses multidimensionnelles ;
- recherche d'anomalies dans les données, qui sont susceptibles d'indiquer des erreurs ou des fraudes ;
- élaboration et impression de rapports ;
- production automatique d'un journal des analyses de données.

Utilité d'un logiciel d'audit généralisé. Ce type de logiciel est utile à de nombreux égards :

- il permet aux auditeurs internes de mettre en œuvre les procédures d'audit dans de multiples environnements matériels et logiciels sans nécessiter d'adaptations majeures ;
- il permet aux auditeurs internes de tester des données sans faire appel aux collaborateurs du service informatique de l'organisation ;
- il permet aux auditeurs internes d'analyser aisément de très gros volumes de données ;

Copyright © 2015 Eyrolles.

- contrairement aux tests manuels portant sur un échantillon de données, certaines applications des logiciels d'audit généralisés facilitent l'analyse de populations de données dans leur intégralité et permettent d'effectuer cette analyse de façon quasiment instantanée ;
- le recours à un logiciel d'audit généralisé pour l'exécution de tâches nécessaires mais routinières libère du temps, que l'auditeur interne peut alors consacrer à l'analyse.

Obstacles à l'introduction réussie d'un logiciel d'audit généralisé. Il existe également des obstacles qu'un auditeur interne doit surmonter pour utiliser avec succès un logiciel d'audit généralisé :

- obtenir les droits (ou privilèges) d'accès à des données pertinentes et fiables ;
- obtenir l'accès physique aux données ;
- comprendre le mode de stockage et de formatage des données dans le système ;
- extraire les données et les télécharger sur son ordinateur individuel (PC) ;
- importer dans le logiciel d'audit les données sous un format exploitable.

Pour lever ces obstacles, il faut, dans certains cas, demander l'assistance d'un spécialiste de l'audit des systèmes d'information. Cependant, les deux seules limites insurmontables à la création de valeur ajoutée *via* le recours à un logiciel d'audit généralisé sont la disponibilité de données pertinentes sous un format électronique et le caractère inventif de l'auditeur interne.

ACL et IDEA

Les deux logiciels d'audit disponibles dans le commerce les plus utilisés par les auditeurs.

Logiciels ACL® et IDEA. ACL (*Audit Command Language*®), logiciel d'analyse de données, et IDEA (initialement l'acronyme de *Interactive Data Extraction and Analysis*) fonctionnent tous deux sous Windows et peuvent être installés facilement sur le PC d'un auditeur interne.

Le logiciel ACL est un produit d'ACL Services Ltd. Les lecteurs intéressés peuvent obtenir des informations supplémentaires sur cette organisation en consultant son site Web : www.acl.com.

Le logiciel IDEA est un produit de CaseWare IDEA Inc., société d'édition de logiciels et de marketing à capitaux privés. Audimation Services Inc. est le partenaire commercial de CaseWare IDEA Inc. aux États-Unis. Les lecteurs intéressés peuvent obtenir des informations supplémentaires en consultant les sites Web de ces deux organisations : www.CaseWare-IDEA.com et www.audimation.com.

Copyright © 2015 Eyrolles.

PAPIERS DE TRAVAIL

La Norme 2330, « Documentation des informations », impose aux auditeurs internes de documenter les informations pertinentes pour étayer les conclusions et les résultats de la mission. La MPA 2330-1, « Documentation des informations », formule des orientations concernant les papiers de travail et leur élaboration.

Finalités et contenu des papiers de travail

Les papiers de travail revêtent une importance cruciale en raison de leurs nombreuses finalités, dont voici quelques exemples.

- Aider à planifier et exécuter les missions d'audit.
- Faciliter la supervision de la mission et la revue des travaux effectués.
- Indiquer si les objectifs de la mission ont été atteints.
- Constituer le principal document d'appui au rapport communiqué par les auditeurs internes à l'audité, à la direction générale, au Conseil et aux tiers concernés.
- Fournir une base pour l'évaluation du programme d'assurance qualité de l'audit interne.
- Contribuer au développement professionnel des collaborateurs de l'audit interne.
- Démontrer que l'audit interne se conforme aux *Normes internationales pour la pratique professionnelle de l'audit interne*, définies par l'IIA (les *Normes*).

Le contenu des papiers de travail dépend de la nature de la mission d'audit interne. Néanmoins, les papiers de travail doivent toujours permettre une documentation complète, exacte et concise du processus d'audit.

Les différents types de papiers de travail

Des papiers de travail très divers sont élaborés au cours d'une mission d'audit interne. La liste qui suit est plus illustrative qu'exhaustive.

- Programmes de travail servant à présenter la nature, l'étendue et le calendrier d'application des procédures d'audit spécifiques.
- Budget-temps de la mission et allocation des ressources.
- Questionnaires destinés à obtenir des informations sur l'audité, notamment sur ses objectifs, risques, contrôles et activités opérationnelles.

Copyright © 2015 Eyrolles.

- Cartographies des processus (diagrammes de flux ou de circulation) servant à documenter les activités liées à un processus, les risques et les contrôles (les symboles usuels utilisés pour les cartographies, ainsi que des exemples de cartographies des processus, sont présentés dans le chapitre 5, *Les processus et les risques,* tandis que les symboles utilisés pour les diagrammes de flux, et des exemples de ces diagrammes, sont présentés dans le chapitre 13, *Le déroulement de la mission d'assurance*).
- Diagrammes et graphiques, tels qu'une cartographie des risques qui permet de représenter l'impact et la probabilité d'occurrence des risques opérationnels (le chapitre 13 en donne un exemple).
- Ordres du jour des réunions de l'équipe d'audit interne et des réunions avec l'audité.
- Mémorandum de synthèse documentant les résultats des entretiens et d'autres réunions avec l'audité.
- Données pertinentes relatives à l'organisation de l'audité, par exemple organigrammes, descriptifs de postes, règles et procédures opérationnelles et financières.
- Copie de documents sources, tels que demandes d'achat, bons de commande, bordereaux de réception, factures fournisseurs, pièces justificatives et chèques.
- Copie d'autres documents importants, comme les procès-verbaux des réunions et les contrats.
- Documents relatifs aux SI, notamment listes de programmes et rapports d'anomalies.
- Documents comptables, tels que balances et extraits des journaux et livres.
- Preuves obtenues auprès de tiers, par exemple confirmations émanant de clients et déclarations d'un conseil juridique extérieur.
- Feuilles de travail élaborées par l'auditeur interne, telles que matrice de risques et de contrôles documentant les risques associés à chaque processus, description des contrôles clés, évaluation, par l'auditeur interne, de l'adéquation des contrôles, tests des contrôles et résultats de ces tests (le chapitre 13 présente un exemple de matrice de risques et de contrôles).
- Autres types de papiers de travail établis par l'auditeur interne qui font état des travaux (par exemple, procédures analytiques, analyse informatisée de données, tests directs sur des opérations, événements, soldes de comptes et mesures de performance).
- Preuves rassemblées par l'audité et vérifiées par l'auditeur interne.
- Contrôles effectués par l'audité puis à nouveau par l'auditeur interne (par exemple, rapprochements bancaires).

Copyright © 2015 Eyrolles.

- Correspondance écrite et documentation de la correspondance orale avec l'audité au cours de la mission.
- Exposés des observations, recommandations et conclusions de l'équipe d'audit interne (voir des exemples d'exposés, analysés dans le chapitre 13).
- Rapports définitifs des missions et commentaires du management (voir des exemples de rapports finaux de missions, présentés dans le chapitre 14, *La communication des résultats d'une mission d'assurance et les procédures de suivi*).

Règles relatives à l'élaboration des papiers de travail

C'est au responsable de l'audit interne qu'il appartient de définir les règles et procédures applicables aux papiers de travail. Des règles et procédures bien rédigées favorisent l'efficience et l'efficacité du travail d'audit, tout en facilitant l'adhésion constante aux normes d'assurance qualité.

La normalisation des papiers de travail peut permettre de rationaliser le processus d'audit et de faciliter un travail homogène et de qualité, pour chaque mission. Il convient toutefois d'éviter une normalisation excessive, qui nuirait à la créativité et à l'ingéniosité des auditeurs internes. Une normalisation appropriée peut consister en :

- un système uniforme de références croisées (*cross-references*), pour toutes les missions ;
- une présentation homogène des papiers de travail ;
- une uniformisation des marques de pointage (« *tick marks* ») c'est-à-dire les symboles utilisés dans les papiers de travail pour représenter des procédures d'audit spécifiques ;
- des prescriptions relatives aux types d'informations à stocker dans des dossiers permanents (c'est-à-dire des dossiers contenant les informations pertinentes à caractère permanent qui restent toujours importantes pour l'audité).

Les dossiers de travail doivent être complets et bien organisés. À la fin de chaque mission, ils doivent être mis à jour de manière à ne contenir que la version finale des papiers élaborés au cours de la mission. Chaque papier de travail doit pouvoir être lu de manière autonome. En d'autres termes, il doit par exemple :

- comporter un index ou un numéro de référence ;
- porter le nom de la mission et décrire le contenu ou l'objet du papier de travail ;

Copyright © 2015 Eyrolles.

- être signé (ou paraphé) à la fois par l'auditeur interne qui a effectué le travail et par le (ou les) auditeur(s) interne(s) qui a (ont) vérifié celui-ci (N.B. : cette signature peut être électronique) ;
- préciser les sources des données relatives à l'audité qui y sont mentionnées ;
- expliquer clairement les procédures spécifiques mises en œuvre ;
- être rédigé dans des termes clairs et compréhensibles par des auditeurs internes qui ne savent pas quel travail a été effectué (par exemple, un auditeur interne qui consulte ultérieurement ce papier).

Les papiers de travail doivent donc contenir des informations suffisantes pour permettre à un auditeur interne autre que celui qui a réalisé le travail de refaire celui-ci. En revanche, ils ne doivent pas contenir davantage d'informations que celles nécessaires : les papiers de travail doivent être aussi concis que possible.

De plus, le temps étant une ressource précieuse, les auditeurs internes doivent toujours s'attacher à élaborer correctement, dès le départ, les papiers de travail. En effet, il n'y a pas de temps alloué à la réécriture des papiers de travail. La nécessité cruciale d'établir des papiers de travail de manière correcte, claire, concise et rapide est l'une des raisons essentielles pour laquelle l'auditeur interne doit impérativement posséder de grandes compétences en communication écrite.

Les papiers de travail peuvent être établis sous forme papier ou électronique, ou sous ces deux formes. Il est aujourd'hui fréquent d'utiliser des logiciels servant à automatiser l'élaboration des papiers de travail, qu'ils soient achetés à des fournisseurs extérieurs ou développés en interne. Ils accroissent l'efficience et facilitent l'organisation uniforme et l'archivage des documents qui étayent une mission d'audit interne. Les cas pratiques de TeamMate® qui figurent à la fin du chapitre 6, *Le contrôle interne*, et du chapitre 12, *Introduction au processus d'audit*, offrent aux lecteurs la possibilité d'acquérir une expérience pratique grâce au logiciel TeamMate EWP (*Electronic Working Papers*, papiers de travail électroniques).

Copyright © 2015 Eyrolles.

RÉSUMÉ

Ce chapitre est axé sur la collecte et la documentation des preuves d'audit. Il s'est ouvert sur une analyse des preuves d'audit et des procédures, aussi bien des procédures manuelles que des outils informatiques d'aide à l'audit, que les auditeurs internes peuvent utiliser pour réunir des preuves suffisantes et adéquates. Ce chapitre se termine par un examen des papiers de travail, qui constituent le principal moyen de consigner les procédures effectuées, les preuves obtenues, les conclusions rendues et les recommandations formulées par l'équipe d'audit interne au cours de la mission. L'encadré 10-6 présente 11 éléments essentiels à retenir sur les preuves d'audit et les papiers de travail.

ENCADRÉ 10-6

11 ÉLÉMENTS ESSENTIELS À RETENIR SUR LES PREUVES D'AUDIT ET LES PAPIERS DE TRAVAIL

- La qualité des conclusions et des avis rendus par les auditeurs internes dépend de leur capacité à rassembler et à évaluer des preuves suffisantes et adéquates.
- Le *scepticisme professionnel* désigne l'état d'esprit qui consiste à ne rien tenir pour acquis. Les auditeurs internes remettent constamment en question ce qu'ils entendent et voient, et portent un regard critique sur les preuves d'audit.
- Une preuve convaincante est pertinente, fiable et suffisante.
- Les *procédures d'audit* sont les tâches spécifiques effectuées afin de recueillir les preuves nécessaires à la réalisation des objectifs de l'audit.
- Une *piste d'audit ascendante* consiste à *rechercher* des informations afin d'en vérifier la *validité*.
- *Une piste d'audit descendante* consiste à *retrouver* des informations afin d'en vérifier l'*exhaustivité*.
- Les *procédures analytiques* consistent à comparer les informations obtenues au cours d'une mission aux résultats attendus.
- Les auditeurs internes doivent savoir utiliser un logiciel d'audit généralisé, comme ACL ou IDEA, pour extraire et analyser les données stockées sur un support numérique.
- Les papiers de travail constituent le principal moyen de consigner les procédures exécutées, les preuves obtenues, les conclusions rendues et les recommandations formulées au cours d'une mission d'audit interne.
- Ce sont essentiellement les papiers de travail qui étayent les communications adressées par l'équipe d'audit interne à l'audité, à la direction générale, au Conseil et aux autres parties prenantes.
- Les papiers de travail électroniques, comme TeamMate EWP, accroissent l'efficience et facilitent l'organisation uniforme et l'archivage des documents.

Copyright © 2015 Eyrolles.

Questions de révision

1. Définissez le « scepticisme professionnel ».

2. Qu'entend-on par « assurance raisonnable » ? Pourquoi les auditeurs internes donnent-ils une assurance raisonnable, et non une assurance absolue ?

3. Quelles caractéristiques définissent une preuve d'audit convaincante ?

4. Expliquez la relation entre objectifs d'audit et procédures d'audit.

5. De quoi est-il question lorsque les auditeurs internes parlent de la nature, de l'étendue et du calendrier d'application des procédures d'audit ?

6. Citez quelques qualités courantes que possèdent les personnes maîtrisant les techniques d'entretien.

7. Expliquez la différence entre la procédure (piste) d'audit ascendante et la procédure (piste) d'audit descendante.

8. Citez les différents types de procédures analytiques employées par les auditeurs internes.

9. Citez plusieurs types courants de techniques informatisées d'aide à l'audit.

10. Quels types de procédures d'analyse de données les auditeurs internes peuvent-ils effectuer avec un logiciel d'audit généralisé ?

11. Quels sont les deux principaux logiciels d'audit généralisés les plus utilisés par les auditeurs internes ?

12. Quels sont les objectifs des papiers de travail établis dans le cadre d'une mission d'audit interne ?

13. Citez plusieurs types courants de papiers de travail.

14. Quelles sont les principales caractéristiques de papiers de travail bien préparés ?

Copyright © 2015 Eyrolles.

Questions à choix multiples

Sélectionnez la meilleure réponse pour chacune des questions suivantes.

1. Le « scepticisme professionnel » signifie que les auditeurs internes qui commencent une mission d'assurance doivent :
   a. Présumer que les collaborateurs du client sont malhonnêtes jusqu'à ce qu'ils aient rassemblé des preuves indiquant clairement le contraire.
   b. Présumer que les collaborateurs du client sont honnêtes jusqu'à ce qu'ils aient rassemblé des preuves indiquant clairement le contraire.
   c. Présumer que les collaborateurs du client ne sont ni honnêtes ni malhonnêtes.
   d. Présumer que les contrôles internes sont conçus de manière inadéquate et/ou ne fonctionnent pas de manière effective.

2. Quelle serait l'affirmation la moins appropriée d'un auditeur interne à propos des preuves d'audit ?
   a. « Je prends en compte le niveau de risque en jeu pour décider du type de preuve à collecter. »
   b. « Je ne mets pas en œuvre des procédures qui apportent des preuves convaincantes, car je dois obtenir des preuves concluantes. »
   c. « J'évalue à la fois l'utilité d'une preuve que je peux obtenir et le coût de son obtention. »
   d. « Je suis rarement tout à fait certain des conclusions que je formule sur la base des preuves que j'examine. »

3. Une preuve d'audit est généralement jugée suffisante si :
   a. Elle est adéquate.
   b. Elle suffit à étayer des conclusions bien fondées.
   c. Elle est pertinente, fiable et exempte de biais.
   d. Elle a été obtenue au moyen d'un échantillonnage aléatoire.

4. Les documents probants sont l'un des principaux types d'éléments de corroboration que peut employer un auditeur interne. Parmi les exemples suivants de documents probants, lequel est généralement considéré comme le plus fiable ?
   a. La facture d'un fournisseur, obtenue auprès du service fournisseurs.
   b. Un avoir édité par le manager du service crédit.
   c. Un bordereau de réception, obtenu auprès du service de la réception.
   d. Une copie de la facture client éditée par le service commercial.

Copyright © 2015 Eyrolles.

5. Un auditeur interne doit comparer le coût d'une procédure d'audit et le caractère convaincant des preuves à recueillir. L'observation est une procédure d'audit qui suppose des arbitrages coûts/bénéfices. Parmi les affirmations suivantes concernant l'observation considérée comme une procédure d'audit, laquelle est juste ?

   I. L'observation est limitée par le fait que les personnes peuvent réagir différemment lorsqu'elles se savent observées.

   II. L'observation est plus efficace pour tester l'exhaustivité que pour tester les éléments de preuve.

   III. L'observation apporte des preuves indiquant si certains contrôles fonctionnent comme prévu.

   a. I uniquement.

   b. II uniquement.

   c. I et III.

   d. I, II et III.

6. Un auditeur interne a recueilli les informations suivantes concernant l'évolution des comptes clients et l'analyse des ratios :

	Exercice		
	3	**2**	**1**
Comptes clients nets en pourcentage du total de l'actif	30,8 %	27,3 %	23,4 %
Rotation des comptes clients (chiffre d'affaires net [TTC] ÷ moyenne des comptes clients)	5,21	6,05	6,98

   Laquelle des explications suivantes est la plus raisonnable à propos des changements observés par l'auditeur ?

   a. Des ventes fictives ont été enregistrées sur les exercices 2 et 3.

   b. L'efficacité des procédures de crédit et de recouvrement s'est dégradée sur les trois exercices considérés.

   c. Les retours de ventes pour l'obtention d'un avoir ont été surévalués sur les exercices 2 et 3.

   d. La provision pour créances douteuses a été sous-évaluée sur les exercices 2 et 3.

Copyright © 2015 Eyrolles.

Questions à choix multiples

7. Votre objectif d'audit consiste à vérifier que les achats de fournitures de bureau ont été dûment autorisés. Si ces achats passent par le département des achats, laquelle des procédures suivantes est la plus appropriée ?
   a. Rapprocher les bons de commande et les demandes d'achat ayant reçu une autorisation.
   b. Comparer les demandes d'achat ayant reçu une autorisation et les bons de commande.
   c. Examiner les demandes d'achat pour vérifier qu'elles ont été dûment autorisées.
   d. Rapprocher les bons de réception et les bons de commande validés.

8. L'un des managers de la production de l'organisation MSM a commandé un volume excessif de matières premières et l'a fait livrer à une autre organisation qu'il dirige. Ce manager a falsifié les bons de réception et établi le bon à payer des factures (autorisation de la mise en paiement). Quelle serait la procédure la plus susceptible de détecter cette fraude ?
   a. Rapprocher les décaissements avec les bons de réception et les factures.
   b. Faire confirmer aux fournisseurs les volumes de matières premières achetés, les prix d'achat et les dates d'expédition.
   c. Effectuer une analyse des ratios et des tendances. Comparer le coût des matières premières achetées et celui des biens produits.
   d. Observer le quai de déchargement et compter les matières reçues. Comparer cette quantité aux bons de réception remplis par les collaborateurs chargés de la réception.

9. Un auditeur interne soupçonne une fraude portant sur des paiements à des fournisseurs fictifs. Les acheteurs de l'organisation, responsables de l'acquisition de lignes de produits spécifiques, sont habilités à autoriser des dépenses allant jusqu'à 10 000. Parmi les applications suivantes d'un logiciel d'audit généralisé, laquelle serait la plus efficace pour vérifier si le soupçon de l'auditeur est fondé ?
   a. Dresser la liste de tous les achats supérieurs à 10 000 afin de déterminer s'ils ont été dûment autorisés.
   b. Sélectionner un échantillon aléatoire parmi toutes les dépenses inférieures à 10 000 afin de déterminer si ces éléments ont été dûment autorisés.
   c. Dresser la liste des principaux fournisseurs par ligne de produits. Sélectionner un échantillon des plus importants et examiner tous les documents justifiant les biens et services reçus.
   d. Dresser la liste des principaux fournisseurs par ligne de produits. Sélectionner un échantillon des plus importants et envoyer des confirmations négatives pour valider le fait qu'ils ont effectivement fourni des biens ou services.

Copyright © 2015 Eyrolles.

10. Parmi les propositions suivantes, laquelle décrit le plus exhaustivement le contenu des papiers de travail élaborés par l'audit interne dans le cadre d'une mission d'assurance ?
    a. Les objectifs, procédures et conclusions.
    b. Le but, les critères, techniques et conclusions.
    c. Les objectifs, procédures, faits, conclusions et recommandations.
    d. Le sujet, le but, les éléments faisant l'objet d'un échantillonnage et l'analyse.

11. L'équipe d'audit interne en charge de la mission prépare des papiers de travail pour :
    a. L'audité.
    b. L'audit interne.
    c. Le Conseil et la direction générale.
    d. L'auditeur externe.

Copyright © 2015 Eyrolles.

Thèmes de discussion

A. Vous étudiez à la bibliothèque de votre université pour préparer votre prochain examen d'audit interne avec Mark et Ann, deux de vos camarades.

Mark : « Je ne comprends vraiment pas ces pistes d'audit descendantes et ascendantes. Par exemple, quelle est la différence si je commence par les factures de vente et que je les compare aux documents d'expédition ou si je commence par les documents d'expédition et que je les compare aux factures de vente ? »

Ann : « Je ne comprends pas non plus. J'espère qu'il n'y aura pas de questions là-dessus à l'examen. »

Vous : « Je ne parierai pas dessus ! M. Smart semble aimer nous poser des questions difficiles. Je crois qu'il vaut donc mieux que nous arrivions à comprendre et que nous soyons préparés. Deux précautions valent mieux qu'une. »

Considérez les deux objectifs d'audit suivants.

1. Déterminer si les ventes facturées aux clients ont été expédiées.
2. Déterminer si les livraisons aux clients ont été facturées.

Répondez aux questions suivantes :

a. Quelle est la différence entre ces deux objectifs d'audit ?

b. Quelle procédure d'audit mettriez-vous en œuvre pour atteindre chaque objectif d'audit ? Détaillez votre réponse.

c. Pourquoi est-il important que, pour chaque objectif d'audit, vous sélectionniez le document approprié comme point de départ pour votre test d'audit et que vous compariez ces deux documents ?

B. Une division de votre organisation a acheté un grand nombre de nouveaux ordinateurs de bureau sur l'exercice en cours. Un directeur de l'audit interne vous demande d'auditer le processus mis en œuvre pour cet achat. Il souhaite également que vous déterminiez si les ordinateurs sont utilisés et comptabilisés correctement. Ce directeur a spécifié un ensemble d'objectifs d'audit pour vous guider dans vos vérifications. Il souhaite notamment que vous déterminiez si :

1. l'achat des ordinateurs a été dûment autorisé ;
2. les responsabilités vis-à-vis des ordinateurs sont correctement séparées ;
3. les ordinateurs, ainsi que les logiciels et les informations qu'ils contiennent, sont bien protégés. Il convient de tenir compte à la fois de l'accès physique et de l'accès logique ;
4. les lois et règlements portant sur l'utilisation de logiciels sont respectés ;
5. les ordinateurs, comptabilisés dans les achats, existent réellement ;
6. tous les ordinateurs achetés ont été comptabilisés ;

Copyright © 2015 Eyrolles.

7. les montants enregistrés pour l'achat des ordinateurs sont corrects ;
8. la durée de vie utile estimée et la valeur de récupération des ordinateurs sont raisonnables ;
9. la dotation aux amortissements a été calculée correctement.

a. Décrivez les procédures que vous pourriez appliquer pour comprendre comment les ordinateurs ont été achetés, utilisés et comptabilisés.

b. Décrivez les procédures que vous pourriez appliquer pour atteindre chacun des objectifs d'audit énoncés ci-dessus ? Détaillez votre réponse.

C. Nous disposons des informations suivantes concernant l'organisation MVF (les sommes sont exprimées en millions) :

	2009	2008	2007	2006
Chiffre d'affaires net	23,2	21,7	19,6	17,4
Coût des produits vendus	17,1	16,8	15,2	13,5
Stock initial de produits finis	2,3	2,1	1,9	1,5
Stock final de produits finis	2,9	2,3	2,1	1,9
Coût des matières premières	10,6	8,8	7,5	7,1

1. Calculez les ratios suivants pour chaque exercice :
   - Ratio de marge brute.
   - Rotation des stocks de produits finis.
   - Part des matières premières dans le coût des produits finis.

2. Analysez les résultats obtenus au point 3.a. ci-dessus.
   - Décrivez l'évolution des ratios observée pour 2009.
   - Proposez au moins deux causes possibles pour chaque évolution observée[4].

Copyright © 2015 Eyrolles.

Thèmes de discussion

D. L'ensemble du chiffre d'affaires de l'organisation Kola correspond à des ventes à crédit, expédiées franco de port au point d'expédition. Normalement, Kola enregistre les transactions (c'est-à-dire les ventes et les coûts des marchandises vendues) tout au long de l'année à la date de facturation. L'auditeur interne a relevé les informations suivantes, qu'il a consignées dans ses papiers de travail.

Numéro de facture	Date d'expédition	Date de facturation
8351	28/12/2008	29/12/2008
8352	29/12/2008	02/01/2009
8353	02/01/2009	31/12/2008
8354	02/01/2009	03/01/2009

1. Décrivez quelles procédures d'audit spécifiques il convient de mettre en œuvre pour déterminer si les transactions de vente se déroulant immédiatement avant et après la fin de l'exercice sont comptabilisées sur la bonne période.

2. Indiquez quelles écritures de régularisation (ignorez les montants) l'auditeur interne doit proposer, en se basant sur les données ci-dessus, relatives à la date de séparation des exercices (*seizure, cut-off*). Donnez une explication claire et concise pour chaque écriture proposée.

E. Les auditeurs internes sont tenus de documenter leurs travaux dans des papiers de travail qui permettent une documentation complète, exacte et concise du processus d'audit. Expliquez quelles peuvent être les conséquences négatives d'une mauvaise préparation des papiers de travail dans le cadre d'une mission d'audit interne.

Copyright © 2015 Eyrolles.


Copyright © 2015 Eyrolles



CHAPITRE 11
L'ÉCHANTILLONNAGE EN AUDIT

Objectifs pédagogiques

- Comprendre l'échantillonnage en audit et les risques d'audit y afférents.
- Savoir mettre en œuvre un échantillonnage statistique et non statistique pour tester des contrôles.
- Être au fait des autres méthodes d'échantillonnage statistique utilisées pour tester des valeurs monétaires.

Le chapitre 10, *Les preuves d'audit et les papiers de travail*, décrit les procédures d'audit comme des tâches spécifiques que les auditeurs internes doivent effectuer pour atteindre les objectifs prescrits pour une mission d'audit interne. Il examine en quoi l'obtention de preuves adéquates et suffisantes, pour réaliser les objectifs de la mission, dépend de la nature, de l'étendue et du calendrier d'application des procédures exécutées.

Le présent chapitre s'intéresse à la *portée* des procédures que l'auditeur interne doit réaliser pour rassembler les quantités de preuves requises pour atteindre les objectifs de la mission. Des contraintes économiques et de temps empêchent généralement les auditeurs internes de tester la totalité de ce qu'ils souhaiteraient tester. L'échantillonnage en audit consiste, par définition, à appliquer une procédure d'audit à moins de 100 % des éléments d'une population concernée par une mission, afin d'en tirer une conclusion pour l'ensemble de la population. Il est très fréquemment utilisé par les auditeurs internes pour tester le fonctionnement effectif des contrôles.

Plus précisément, ce chapitre introduit les deux grandes approches générales de l'échantillonnage en audit : l'approche statistique et l'approche non statistique. Il décrit en outre le risque d'échantillonnage et le risque discrétionnaire. Il présente également les échantillonnages statistique et non statistique, tels qu'ils sont appliqués par les auditeurs internes lorsqu'ils testent les contrôles. Enfin, il explore deux méthodes d'échantillonnage statistique que les auditeurs internes utilisent pour obtenir des preuves directes concernant l'exactitude des valeurs monétaires.

Le lecteur pourra se reportera à la MPA 2320-3, L'échantillonnage en audit, publiée en mai 2013, ou à d'autres sources dont certaines sont citées dans ce chapitre.

INTRODUCTION À L'ÉCHANTILLONNAGE EN AUDIT

Comme indiqué ci-dessus, l'*échantillonnage en audit* consiste à appliquer une procédure d'audit à moins de 100 % des éléments d'une population, afin d'en tirer une conclusion pour l'ensemble de la population. Une population d'audit peut être, par exemple, l'ensemble des bordereaux de réception établis pendant l'exercice, ou tous les soldes du grand livre auxiliaire des comptes clients. L'échantillonnage est le plus souvent utilisé lorsque l'on met en œuvre des procédures d'audit telles que la vérification par piste d'audit ascendante (*vouching*) et descendante (*tracing*), qui nécessitent l'inspection d'une forme de piste d'audit constituée de pièces compilées manuellement. Il peut aussi être éventuellement appliqué à des procédures d'audit telles que la demande de renseignements ou l'observation. Si les résultats de l'étude d'un ensemble restreint de transactions au moyen d'un processus particulier en vue de mieux en comprendre le fonctionnement n'ont pas vocation à être extrapolés à l'ensemble de la population, il ne s'agit pas d'un échantillonnage.

Grâce aux progrès dans les SI, les auditeurs internes n'utilisent plus autant l'échantillonnage. En effet, il suffit de tester une seule fois le fonctionnement effectif d'un contrôle intégré dans un programme applicatif pour déterminer s'il fonctionne de manière effective à un moment donné. L'auditeur interne s'appuiera ensuite sur diverses procédures, telles que le test des contrôles, lorsque des changements sont apportés au programme applicatif, pour obtenir l'assurance que le contrôle a fonctionné de façon constante sur une période donnée. Par ailleurs, il est plus rapide de tester 100 % des éléments stockés dans un fichier informatique au moyen d'un logiciel d'audit généralisé que d'en sélectionner et d'en tester un échantillon.

Deux approches de l'échantillonnage en audit

Il existe deux approches d'échantillonnage : statistique et non statistique. Elles font toutes deux appel au jugement professionnel, tant dans la conception du plan d'échantillonnage que dans l'exécution de ce plan et l'analyse des résultats obtenus. L'auditeur interne choisira l'une ou l'autre en fonction des procédures d'audit spécifiques qu'il entend mettre en œuvre, de son avis sur le caractère approprié des preuves ainsi obtenues ou des actions qu'il entreprendra selon les résultats de l'échantillonnage. Ces deux approches peuvent apporter des preuves suffisantes et adéquates si elles sont appliquées correctement. L'échantillonnage non statistique est parfois appelé « échantillonnage au jugé » ; les auteurs ont délibérément choisi de ne pas utiliser cette terminologie afin d'éviter toute confusion. En effet, le jugement d'un expert de l'audit intervient aussi bien dans l'échantillonnage statistique que dans l'échantillonnage non statistique.

Copyright © 2015 Eyrolles.

Le choix que l'auditeur interne doit opérer entre les deux méthodes se résume en fait à un arbitrage coût/avantages. L'échantillonnage statistique est un outil qui peut aider l'auditeur interne à mesurer le caractère suffisant des preuves obtenues et à évaluer quantitativement les résultats d'échantillonnage. Il lui permet surtout de quantifier, de mesurer et de maîtriser le risque d'échantillonnage. C'est pourquoi on estime généralement que l'échantillonnage statistique apporte des preuves plus convaincantes que l'échantillonnage non statistique. Cependant, il est aussi considéré comme plus onéreux : il induit des coûts de formation supplémentaires. Il génère également un surcoût lors de la définition de l'échantillon, le choix des éléments à examiner et l'évaluation des résultats. Les échantillonnages statistique et non statistique sont détaillés dans la suite de ce chapitre.

Risque d'audit, risque d'échantillonnage

Risque d'audit

Risque d'aboutir à une conclusion d'audit non valide et/ou d'apporter un conseil inadéquat sur la base des travaux d'audit menés.

Comme nous l'avons vu dans le chapitre 10, *Les preuves d'audit et les papiers de travail*, le risque d'audit est le risque d'aboutir à une conclusion d'audit non valide et/ou d'apporter un conseil inadéquat sur la base des travaux d'audit menés. Dans le contexte de l'échantillonnage, il recouvre deux types de risques : le risque d'échantillonnage et le risque discrétionnaire.

Également appelé risque aléatoire, *le risque d'échantillonnage* est le risque que les conclusions que l'auditeur interne tire du test d'un échantillon diffèrent de celles qu'il aurait tirées si la procédure d'audit avait été appliquée à la totalité de la population. Cela tient au fait que l'on teste moins de 100 % des éléments de la population. Même un échantillon correctement sélectionné peut ne pas être représentatif de la population. Il existe une relation inverse entre le risque d'échantillonnage et la taille de l'échantillon. Si l'auditeur interne teste 100 % d'une population (il ne s'agit donc pas d'un échantillon), il n'y a pas de risque d'échantillonnage.

Lorsque l'auditeur interne teste des contrôles, il doit prêter attention à deux aspects du risque d'échantillonnage :

Le risque de sous-estimer le risque de non-contrôle (erreur de type II ou risque de 2e espèce ou risque bêta). Également assimilable au risque de surestimation de l'efficacité des contrôles internes, il s'agit de l'éventualité que le niveau de risque de non-contrôle évalué à partir des résultats de l'échantillonnage soit inférieur à ce que l'auditeur interne aurait trouvé si 100 % de la population avait été testée. En d'autres termes, c'est le risque que l'auditeur interne conclue à un niveau d'efficacité d'un contrôle donné supérieur à ce qu'il n'est en réalité. On peut encore le formuler autrement : il s'agit du risque que l'auditeur interne surestime la confiance que le management peut placer dans un contrôle pour ramener le risque résiduel à un niveau suffisamment faible.

Copyright © 2015 Eyrolles.

Le risque de surestimer le risque de non-contrôle (erreur de type I ou risque de 1re espèce ou risque alpha). Également assimilable au risque de sous-estimation de l'efficacité des contrôles internes, il s'agit de l'éventualité que le niveau de risque de non-contrôle évalué à partir des résultats de l'échantillonnage soit supérieur à ce que l'auditeur interne aurait trouvé si 100 % de la population avait été testée. En d'autres termes, c'est le risque que l'auditeur interne conclue à un niveau d'efficacité d'un contrôle donné inférieur à ce qu'il n'est en réalité. On peut encore le formuler autrement : il s'agit du risque que l'auditeur interne sous-estime la confiance que le management peut placer dans un contrôle pour ramener le risque résiduel à un niveau suffisamment faible.

Risque d'échantillonnage

Risque que les conclusions que l'auditeur interne tire du test d'un échantillon diffèrent de celles qu'il aurait tirées si la procédure d'audit avait été appliquée à la totalité de la population. Également appelé risque aléatoire.

Le *risque de non-contrôle*, auquel il est fait référence pour la première fois dans les deux paragraphes précédents, est le risque que les contrôles ne permettent pas de ramener un *risque maîtrisable* à un niveau acceptable. Nous avons vu dans le chapitre 6, *Le contrôle interne*, que le risque maîtrisable est la portion du risque inhérent que le management peut réduire grâce aux activités quotidiennes. Les contrôles sont précisément effectués dans le but de réduire le risque maîtrisable, l'objectif étant de le ramener à un niveau correspondant au seuil de tolérance au risque fixé par le management (c'est-à-dire le niveau de risque qui semble acceptable par le management). Le *risque résiduel* est le risque qui subsiste après que les contrôles ont été effectués. Si le risque résiduel dépasse la tolérance au risque du management, alors les contrôles sont inefficaces, soit parce que leur conception est inadéquate, soit parce qu'ils ne fonctionnent pas de manière effective. Si le risque est ramené en deçà du seuil de tolérance, alors les contrôles internes sont supposés être conçus de manière adéquate et fonctionner de manière effective. Cependant, il y a également un risque que les contrôles soient excessifs et mobilisent davantage de ressources que nécessaire.

Risque discrétionnaire

Risque qui survient du fait d'une mauvaise sélection, application ou interprétation d'une procédure d'audit de la part de l'auditeur interne.

Contrairement au risque d'échantillonnage, le *risque discrétionnaire*, ou risque non lié à la sélection d'un échantillon, ne découle pas du fait que l'on teste moins de 100 % des éléments d'une population. Ce risque renvoie à la possibilité de commettre des erreurs telles qu'appliquer des procédures d'audit inappropriées, de mal appliquer une procédure appropriée (notamment si l'auditeur interne ne détecte pas un écart par rapport au contrôle prescrit ou une erreur de montant) ou de mal interpréter les résultats de l'échantillonnage. Il est maîtrisé (ramené à un niveau suffisamment faible) grâce à une planification appropriée de l'audit, à la supervision de chaque mission d'audit et à l'application généralisée de procédures d'assurance qualité adéquates.

Copyright © 2015 Eyrolles.

ÉCHANTILLONNAGE STATISTIQUE DANS LES TESTS DES CONTRÔLES

Les méthodes d'échantillonnage d'attributs

Échantillonnage d'attributs

Méthode d'échantillonnage statistique qui permet d'aboutir à une conclusion grâce au calcul d'un taux d'occurrence dans une population.

L'*échantillonnage d'attributs* (ou échantillonnage sur attribut ou échantillonnage par attribut) est une méthode d'échantillonnage statistique reposant sur la loi binomiale (loi de Bernoulli), qui permet d'aboutir à une conclusion grâce au calcul d'un taux d'occurrence dans une population. La distribution binomiale est la distribution de tous les échantillons possibles où chaque élément de la population se trouve dans l'un des deux états possibles (par exemple écart ou absence d'écart par rapport au contrôle prescrit). L'échantillonnage d'attributs est le plus souvent utilisé pour évaluer l'efficacité d'un contrôle donné. L'auditeur interne teste le taux d'écarts par rapport au contrôle tel que prescrit, afin de déterminer si ce taux d'occurrence est « acceptable » et, en conséquence, s'il est raisonnable de se fier à ce contrôle. Généralement, l'approche la plus générique d'échantillonnage d'attributs suppose de sélectionner un seul échantillon dont la taille a été calculée mathématiquement.

L'*échantillonnage d'attributs stratifié* est une variante de l'échantillonnage d'attributs applicable à une population qui peut être subdivisée. Par exemple, une population de transactions d'achats peut être scindée en celles de montant relativement peu élevé, que les managers locaux peuvent autoriser, celles de montant moyen, qui doivent être approuvées par les managers régionaux, et celles de gros montant, qui nécessitent le feu vert de la direction générale. Si des contrôles différents sont appliqués à des transactions de même type mais à des niveaux différents, ces niveaux doivent être pris en compte séparément comme des populations distinctes. La raison en est simple : lorsque les contrôles mis en œuvre sont différents, leur niveau d'efficacité peut varier.

L'*échantillonnage stop-or-go* ou séquentiel constitue une autre variante de l'échantillonnage d'attributs. Il est tout à fait approprié lorsque l'on prévoit des taux d'écarts très faibles, car il réduit au minimum la taille de l'échantillon nécessaire pour un niveau donné de risque d'échantillonnage. Un échantillon initial relativement restreint est extrait et analysé. L'auditeur interne décide alors, en fonction des résultats tirés de cet échantillon de base, si l'échantillon doit être agrandi. S'il constate un nombre suffisamment faible d'écarts dans l'échantillon initial, il arrête l'échantillonnage et formule ses conclusions. Si le nombre d'écarts constatés est supérieur au niveau considéré comme suffisamment faible, l'auditeur interne extrait davantage d'éléments avant de tirer une conclusion.

L'*échantillonnage de dépistage* est une troisième variante de l'échantillonnage d'attributs. L'échantillon est conçu de manière à contenir au moins un écart, si un tel écart est observé dans la

Copyright © 2015 Eyrolles.

population à un taux donné. Un échantillon statistique est extrait de façon à ce que l'auditeur interne puisse tester la probabilité de trouver au moins un écart. Cette méthode est le plus souvent utilisée pour détecter une fraude. Elle est tout à fait appropriée lorsque l'on prévoit des taux d'écarts très faibles et que l'auditeur interne souhaite définir un échantillon à partir d'une probabilité donnée de trouver une occurrence. En raison du contexte dans lequel s'applique l'échantillonnage de dépistage et de la nature des écarts potentiels recherchés, l'échantillon est généralement bien plus grand que ceux utilisés dans l'échantillonnage d'attributs classique.

Élaborer un plan d'échantillonnage d'attributs, exécuter ce plan et en analyser les résultats

L'échantillonnage d'attributs se déroule en neuf étapes.

1. Définir un objectif de contrôle interne précis et identifier le ou les contrôles qui permettront d'atteindre cet objectif.
2. Définir ce que l'on entend par écart par rapport au contrôle prescrit.
3. Définir la population et l'unité d'échantillonnage.
4. Déterminer les valeurs appropriées pour les facteurs ayant une incidence sur la taille de l'échantillon.
5. Déterminer la taille adéquate de l'échantillon.
6. Extraire l'échantillon de manière aléatoire.
7. Auditer les éléments de l'échantillon retenu et dénombrer les écarts par rapport au contrôle prescrit.
8. Déterminer le plafond d'écarts tolérés.
9. Évaluer les résultats d'échantillonnage.

Chacune de ces étapes est explicitée ci-dessous et illustrée à partir de la situation hypothétique suivante : un auditeur interne doit utiliser un échantillonnage statistique pour tester les contrôles portant sur les acquisitions de matériel. Précisément, l'objectif d'audit essentiel est de déterminer si tous ces achats ont obtenu l'autorisation adéquate.

Étape 1 : définir un objectif de contrôle interne précis et identifier le ou les contrôles qui permettront d'atteindre cet objectif

L'objectif d'audit précis est le principal facteur qui permet de déterminer ce qu'il faut sonder. Dans notre exemple, le but de l'audit est de déterminer si tous les achats de matériel ont reçu l'autorisation

Copyright © 2015 Eyrolles.

adéquate. Il se rapporte à l'objectif de validité des transactions que se fixe l'organisation : le management veut être sûr que tous les achats sont valides, autrement dit qu'aucun achat non autorisé n'a été effectué. En conséquence, l'objectif du contrôle interne est de donner une assurance raisonnable que l'objectif du management est atteint (à savoir que toutes les acquisitions ont bien obtenu l'autorisation adéquate). La définition précise du contrôle et de son objectif est cruciale. À défaut, l'auditeur interne risque d'appliquer des procédures d'audit inappropriées et, par conséquent, de tirer des conclusions erronées. C'est là un exemple de risque discrétionnaire.

Dans notre exemple, supposons que la politique d'acquisition de matériel de l'organisation précise que les achats sont déclenchés par l'élaboration, par la personne habilitée, d'une demande écrite formelle (demande d'achat) pour le matériel nécessaire. Les demandes d'achat ayant reçu une autorisation sont transmises au service des approvisionnements, où elles servent d'autorisation pour commander le matériel requis. Le service des approvisionnements remplit un bon de commande prénuméroté, qui fait alors partie de la piste d'audit constituée de documents probants à l'appui des transactions d'achat. L'auditeur interne décide de vérifier, sur la base d'un échantillon, si les bons de commande préparés sur les 12 derniers mois s'appuient sur des demandes d'achat ayant reçu l'autorisation adéquate.

Étape 2 : définir ce que l'on entend par écart par rapport au contrôle prescrit

Il est tout aussi important de définir soigneusement le contrôle et son objectif que de définir soigneusement ce que l'on entend par écart par rapport à un contrôle prescrit (autrement dit, l'attribut de contrôle pertinent). À défaut, l'auditeur interne risque de ne pas détecter un écart, ce qui constitue un autre cas de risque discrétionnaire.

Dans notre exemple, l'auditeur interne souhaite s'assurer que les bons de commande s'appuient sur des demandes d'achat ayant reçu l'autorisation adéquate. Les éléments suivants peuvent constituer des écarts par rapport au contrôle prescrit : demande d'achat manquante, absence de preuve concernant l'approbation de la demande d'achat, approbation émanant d'une personne non habilitée, différence entre les articles achetés conformément au bon de commande et les articles requis dans la demande d'achat.

Copyright © 2015 Eyrolles.

Étape 3 : définir la population et l'unité d'échantillonnage

Comme indiqué à l'étape 1, l'objectif d'audit consiste, dans notre exemple, à tester la validité des bons de commande. La piste d'audit ascendante (*vouching*) permet de tester la validité des informations enregistrées. Elle consiste à vérifier si les informations contenues dans un document sont corroborées par celles contenues dans le document établi en amont (la demande d'achat).

La population qui intéresse l'auditeur interne est, dans notre exemple, la population des bons de commande prénumérotés remplis au cours des 12 derniers mois. L'unité d'échantillonnage est chaque bon de commande qui est testé en vue de déterminer s'il s'appuie sur une demande d'achat ayant reçu l'autorisation adéquate. Pour effectuer son contrôle, l'auditeur interne doit partir des bons de commande et rapprocher chacun avec la demande d'achat correspondante.

Pourquoi serait-il inapproprié, dans notre exemple, que l'auditeur interne suive une piste d'audit descendante (*tracing*) en partant des demandes d'achat afin de déterminer si un bon de commande correspondant a été établi ? Souvenons-nous que l'objectif d'audit était de déterminer si les bons de commande s'appuyaient sur une demande d'achat ayant reçu l'autorisation adéquate. Si l'auditeur interne extrait un échantillon de demandes d'achat et observe leur traitement ultérieur jusqu'à l'établissement du bon de commande, il n'aura aucune chance de déceler une situation dans laquelle un bon de commande existant n'a pas fait suite à une demande d'achat.

Étape 4 : déterminer les valeurs appropriées pour les facteurs ayant une incidence sur la taille de l'échantillon

Facteurs ayant une incidence sur la taille de l'échantillon

– Le niveau acceptable de risque de sous-estimer le risque de non-contrôle.
– Le taux d'écarts acceptable.
– Le taux d'écarts attendu de la population.

Dans l'échantillonnage d'attributs, l'auditeur interne doit exercer son jugement professionnel lorsqu'il précise les valeurs appropriées pour les trois facteurs ayant une incidence sur la taille de l'échantillon :

- le niveau acceptable de risque de sous-estimer le risque de non-contrôle (lié au niveau de confiance) ;
- le taux d'écarts acceptable ;
- le taux d'écarts attendu de la population.

Notons que la taille de la population a peu d'influence sur la taille de l'échantillon pour l'échantillonnage d'attributs, sauf si la population est très restreinte. Pour les populations comptant moins de 200 éléments, la taille de l'échantillon est directement corrélée à la taille de la population. La taille de l'échantillon augmentera légèrement pour les populations comptant de 200 à 2 000 éléments.[1]

Copyright © 2015 Eyrolles.

Les tables de tailles d'échantillon calculées statistiquement et présentées dans l'encadré 11-1 s'appuient sur de vastes populations, à savoir plus de 2 000 éléments. C'est donc faire preuve de prudence que de les utiliser pour une population de moins de 2 000 éléments. L'auditeur interne pourra cependant prendre en compte la taille de la population aux fins de l'efficience de l'audit dans le cas où un contrôle n'est pas effectué fréquemment (par exemple moins d'une fois par semaine).

Pour notre exemple, supposons que la population compte 2 500 bons de commande.

Le niveau acceptable de risque de sous-estimer le risque de non-contrôle. Rappelons qu'il s'agit du risque que l'auditeur interne conclue à un niveau d'efficacité d'un contrôle donné supérieur à ce qu'il n'est en réalité. Il existe une relation inverse entre le risque de sous-estimer le risque de non-contrôle et la taille de l'échantillon : plus le niveau de risque acceptable est bas, plus l'échantillon doit être grand.

Risque de sous-estimer le risque de non-contrôle

Risque que l'auditeur interne conclue à un niveau d'efficacité d'un contrôle donné supérieur à ce qu'il n'est en réalité.

Le jugement professionnel émis par l'auditeur interne à propos du niveau acceptable pour le risque de sous-estimer le risque de non-contrôle dépend du degré de confiance qu'il souhaite atteindre dans l'exactitude des conclusions qu'il tirera concernant le fonctionnement effectif de la procédure de contrôle testée. En fait, le risque de sous-estimer le risque de non-contrôle est le complément inverse du niveau de confiance, également appelé niveau de fiabilité (par exemple, si l'auditeur interne décide de fixer à 5 % le risque de sous-estimer le risque de non-contrôle, il indique qu'il souhaite obtenir un niveau de confiance de 95 % d'aboutir à une conclusion correcte). Les deux niveaux acceptables de risque de sous-estimer le risque de non-contrôle les plus couramment utilisés sont 5 % et 10 %. Pour notre exemple, supposons que l'auditeur interne décide de fixer ce niveau à 10 % (notons que le risque de surestimer le risque de non-contrôle n'est pas explicitement pris en compte lors de la définition de la taille appropriée de l'échantillon pour un échantillonnage d'attributs).

Le taux d'écarts acceptable. Rappelons qu'il s'agit du taux d'écarts maximal que l'auditeur interne est prêt à accepter tout en concluant que le contrôle présente un niveau d'efficacité acceptable (en d'autres termes, que l'on peut se fier au contrôle pour ramener le risque résiduel à un niveau suffisamment faible). Il existe une relation inverse entre le taux d'écarts acceptable et la taille de l'échantillon.

Taux d'écarts acceptable

Taux d'écarts maximal que l'auditeur interne est prêt à accepter tout en concluant que le contrôle présente un niveau d'efficacité acceptable.

Le jugement professionnel émis par l'auditeur interne à propos du taux d'écarts acceptable repose sur l'importance relative du contrôle testé. Si, par exemple, l'auditeur interne estime que le contrôle est

Copyright © 2015 Eyrolles.

critique, il fixera le taux d'écarts acceptable à un niveau très bas. Supposons, dans notre cas, que ce taux est fixé à 5 %.

Taux d'écarts attendu de la population

Meilleure estimation, par l'auditeur interne, du taux d'écarts effectif dans la population d'éléments examinés.

Le taux d'écarts attendu de la population. Il s'agit de la meilleure estimation, par l'auditeur interne, du taux d'écarts effectif dans la population d'éléments examinés. Le taux d'écarts attendu de la population a une incidence directe sur la taille de l'échantillon. Cependant, ce taux devra être inférieur au taux d'écarts acceptable, sans quoi l'auditeur interne ne procédera pas à l'échantillonnage d'attributs envisagé. Pour les auditeurs internes, la différence entre taux d'écarts acceptable et attendu correspond à la *marge de tolérance prévue pour le risque d'échantillonnage ou précision prévue*.

Si l'auditeur interne a au préalable recouru à un échantillonnage d'attributs pour vérifier l'efficacité d'un contrôle donné, le niveau adéquat pour le taux d'écarts attendu de la population sera le même que celui utilisé précédemment, corrigé de tout changement connu dans l'application du contrôle. Sinon, l'auditeur interne peut sélectionner et auditer un petit échantillon préliminaire afin de déterminer le taux d'écarts attendu. Supposons que, dans notre exemple, l'auditeur interne estime le taux d'écarts de la population à 1 %.

Étape 5 : déterminer la taille adéquate de l'échantillon

Une fois que l'auditeur interne a fixé les valeurs des facteurs ayant une incidence sur la taille de l'échantillon, le moyen le plus simple de déterminer la taille adéquate de l'échantillon consiste à se référer aux tables de tailles d'échantillon, que l'on trouve facilement, telles que celles présentées dans l'encadré 11-1.

Dans notre exemple, l'auditeur interne a fixé le risque de sous-estimer le risque de non-contrôle à 10 %, le taux d'écarts acceptable à 5 % et le taux d'écarts attendu de la population à 1 %. L'encadré 11-1 montre que la taille d'échantillon adéquate est alors de 77. L'auditeur interne peut arrondir ce chiffre à 80 pour des raisons que nous expliquerons à l'étape 8 ci-dessous.

Notons que ce calcul de la taille de l'échantillon est extrêmement utile pour l'échantillonnage statistique. Si l'auditeur interne souhaite un niveau de confiance de 100 % dans la conclusion à laquelle il aboutira concernant la validité des bons de commande, il lui faudra procéder à un rapprochement pour 100 % d'entre eux. En revanche, on peut atteindre un niveau de confiance de 90 % (complémentaire d'un risque de 10 % de sous-estimer le risque de non-contrôle) grâce au rapprochement par piste d'audit ascendante de 80 bons de commande.

Copyright © 2015 Eyrolles.

TABLES DE TAILLES D'ÉCHANTILLON POUR L'ÉCHANTILLONNAGE D'ATTRIBUTS

Risque de 5 % de sous-estimer le risque de non-contrôle

Taux d'écarts attendu de la population (%)	Taux d'écarts acceptable (entre parenthèses, le nombre d'erreurs attendues)								
	2 %	3 %	4 %	5 %	6 %	7 %	8 %	9 %	10 %
0,00	149 (0)	99 (0)	74 (0)	59 (0)	49 (0)	42 (0)	36 (0)	32 (0)	29 (0)
0,50	313 (2)	157 (1)	117 (1)	93 (1)	78 (1)	66 (1)	58 (1)	51 (1)	46 (1)
1,00	590 (6)	257 (3)	156 (2)	93 (1)	78 (1)	66 (1)	58 (1)	51 (1)	46 (1)
1,50	— —	392 (6)	192 (3)	124 (2)	103 (2)	66 (1)	58 (1)	51 (1)	46 (1)
2,00	— —	846 (17)	294 (6)	181 (4)	127 (3)	88 (2)	77 (2)	68 (2)	46 (1)
2,50	— —	— —	513 (13)	234 (6)	150 (4)	109 (3)	77 (2)	68 (2)	61 (2)
3,00	— —	— —	1 098 (33)	361 (11)	195 (6)	129 (4)	95 (3)	84 (3)	61 (2)
4,00	— —	— —	— —	1 348 (54)	421 (17)	221 (9)	146 (6)	100 (4)	89 (4)
5,00	— —	— —	— —	— —	1 580 (79)	478 (24)	240 (12)	158 (8)	116 (6)
6,00	— —	— —	— —	— —	— —	1 832 (110)	532 (32)	266 (16)	179 (11)

Risque de 10 % de sous-estimer le risque de non-contrôle

Taux d'écarts attendu de la population (%)	Taux d'écarts acceptable (entre parenthèses, le nombre d'erreurs attendues)								
	2 %	3 %	4 %	5 %	6 %	7 %	8 %	9 %	10 %
0,00	114 (0)	76 (0)	57 (0)	45 (0)	38 (0)	32 (0)	28 (0)	25 (0)	22 (0)
0,50	194 (1)	129 (1)	96 (1)	77 (1)	64 (1)	55 (1)	48 (1)	42 (1)	38 (1)
1,00	398 (4)	176 (2)	96 (1)	77 (1)	64 (1)	55 (1)	48 (1)	42 (1)	38 (1)
1,50	1 463 (22)	265 (4)	132 (2)	105 (2)	64 (1)	55 (1)	48 (1)	42 (1)	38 (1)
2,00	— —	590 (12)	198 (4)	132 (3)	88 (2)	75 (2)	48 (1)	42 (1)	38 (1)
2,50	— —	— —	353 (9)	158 (4)	110 (3)	75 (2)	65 (2)	58 (2)	38 (1)
3,00	— —	— —	730 (22)	258 (8)	132 (4)	94 (3)	65 (2)	58 (2)	52 (2)
4,00	— —	— —	— —	873 (35)	274 (11)	149 (6)	98 (4)	73 (3)	65 (3)
5,00	— —	— —	— —	— —	1 019 (51)	318 (16)	160 (8)	115 (6)	78 (4)
6,00	— —	— —	— —	— —	— —	1 150 (69)	349 (21)	182 (11)	116 (7)

Note : Les échantillons comportant plus de 2 000 éléments ne sont pas présentés. Ces tables supposent une vaste population.

D'après *Audit Guide : Audit Sampling, American Institute of Certified Public Accountants*, 2008, p.112–113.
Copyright 2008, AICPA. Adaptation autorisée.

ENCADRÉ 11-1

Étape 6 : extraire l'échantillon de manière aléatoire

Lorsque l'on applique un échantillonnage aux tests des contrôles, il importe que des éléments provenant de l'ensemble de la période auditée aient une chance d'être sélectionnés. Avec un échantillonnage statistique, il est également essentiel que l'auditeur interne

Copyright © 2015 Eyrolles.

Échantillonnage aléatoire

Prélèvement d'un échantillon tel que tous les éléments de la population ont une probabilité de sélection égale.

emploie une technique de sélection aléatoire (en d'autres termes, tous les éléments de la population doivent avoir une probabilité de sélection égale). Les deux méthodes les plus courantes pour sélectionner un échantillon sur attribut sont l'échantillonnage aléatoire simple et l'échantillonnage systématique avec une ou plusieurs origines choisies au hasard.

L'*échantillonnage aléatoire simple* est généralement la méthode la plus simple lorsque l'on échantillonne des documents prénumérotés. L'auditeur interne peut par exemple utiliser une table de nombres aléatoires, ou bien un générateur de nombres aléatoires (programme informatique).

Pour l'*échantillonnage systématique*, l'auditeur interne désigne une origine au hasard, puis sélectionne un élément tous les n. L'échantillonnage systématique est approprié dès lors qu'il n'y a pas de raison de penser que la régularité des intervalles biaisera systématiquement l'échantillon. Pour réduire la probabilité de sélectionner un échantillon biaisé, les auditeurs internes peuvent parfois choisir des origines multiples. Ils utilisent généralement l'échantillonnage systématique lorsque les différents éléments de la population ne sont pas prénumérotés.

Dans notre exemple, les bons de commande sont prénumérotés, si bien que l'auditeur interne choisit d'utiliser un générateur de nombres aléatoires pour sélectionner un échantillon aléatoire de bons de commande établis au cours des 12 derniers mois. La période de 12 mois couvre les trois derniers mois de l'exercice précédent et les neuf premiers de l'exercice en cours. Notons que l'auditeur interne n'a pas toujours la possibilité d'extraire l'échantillon de l'ensemble de l'exercice. Il doit en tenir compte lorsqu'il évalue les résultats d'échantillonnage.

Étape 7 : auditer les éléments de l'échantillon retenu et dénombrer les écarts par rapport au contrôle prescrit

Dans notre exemple, l'auditeur interne part des bons de commande de l'échantillon pour rapprocher chacun avec la demande d'achat correspondante. Chaque demande d'achat est inspectée de manière à trouver la preuve qu'une personne habilitée a donné son feu vert, et à vérifier la correspondance entre les articles achetés conformément au bon de commande et les articles requis dans la demande d'achat. Supposons deux issues possibles : (1) l'auditeur interne constate un écart (c'est-à-dire qu'en une occurrence, aucune demande d'achat ne correspond au bon de commande sélectionné dans l'échantillon), et (2) l'auditeur interne en constate deux (c'est-à-dire qu'en deux occurrences, aucune demande d'achat ne correspond au bon de commande sélectionné dans l'échantillon).

Copyright © 2015 Eyrolles.

Étape 8 : déterminer le plafond d'écarts tolérés

L'auditeur interne utilise les tables d'évaluation des échantillonnages d'attributs, telles que celles présentées dans l'encadré 11-2, pour déterminer le plafond d'écarts tolérés pour une application donnée.

Le plafond d'écarts tolérés pour les deux issues envisagées serait :

Nombre d'écarts dans l'échantillon	Plafond d'écarts tolérés
1	4,8 %
2	6,6 %

La raison pour laquelle nous avons suggéré, à l'étape 5, que l'auditeur interne pouvait arrondir la taille de l'échantillon à 80, au lieu de 77, s'explique ici clairement : les tables présentées à l'encadré 11-2 n'indiquent pas un plafond d'écarts tolérés pour absolument toutes les valeurs. Arrondir la taille de l'échantillon à la valeur suivante qui apparaît dans la table est un choix prudent. Une autre approche consiste à auditer un échantillon de 77 éléments et à calculer par interpolation le plafond d'écarts tolérés.

Étape 9 : évaluer les résultats d'échantillonnage

Évaluer les résultats d'un échantillonnage d'attributs suppose de :

- formuler une conclusion statistique ;
- prendre une décision d'audit sur la base de résultats quantitatifs ;
- prendre en compte les aspects qualitatifs des résultats d'échantillonnage.

Formuler une conclusion statistique. L'échantillonnage statistique a un grand avantage sur l'échantillonnage non statistique : il permet à l'auditeur interne de quantifier, mesurer et maîtriser le risque d'échantillonnage. Dans l'échantillonnage d'attributs, l'auditeur interne maîtrise explicitement le risque de sous-estimer le risque de non-contrôle, qui est complémentaire du niveau de confiance. Dans notre exemple, l'auditeur interne fixe à 10 % le risque de sous-estimer le risque de non-contrôle, valeur qui a été utilisée pour calculer la taille adéquate de l'échantillon. Pour déterminer le plafond d'écarts tolérés, il faut se référer à la partie de la table correspondant à un risque de 10 % de sous-estimer le risque de non-contrôle.

Pour l'auditeur interne, la meilleure estimation du taux d'écarts de la population concernant la première hypothèse (1 écart) est de 1/80 = 1,25 %. Concernant la seconde hypothèse (2 écarts), elle est

Copyright © 2015 Eyrolles.

de 2/80 = 2,5 %. Cependant, ces estimations ne sont pas exemptes d'incertitude, puisque l'auditeur interne a appliqué la procédure d'audit à un échantillon, autrement dit, il n'a pas testé 100 % de la population. En d'autres termes, il ne peut conclure avec certitude que le taux d'écarts de la population est de, respectivement, 1,25 % et 2,5 %.

Dans la première hypothèse (1 écart), l'auditeur interne peut tirer la conclusion statistique suivante.

- Je suis sûr à 90 % que la valeur vraie mais inconnue du taux d'écarts de la population est inférieure ou égale à 4,8 %.

Dans la deuxième hypothèse (2 écarts), l'auditeur interne peut tirer la conclusion statistique suivante.

- Je suis sûr à 90 % que la valeur vraie mais inconnue du taux d'écarts de la population est inférieure ou égale à 6,6 %.

Marge de tolérance obtenue pour le risque d'échantillonnage

Différence entre le taux d'écarts de l'échantillon et le plafond d'écarts tolérés.

Notons que la différence entre la meilleure estimation du taux d'écarts de la population (à savoir le taux d'écarts de l'échantillon) et le plafond d'écarts tolérés est appelée *marge de tolérance obtenue pour le risque d'échantillonnage* ou *précision obtenue*.

Prendre une décision d'audit sur la base de résultats quantitatifs. L'échantillonnage d'attributs a été conçu de façon à ce que l'auditeur interne puisse conclure que le contrôle est efficace, d'après les résultats de l'échantillonnage, si l'on pouvait établir avec un niveau de confiance de 90 % que la valeur vraie mais inconnue du taux d'écarts de la population est inférieure ou égale à 5 % (soit le taux d'écarts acceptable défini par l'auditeur interne). La première hypothèse répond à ce critère puisque le plafond d'écarts tolérés (4,8 %) est inférieur à 5 %. Tel n'est pas le cas pour la seconde, puisque le plafond d'écarts tolérés (6,6 %) est supérieur à 5 %.

Si le plafond d'écarts tolérés est inférieur ou égal au taux d'écarts acceptable, les résultats quantitatifs de l'échantillonnage d'attributs indiquent que le contrôle testé est suffisamment efficace (c'est-à-dire que l'on peut s'y fier pour ramener le risque résiduel à un niveau suffisamment faible). À l'inverse, si le plafond d'écarts tolérés est supérieur au taux d'écarts acceptable, les résultats quantitatifs de l'échantillonnage d'attributs indiquent que le contrôle testé n'est pas suffisamment efficace (c'est-à-dire que l'on ne peut pas s'y fier pour ramener le risque résiduel à un niveau suffisamment faible).

L'auditeur interne est alors prêt à interpréter les résultats quantitatifs de l'échantillon. Rappelons que l'objectif d'audit exprimé dans notre exemple est de déterminer si tous les achats de matériel ont bénéficié d'une autorisation adéquate. L'auditeur interne a défini à l'avance que son objectif était d'être à 90 % sûr que la

Copyright © 2015 Eyrolles.

TABLES D'ÉVALUATION DE L'ÉCHANTILLONNAGE D'ATTRIBUTS (PLAFONDS D'ÉCARTS TOLÉRÉS)

Risque de 5 % de sous-estimer le risque de non-contrôle

Taille de l'échantillon	Nombre effectif d'écarts constatés								
	0	1	2	3	4	5	6	7	8
20	14,0	21,7	28,3	34,4	40,2	45,6	50,8	55,9	60,7
25	11,3	17,7	23,2	28,2	33,0	37,6	42,0	46,3	50,4
30	9,6	14,9	19,6	23,9	28,0	31,9	35,8	39,4	43,0
35	8,3	12,9	17,0	20,7	24,3	27,8	31,1	34,4	37,5
40	7,3	11,4	15,0	18,3	21,5	24,6	27,5	30,4	33,3
45	6,5	10,2	13,4	16,4	19,2	22,0	24,7	27,3	29,8
50	5,9	9,2	12,1	14,8	17,4	19,9	22,4	24,7	27,1
55	5,4	8,4	11,1	13,5	15,9	18,2	20,5	22,6	24,8
60	4,9	7,7	10,2	12,5	14,7	16,8	18,8	20,8	22,8
65	4,6	7,1	9,4	11,5	13,6	15,5	17,5	19,3	21,2
70	4,2	6,6	8,8	10,8	12,7	14,5	16,3	18,0	19,7
75	4,0	6,2	8,2	10,1	11,8	13,6	15,2	16,9	18,5
80	3,7	5,8	7,7	9,5	11,1	12,7	14,3	15,9	17,4
90	3,3	5,2	6,9	8,4	9,9	11,4	12,8	14,2	15,5
100	3,0	4,7	6,2	7,6	9,0	10,3	11,5	12,8	14,0
125	2,4	3,8	5,0	6,1	7,2	8,3	9,3	10,3	11,3
150	2,0	3,2	4,2	5,1	6,0	6,9	7,8	8,6	9,5
200	1,5	2,4	3,2	3,9	4,6	5,2	5,9	6,5	7,2

Risque de 10 % de sous-estimer le risque de non-contrôle

Taille de l'échantillon	Nombre effectif d'écarts constatés								
	0	1	2	3	4	5	6	7	8
20	10,9	18,1	24,5	30,5	36,1	41,5	46,8	51,9	56,8
25	8,8	14,7	20,0	24,9	29,5	34,0	38,4	42,6	46,8
30	7,4	12,4	16,8	21,0	24,9	28,8	32,5	36,2	39,7
35	6,4	10,7	14,5	18,2	21,6	24,9	28,2	31,4	34,5
40	5,6	9,4	12,8	16,0	19,0	22,0	24,9	27,7	30,5
45	5,0	8,4	11,4	14,3	17,0	19,7	22,3	24,8	27,3
50	4,6	7,6	10,3	12,9	15,4	17,8	20,2	22,5	24,7
55	4,2	6,9	9,4	11,8	14,1	16,3	18,4	20,5	22,6
60	3,8	6,4	8,7	10,8	12,9	15,0	16,9	18,9	20,8
65	3,5	5,9	8,0	10,0	12,0	13,9	15,7	17,5	19,3

Copyright © 2015 Eyrolles.

Risque de 10 % de sous-estimer le risque de non-contrôle									
Taille de l'échantillon	**Nombre effectif d'écarts constatés**								
	0	1	2	3	4	5	6	7	8
70	3,3	5,5	7,5	9,3	11,1	12,9	14,6	16,3	18,0
75	3,1	5,1	7,0	8,7	10,4	12,1	13,7	15,2	16,8
80	2,9	4,8	6,6	8,2	9,8	11,3	12,8	14,3	15,8
90	2,6	4,3	5,9	7,3	8,7	10,1	11,5	12,8	14,1
100	2,3	3,9	5,3	6,6	7,9	9,1	10,3	11,5	12,7
125	1,9	3,1	4,3	5,3	6,3	7,3	8,3	9,3	10,2
150	1,6	2,6	3,6	4,4	5,3	6,1	7,0	7,8	8,6
200	1,2	2,0	2,7	3,4	4,0	4,6	5,3	5,9	6,5

Note : Cette table présente les plafonds (corps du tableau) en pourcentage.
Elle suppose une vaste population.

D'après *Audit Guide: Audit Sampling, American Institute of Certified Public Accountants*, 2008, p.114–115. Copyright 2008, AICPA. Adaptation autorisée.

valeur vraie mais inconnue du taux d'écarts est inférieure à 5 %. Comme indiqué plus haut, dans la première hypothèse, ce critère est rempli, mais pas dans la seconde. L'auditeur interne doit donc conclure, pour le premier cas, que le niveau d'efficacité du contrôle portant sur la validité des expéditions de marchandises est acceptable, c'est-à-dire que les résultats d'échantillonnage indiquent que l'on peut se fier à ce contrôle pour ramener le risque résiduel à un niveau suffisamment faible. Dans le second cas, en revanche, il doit conclure que le niveau d'efficacité du contrôle n'est pas acceptable, c'est-à-dire que les résultats de l'échantillonnage indiquent que l'on ne peut pas se fier à ce contrôle pour ramener le risque résiduel à un niveau suffisamment faible. Le second cas constitue une observation d'audit que l'auditeur interne doit documenter et inclure dans le rapport de la mission.

Il faut noter que l'interprétation, par l'auditeur interne, des résultats quantitatifs de l'échantillon porte sur l'efficacité du contrôle sur 12 mois, répartis comme suit : les trois derniers mois de l'exercice précédent et les neuf premiers de l'exercice en cours. Il serait inapproprié que l'auditeur interne tire, sur la base des résultats d'échantillonnage, une conclusion concernant l'efficacité du contrôle sur les trois derniers mois de l'exercice en cours puisque l'échantillon ne comportait pas de bons de commande édités sur ces trois mois.

Prendre en compte les aspects qualitatifs des résultats d'échantillonnage. Outre l'évaluation des résultats quantitatifs de l'échantillonnage d'attributs, l'auditeur interne doit envisager les aspects qualitatifs de tout écart mis au jour par rapport aux

Copyright © 2015 Eyrolles.

contrôles prescrits. En effet, si cet écart résulte d'une fraude, cela lui confère une importance particulière. Supposons, par exemple, que les résultats quantitatifs aillent dans le sens d'une conclusion selon laquelle un contrôle fonctionne de manière effective. Des preuves démontrant que les écarts constatés dans l'échantillon pourraient découler d'une fraude viendraient contredire les résultats quantitatifs et pousseraient l'auditeur interne à conclure que le contrôle n'est pas efficace (c'est-à-dire qu'on ne peut pas s'y fier pour ramener le risque à un niveau suffisamment faible). L'auditeur interne doit également déterminer quelles répercussions éventuelles la découverte de la fraude pourrait avoir sur les autres aspects de la mission.

Cas de documents manquants ou invalidés. Que doit faire un auditeur interne lorsque des documents pertinents pour tester des contrôles sont manquants ou ont été invalidés ? Étudions les cas suivants.

- **Cas 1.** Comme dans l'exemple donné en illustration ci-dessus, l'auditeur interne suit une piste d'audit ascendante (*vouching*) en partant d'un échantillon de bons de commande, en les rapprochant des demandes d'achat correspondantes. Mais il manque deux demandes d'achat qu'il ne peut pas retrouver. Ces deux demandes manquantes constituent à l'évidence des écarts par rapport au contrôle ; il n'existe aucun document probant d'autorisation pour l'établissement de ces deux bons de commande.
- **Cas 2.** L'auditeur interne a pris au hasard, en fonction de leur numéro, des bons de commande pour les tester et constate que l'un d'entre eux a été invalidé. Après une enquête de suivi sur le bon de commande invalidé, on détermine que tout est en ordre. Dans ce cas, la procédure appropriée consiste à sélectionner un autre bon de commande aux fins de vérification. Un nombre significatif de bons de commande invalidés pourrait signaler un autre problème nécessitant que l'audit continue d'y prêter attention.
- **Cas 3.** L'auditeur interne a pris au hasard, en fonction de leur numéro, des bons de commande pour les tester et constate qu'il en manque un. Après une enquête de suivi sur le bon de commande manquant, l'auditeur interne ne peut obtenir d'explication raisonnable à cette absence. Bien sûr, l'auditeur interne ne peut appliquer une procédure d'audit à un élément sélectionné qu'il ne peut trouver. Cette situation doit-elle être considérée comme un écart par rapport au contrôle prescrit ? L'*American Institute of Certified Public Accountants* (AICPA) est de cet avis : « Lorsque l'auditeur ne peut appliquer la procédure d'audit planifiée ou une autre procédure appropriée aux éléments sélectionnés, il doit prendre en compte les raisons de cette restriction et doit généralement considérer ces éléments comme des écarts par rapport à la politique ou procédure prescrite aux fins de l'évaluation de l'échantillon. »[2] Certains auditeurs internes sont

Copyright © 2015 Eyrolles.

en désaccord avec cette position parce qu'il est impossible de tester les contrôles prescrits à partir d'un document manquant. Selon eux, l'absence d'un document soulève un problème distinct qu'il faut prendre en compte séparément. Ils choisiraient donc de sélectionner un autre bon de commande pour effectuer le test. Que le bon de commande manquant soit considéré comme un écart par rapport au contrôle prescrit ou comme un problème différent à prendre en compte séparément, l'auditeur interne doit signaler dans ses papiers de travail le fait qu'il manque un bon de commande et décider si ce fait est suffisamment important pour faire l'objet d'une observation d'audit.

ÉCHANTILLONNAGE NON STATISTIQUE DANS LES TESTS DES CONTRÔLES

Sélectionner et évaluer un échantillon non statistique

L'échantillonnage statistique requiert deux éléments fondamentaux : l'échantillon doit être sélectionné de manière aléatoire, et les résultats d'échantillonnage doivent être évalués mathématiquement, sur la base de la théorie des probabilités. L'échantillonnage non statistique offre à l'auditeur interne une plus grande latitude pour sélectionner et évaluer l'échantillon.

Échantillonnage à l'aveuglette

Technique de sondage non aléatoire utilisée par les auditeurs internes pour sélectionner un échantillon qui doit être représentatif de la population.

L'auditeur interne doit néanmoins sélectionner un échantillon qu'il estime représentatif de la population, tenant compte des facteurs ayant une incidence sur la taille de l'échantillon. L'échantillonnage à l'aveuglette est une technique de sondage non aléatoire utilisée par les auditeurs internes pour sélectionner un échantillon qui doit être représentatif de la population. Dans ce contexte, « à l'aveuglette » n'induit aucune notion de négligence ou d'imprudence : cette expression signifie simplement que l'auditeur interne sélectionne l'échantillon sans choisir délibérément d'inclure ou d'exclure telle ou telle unité.

Un auditeur interne recourant à un échantillonnage non statistique doit également extrapoler les résultats de l'échantillon à l'ensemble de la population. De surcroît, il doit toujours rassembler des preuves suffisantes et adéquates pour étayer une conclusion valide. Il ne serait pas recevable, par exemple, de choisir un échantillonnage non statistique pour éviter d'avoir à justifier la taille de l'échantillon choisi. Au contraire, on pourrait même dire que les auditeurs internes qui optent pour l'échantillonnage non statistique auraient plutôt tendance à prendre des échantillons plus grands dans l'idée de compenser une méthode de sélection moins rigoureuse et l'incapacité de maîtriser quantitativement le risque de non-contrôle.

Copyright © 2015 Eyrolles.

L'incapacité de quantifier statistiquement le risque d'échantillonnage est ce qui le distingue le plus de l'échantillonnage statistique. La conclusion sur l'ensemble de la population que l'auditeur interne peut tirer à partir de l'échantillon repose exclusivement sur son jugement professionnel, et non sur la théorie des probabilités. Il est donc important que l'auditeur interne détermine s'il peut aboutir à des conclusions valides au moyen d'un échantillonnage non statistique ou s'il lui faut recourir à un échantillonnage statistique, potentiellement plus coûteux et chronophage, qui nécessite un échantillonnage aléatoire et dont les conclusions reposent sur la théorie des probabilités.

Méthodes d'échantillonnage non statistique classiquement utilisées

Une méthode classique d'échantillonnage non statistique consiste à sélectionner « à l'aveuglette » un échantillon relativement restreint, par exemple 25 éléments pour toutes les applications d'échantillonnage en partant de l'hypothèse que la population ne présente aucun écart par rapport au contrôle prescrit, et à conclure que le contrôle n'a pas une efficacité acceptable dès lors que l'on constate au moins un écart. Si cette approche est pratique, elle présente néanmoins un inconvénient de taille : elle ne prend pas en considération deux facteurs fondamentaux dont les auditeurs internes doivent tenir compte lorsqu'ils déterminent la taille appropriée de l'échantillon, à savoir le risque de sous-estimer le risque de non-contrôle et le taux d'écarts acceptable.

Pour nous en convaincre, regardons d'un peu plus près l'encadré 11-1. Où, dans cet encadré, trouve-t-on un échantillon de 25 unités ou moins ? Seulement à la première ligne du cadre inférieur du tableau, dans les deux dernières colonnes. On peut en déduire que si l'auditeur interne avait déterminé la taille de l'échantillon au moyen d'une méthode statistique, il aurait utilisé les paramètres suivants : risque de 10 % de sous-estimer le risque de non-contrôle, taux d'écarts acceptable de 9-10 % et taux d'écarts attendu de 0 %. Ces niveaux correspondent à une grande tolérance, qui n'est peut-être pas appropriée à toutes les applications d'échantillonnage employées en audit pour tester le fonctionnement effectif des contrôles.

L'encadré 11-3 montre une approche un peu plus prudente qu'utilisent certains auditeurs internes pour définir la taille d'un échantillon non statistique. On y présente la taille de l'échantillon qu'une organisation considère adéquate pour étayer la conclusion que les contrôles fonctionnent de manière effective si aucun écart n'est constaté dans les échantillons extraits de populations de tailles différentes. L'auditeur interne ajuste la taille de l'échantillon dans chaque fourchette, prenant en compte les facteurs ayant une

Copyright © 2015 Eyrolles.

incidence sur la taille de l'échantillon. Si, par exemple, le contrôle testé est jugé critique et que l'auditeur interne souhaite prendre un risque d'échantillonnage moindre, il choisira une taille d'échantillon dans la partie haute de la fourchette pertinente.

Un exemple d'échantillonnage non statistique

Partons de l'hypothèse suivante, soit un auditeur interne qui doit déterminer, sur la base d'un échantillonnage non statistique, si les rapprochements bancaires effectués ces 10 derniers mois ont été réalisés correctement. L'organisation a 10 comptes bancaires, qui ont tous fait l'objet d'un rapprochement bancaire sur les 10 derniers mois par la même personne, selon une méthode et un modèle imposés. L'auditeur interne anticipe qu'il ne trouvera aucun rapprochement qui n'ait pas été effectué correctement. S'il détecte un ou plusieurs rapprochements qui n'ont pas été effectués avec exactitude, il conclura que le fonctionnement effectif du contrôle du rapprochement bancaire présentait un niveau inacceptable sur les 10 derniers mois.

D'après l'encadré 11-3, combien de rapprochements bancaires devraient être testés ? Les rapprochements étant mensuels, l'auditeur interne pourrait raisonnablement décider d'en tester deux à cinq pour chaque compte bancaire. Dans ce cas, l'auditeur interne devrait tirer une conclusion distincte pour chaque compte. Une autre méthode raisonnable consisterait à considérer les 100 rapprochements bancaires comme une seule et même population, puisque les rapprochements sur chacun des 10 comptes font l'objet de contrôles identiques. Dans ce cas, la fourchette de tailles adéquates de l'échantillon se situera, selon l'encadré 11-3, entre la fourchette prescrite pour un contrôle hebdomadaire et celle pour

ENCADRÉ 11-3

EXEMPLE DE TAILLES D'ÉCHANTILLONS NON STATISTIQUES

Fréquence du contrôle	Taille adéquate de l'échantillon
Annuelle	1
Trimestrielle	2
Mensuelle	2 à 5
Hebdomadaire	5 à 15
Quotidienne	20 à 40
Plusieurs fois par jour	25 à 60

Source : D'après *Sarbanes-Oxley Act: Section 404 – Practical Guidance for Management*, PricewaterhouseCoopers, juillet 2004, p. 61.

Copyright © 2015 Eyrolles.

un contrôle quotidien. On peut alors logiquement décider de tester 20 à 25 des 100 rapprochements bancaires. Cette approche permet à l'auditeur interne d'aboutir à une conclusion globale. Cependant, il faut veiller à choisir un échantillon qui soit représentatif de la population.

La sélection « à l'aveuglette » des différents éléments de l'échantillon sur l'ensemble de la population (les 100 rapprochements bancaires) serait donc ici appropriée.

Supposons que l'auditeur interne sélectionne « à l'aveuglette » 25 rapprochements bancaires. Après avoir testé ces 25 unités, il établit que chaque rapprochement a été effectué correctement. Quelle conclusion peut-il en tirer ? Il ne peut formuler de conclusion statistique sur la population des 100 rapprochements bancaires, mais il peut dire que les résultats de l'échantillon viennent corroborer la conclusion selon laquelle les rapprochements bancaires ont été effectués correctement (c'est-à-dire que le contrôle des rapprochements bancaires revêtait une efficacité acceptable) sur les 10 derniers mois.

Supposons, à l'inverse, que l'auditeur interne constate que l'un des 25 rapprochements n'a pas été effectué correctement, contrairement à ce qu'il anticipait (à savoir qu'on ne trouverait aucun écart). Que peut-il alors en conclure ? Parce qu'un écart par rapport au contrôle prescrit a été constaté, l'auditeur interne doit conclure que le contrôle portant sur les rapprochements bancaires n'a pas été d'une efficacité acceptable ces 10 derniers mois. L'auditeur interne doit documenter cette observation et l'inclure dans le rapport de la mission.

ÉCHANTILLONNAGE STATISTIQUE DANS L'ÉCHANTILLONNAGE PAR UNITÉS MONÉTAIRES

En plus d'utiliser l'échantillonnage dans le cadre du test des contrôles, les auditeurs internes y recourent également lorsqu'ils effectuent des tests en vue d'obtenir des preuves directes de l'exactitude de valeurs monétaires, par exemple pour les soldes d'un compte, ou celui des stocks. Pour réaliser un Échantillonnage par unités monétaires (EUM), l'auditeur interne doit s'intéresser à deux aspects du risque d'échantillonnage.

- **Le risque d'acceptation à tort (erreur de type II ou risque bêta).** Il s'agit du risque que l'échantillon permette de conclure que la valeur testée (par exemple un solde de compte) ne comporte pas d'anomalie significative alors qu'elle en comporte.
- **Le risque de rejet à tort (erreur de type I ou risque alpha).** Il s'agit du risque que l'échantillon permette de conclure que la valeur testée (par exemple un solde de compte) comporte des anomalies significatives alors que ce n'est pas le cas.

Copyright © 2015 Eyrolles.

L'Échantillonnage par unités monétaires (EUM)

L'Échantillonnage par unités monétaires (EUM), également appelé échantillonnage proportionnel à la taille (EPT), est une variante de l'échantillonnage d'attributs utilisée pour obtenir des conclusions concernant des valeurs monétaires plutôt que des taux d'occurrence. L'EUM s'utilise donc essentiellement lorsque l'on recherche des montants surestimés, notamment lorsque le nombre de surestimations attendues dans la population est peu élevé, sans quoi cette méthode a peu de chances d'être rentable.

Sélection de l'échantillon. Comme dans le cas de l'échantillonnage d'attributs, il est également essentiel, dans un EUM, que l'échantillon soit sélectionné de manière aléatoire, c'est-à-dire que tous les éléments de la population aient une probabilité de sélection égale. Dans ce type d'échantillonnage, la population est l'ensemble des unités monétaires contenues dans le compte qui est soumis à examen. L'unité d'échantillonnage est l'unité monétaire. L'auditeur interne emploie une méthode d'échantillonnage systématique, c'est-à-dire qu'il sélectionne chaque $n^{ième}$ unité monétaire de la population à partir d'une origine aléatoire. Cependant, toutes les unités monétaires sélectionnées ne présentent pas un intérêt pour l'audit. Les éléments intéressants sont des « unités logiques » contenant des unités monétaires. Une unité logique serait, par exemple, un élément spécifique du stock enregistré dans le compte de stocks. Les unités logiques plus vastes sont plus à même d'être sélectionnées pour le test qu'une unité logique plus petite. En fait, la probabilité pour une unité logique d'être sélectionnée est proportionnelle à sa taille (d'où le nom d'échantillonnage proportionnel à la taille).

Échantillonnage par unités monétaires (EUM)

Variante de l'échantillonnage d'attributs utilisée pour obtenir des conclusions concernant des valeurs monétaires plutôt que des taux d'occurrence.

Les facteurs ayant une incidence sur la taille de l'échantillon d'un EUM sont les suivants :

- **la valeur comptable de la population.** La valeur comptable de la population (par exemple la valeur totale comptabilisée du stock en fin d'exercice) a une incidence directe sur la taille de l'échantillon ;
- **le risque d'acceptation à tort.** Le risque d'acceptation à tort a été défini ci-dessus comme le risque que l'échantillon permette de conclure que la valeur testée (par exemple le solde du stock comptabilisé) ne comporte pas d'anomalie significative alors qu'elle en comporte. Il existe une relation inverse entre ce risque, qui est une composante du risque d'échantillonnage, et la taille de l'échantillon ;
- **l'anomalie tolérable.** L'anomalie tolérable est l'anomalie maximale qui peut exister dans la valeur comptabilisée avant que l'auditeur interne n'estime qu'il s'agisse d'une anomalie significative. Il existe une relation inverse entre l'anomalie tolérable et la taille de l'échantillon ;

Copyright © 2015 Eyrolles.

- **l'anomalie estimée.** L'anomalie estimée ou attendue est le montant de l'anomalie que l'auditeur interne s'attend à constater dans la valeur comptabilisée. Elle a une incidence directe sur la taille de l'échantillon.

Évaluation des résultats d'échantillonnage. Après avoir sélectionné et audité l'échantillon, l'auditeur interne extrapole, à partir de l'EUM, les résultats pour l'ensemble de la population, formule une conclusion statistique et détermine si les preuves quantitatives et qualitatives tirées de l'échantillon indiquent que la valeur monétaire comptabilisée semble juste ou qu'elle présente une anomalie significative. La description précise du déroulement de ces étapes sortirait du cadre du présent manuel.

Les méthodes classiques d'échantillonnage de variables

Échantillonnage de variables classique

Méthode d'échantillonnage statistique qui s'appuie sur la distribution de Gauss (aussi appelée distribution normale).

L'échantillonnage de variables classique est une méthode d'échantillonnage statistique qui s'appuie sur la distribution de Gauss (aussi appelée distribution normale). Elle est utilisée pour obtenir des conclusions concernant des valeurs monétaires. On considère généralement que cet échantillonnage est plus difficile à appliquer que l'EUM, surtout parce qu'il suppose des calculs bien plus complexes pour la détermination de la taille des échantillons et l'évaluation des résultats.

Sélectionner l'échantillon. Là encore, il est très important pour l'échantillonnage de variables classique que l'échantillon réponde à une sélection aléatoire. Les deux approches retenues pour sélectionner un échantillon aléatoire de variables sont l'échantillonnage aléatoire simple et l'échantillonnage systématique avec une ou plusieurs origines choisies au hasard.

Les facteurs suivants ont une incidence sur la taille de l'échantillon :

- **la taille de la population.** La taille de la population est le nombre d'éléments que compte la population (par exemple, le nombre d'unités de stock enregistrées en comptabilité). Elle a une incidence directe sur la taille de l'échantillon ;
- **l'écart-type estimé de la population.** L'écart-type estimé de la population, qui est une mesure de la variabilité de la population, a une incidence directe sur la taille de l'échantillon ;
- **le risque d'acceptation à tort.** Le risque d'acceptation à tort a été défini ci-dessus comme le risque que l'échantillon permette de conclure que la valeur testée (par exemple le solde du stock comptabilisé) ne comporte pas d'anomalie significative alors qu'elle en comporte. Il existe une relation inverse entre ce risque, qui est une composante du risque d'échantillonnage, et la taille de l'échantillon ;

Copyright © 2015 Eyrolles.

Facteurs ayant une incidence sur la taille de l'échantillon pour un EUM

– La valeur comptable de la population.
– Le risque d'acceptation à tort.
– L'anomalie tolérable.
– L'anomalie estimée.

Facteurs ayant une incidence sur la taille de l'échantillon de variables classique

– La taille de la population.
– L'écart-type estimé de la population.
– Le risque d'acceptation à tort.
– Le risque de rejet à tort (erreur de type I ou risque alpha).
– L'anomalie tolérable.

- **le risque de rejet à tort (erreur de type I ou risque alpha).** Le risque de rejet à tort est le risque que l'échantillon permette de conclure que la valeur théorique (par exemple le solde de compte) comporte des anomalies significatives alors que ce n'est pas le cas. Il existe une relation inverse entre ce risque, qui est la seconde composante du risque d'échantillonnage, et la taille de l'échantillon ;
- **l'anomalie tolérable.** L'anomalie tolérable est l'anomalie maximale qui peut exister dans la valeur comptabilisée avant que l'auditeur interne n'estime qu'il s'agit d'une anomalie significative. Il existe une relation inverse entre l'anomalie tolérable et la taille de l'échantillon.

Évaluation des résultats d'échantillonnage. Comme pour l'EUM, après avoir sélectionné et audité l'échantillon, l'auditeur interne extrapole, à partir de l'échantillonnage de variables classique, les résultats pour l'ensemble de la population, formule une conclusion statistique et détermine si les preuves quantitatives et qualitatives tirées de l'échantillon indiquent que la valeur monétaire comptabilisée semble juste ou si elle présente une anomalie significative. Le processus d'évaluation de l'échantillon est plus complexe pour un échantillonnage de variables classique que pour un EUM. La description précise du déroulement de ces étapes sortirait du cadre du présent manuel.

Échantillonnage par unités monétaires/ échantillonnage de variables classique

L'EUM comme l'échantillonnage de variables classique présentent des avantages et des inconvénients significatifs que les auditeurs internes doivent prendre en considération lorsqu'ils choisissent l'approche la mieux adaptée à un échantillonnage donné. L'encadré 11-4 présente les principaux avantages et inconvénients de chacune des deux approches.

RÉSUMÉ

Dans ce chapitre, nous nous sommes intéressés à l'échantillonnage en audit en tant qu'outil permettant l'application de certaines procédures d'audit dans le but d'atteindre les objectifs de la mission. Nous avons tout d'abord examiné les échantillonnages statistique et non statistique, puis décrit le risque d'échantillonnage et le risque discrétionnaire. Nous avons ensuite étudié en détail l'échantillonnage statistique et l'échantillonnage non statistique tels qu'employés par les auditeurs internes dans les tests des contrôles. Le chapitre s'est terminé sur un aperçu de deux approches d'échantillonnage statistique que les auditeurs internes utilisent pour

Copyright © 2015 Eyrolles.

obtenir des preuves directes quant à l'exactitude des valeurs monétaires. L'encadré 11-5 présente 10 éléments essentiels à retenir sur l'échantillonnage en audit.

ENCADRÉ 11-4

ÉCHANTILLONNAGE PAR UNITÉS MONÉTAIRES/ ÉCHANTILLONNAGE DE VARIABLES CLASSIQUE

Échantillonnage par unités monétaires (EUM)

Principaux avantages

- La plus grande simplicité des calculs rend l'EUM plus facile à utiliser.
- Le calcul de la taille de l'échantillon ne suppose aucune mesure de la variance estimée de la population.
- L'EUM aboutit automatiquement à un échantillon stratifié, parce que la probabilité qu'un élément soit sélectionné est proportionnelle à sa taille.
- La sélection de l'échantillon pour l'EUM identifie automatiquement tout élément de la population individuellement significatif, c'est-à-dire tout élément dépassant une valeur monétaire fixée à l'avance.
- L'EUM est généralement plus efficient (il requiert un échantillon de taille plus restreinte) lorsque la population contient zéro ou peu d'anomalies.

Principaux inconvénients

- Si l'on anticipe des sous-estimations ou des valeurs inférieures à zéro, ce point doit être spécifiquement pris en compte lors de la définition de l'échantillonnage.
- L'identification de sous-estimations dans l'échantillon appelle une prise en compte particulière pour l'évaluation.
- L'EUM donne des résultats excessivement prudents lorsque des erreurs sont détectées. Cette caractéristique accroît le risque de rejet à tort.
- La taille appropriée pour l'échantillon augmente rapidement lorsque le nombre d'anomalies attendues augmente. Lorsque l'on anticipe plus de quelques anomalies, l'EUM est peut-être moins efficient.

Échantillonnage de variables classique

Principaux avantages

- Les échantillons sont généralement plus faciles à agrandir si l'auditeur interne le juge nécessaire.
- Les soldes nuls et négatifs n'ont pas à être pris en compte de manière spécifique lors de la définition de l'échantillon.
- L'auditeur interne peut atteindre son objectif au moyen d'un échantillon de taille plus restreinte si les anomalies (c'est-à-dire les différences entre les valeurs d'audit et les valeurs enregistrées) sont moins nombreuses.

Principaux inconvénients

- L'échantillonnage de variables classique est plus complexe. L'auditeur interne peut avoir besoin de recourir à un programme informatique pour définir et évaluer un échantillon de manière rentable.
- Le calcul de la taille adéquate de l'échantillon impose à l'auditeur interne d'estimer d'abord l'écart-type de la population.

Copyright © 2015 Eyrolles.

ENCADRÉ 11-5

10 ÉLÉMENTS ESSENTIELS À RETENIR SUR L'ÉCHANTILLONNAGE EN AUDIT

- L'échantillonnage en audit consiste à appliquer une procédure d'audit à moins de 100 % des éléments d'une population concernée par une mission, *afin d'en tirer une conclusion pour l'ensemble de la population*.
- Les échantillonnages statistique et non statistique font tous deux appel au jugement professionnel, tant dans la conception du plan d'échantillonnage que dans l'exécution de ce plan et l'analyse des résultats obtenus.
- L'échantillonnage statistique a un grand avantage sur l'échantillonnage non statistique : il permet à l'auditeur interne de quantifier, mesurer et maîtriser le risque d'échantillonnage.
- Également appelé risque aléatoire, le risque d'échantillonnage est le risque que les conclusions que l'auditeur interne tire du test d'un échantillon diffèrent de celles qu'il aurait tirées si la procédure d'audit avait été appliquée à la totalité de la population.
- Il existe une relation inverse entre le risque d'échantillonnage et la taille de l'échantillon.
- L'échantillonnage d'attributs (ou échantillonnage sur attribut ou échantillonnage par attribut) est une méthode d'échantillonnage statistique qui permet d'aboutir à une conclusion grâce au calcul d'un taux d'occurrence dans une population.
- Dans l'échantillonnage d'attributs, l'auditeur interne doit exercer son jugement professionnel lorsqu'il précise les valeurs appropriées pour les trois facteurs ayant une incidence sur la taille de l'échantillon : le niveau acceptable de risque de sous-estimer le risque de non-contrôle, le taux d'écarts acceptable et le taux d'écarts attendu de la population.
- Il existe une relation inverse entre le risque acceptable de sous-estimer le risque de non-contrôle et la taille de l'échantillon. De même, il existe une relation inverse entre le taux d'écarts acceptable et la taille de l'échantillon. En revanche, le taux d'écarts attendu de la population a une incidence directe sur la taille de l'échantillon.
- Avec un échantillonnage statistique, il est essentiel d'employer une technique de sélection aléatoire (en d'autres termes, tous les éléments de la population doivent avoir une probabilité de sélection égale).
- Évaluer les résultats d'un échantillonnage d'attributs suppose de formuler une conclusion statistique, prendre une décision d'audit sur la base de résultats quantitatifs et prendre en compte les aspects qualitatifs des résultats d'échantillonnage.

Copyright © 2015 Eyrolles.

Questions de révision

1. Comment l'« échantillonnage en audit » est-il défini dans ce chapitre ?

2. Quelles sont les deux grandes catégories d'échantillonnage en audit ?

3. Comment le « risque d'échantillonnage » est-il défini dans ce chapitre ? Quels sont les deux aspects du risque d'échantillonnage qu'un auditeur interne doit prendre en compte lorsqu'il teste des contrôles ?

4. En quoi le risque discrétionnaire diffère-t-il du risque d'échantillonnage ?

5. Qu'est-ce que l'échantillonnage d'attributs ? Quelles sont les trois variantes de ce type d'échantillonnage décrites dans ce chapitre ?

6. Quelles sont les neuf étapes de l'échantillonnage d'attributs ?

7. Quels sont les facteurs qui influencent la taille de l'échantillon pour l'échantillonnage d'attributs ?

8. Quelles sont les étapes de l'évaluation des résultats d'un échantillonnage d'attributs ?

9. Que doit faire un auditeur interne lorsque des documents pertinents pour tester des contrôles sont manquants ?

10. Comment l'« échantillonnage à l'aveuglette » est-il défini dans ce chapitre ?

11. Quel est le principal avantage de l'échantillonnage statistique par rapport à l'échantillonnage non statistique ?

12. Pourquoi les auditeurs internes choisissent-ils parfois de recourir à l'échantillonnage non statistique plutôt qu'à l'échantillonnage statistique ?

13. En quoi l'objectif de l'échantillonnage statistique dans les tests d'unités monétaires diffère-t-il de celui de l'échantillonnage statistique dans les tests des contrôles ?

14. Quels sont les facteurs ayant une incidence sur la taille de l'échantillon pour les Échantillonnages par unités monétaires (EUM) ?

15. Quels sont les principaux avantages des EUM par rapport aux échantillonnages de variables classiques ? Quels sont ses principaux inconvénients ?

Copyright © 2015 Eyrolles.

Questions à choix multiples

Sélectionnez la meilleure réponse pour chacune des questions suivantes.

1. Quelle est la raison principale pour laquelle un auditeur interne utilise un échantillonnage statistique plutôt que non statistique ?
   a. Pouvoir quantifier le risque de prendre une mauvaise décision à partir des preuves recueillies au moyen de l'échantillonnage, et donc en tenir compte.
   b. Travailler sur un échantillon plus restreint que ce qui serait nécessaire s'il utilisait un échantillonnage non statistique.
   c. Réduire les problèmes que pose, en cas d'échantillonnage non statistique, le jugement professionnel de l'auditeur concernant le caractère adéquat des preuves réunies.
   d. Obtenir un échantillon plus représentatif de la population que ce que l'on obtiendrait avec des techniques d'échantillonnage non statistiques.

2. Parmi les propositions suivantes, laquelle est associée au risque d'échantillonnage, par opposition au risque discrétionnaire ?
   a. Définir un échantillon trop petit.
   b. Effectuer une procédure d'audit inappropriée.
   c. Ne pas détecter un écart par rapport au contrôle prescrit.
   d. Oublier d'effectuer une procédure d'audit prescrite.

3. À quelle fin un auditeur interne utiliserait-il plus vraisemblablement un échantillonnage d'attributs ?
   a. Pour déterminer si le solde de clôture est surestimé.
   b. Pour sélectionner les nouvelles immobilisations à inspecter.
   c. Pour choisir les éléments du stock à dénombrer par échantillonnage.
   d. Pour vérifier si les fiches de présence des collaborateurs bénéficient de l'approbation adéquate.

4. Si, tous les autres facteurs spécifiés dans le plan d'échantillonnage d'attributs demeurant constants, on portait le taux d'écarts attendu de la population de 1 % à 2 % et qu'on ramenait le taux d'écarts acceptable de 7 % à 6 %, quelle serait l'incidence sur la taille de l'échantillon ?
   a. Elle augmenterait.
   b. Elle diminuerait.
   c. Elle resterait identique.
   d. Elle varierait de 2 %.

Copyright © 2015 Eyrolles.

Questions à choix multiples

5. Un auditeur interne sélectionne un échantillon de factures clients et les compare avec les documents d'expédition. Cette procédure permet de vérifier l'une des affirmations suivantes. Laquelle ?
   a. Toutes les expéditions adressées à des clients sont bien comptabilisées en tant que créances.
   b. Toutes les ventes facturées concernent des biens expédiés à des clients.
   c. Tous les débits sur le grand livre auxiliaire des comptes clients correspondent à des biens expédiés à des clients.
   d. Toutes les expéditions adressées à des clients ont bien été facturées.

6. Un auditeur interne teste des transactions de décaissement. D'après la politique de contrôle interne, toutes les demandes de vérification doivent être accompagnées de pièces justificatives approuvées (c'est-à-dire d'un ensemble de documents prouvant qu'un bien ou un service a été reçu et facturé par le fournisseur). L'approbation des pièces justificatives repose sur une triple correspondance entre le bon de commande, le bordereau de réception et la facture du vendeur. Afin de déterminer si toutes les vérifications sont assorties des pièces requises, l'auditeur interne doit commencer ses procédures de test en sélectionnant des éléments de la population de :
   a. Copies des chèques.
   b. Bons de commande.
   c. Bordereaux de réception.
   d. Pièces justificatives approuvées.

7. Le plafond d'écarts toléré est de 7 % et le risque de sous-estimer le risque de non-contrôle est de 5 %. Comment l'auditeur interne doit-il interpréter le résultat de l'échantillonnage d'attributs ?
   a. Il y a 7 % de chances que le taux d'écarts dans la population soit inférieur ou égal à 5 %.
   b. Il y a 5 % de chances que le taux d'écarts dans la population soit inférieur à 7 %.
   c. Il y a 5 % de chances que le taux d'écarts dans la population dépasse 7 %.
   d. Il y a 95 % de chances que le taux d'écarts dans la population soit de 7 %.

8. En plus d'évaluer le nombre d'écarts, un auditeur interne doit tenir compte des aspects qualitatifs des écarts constatés dans un échantillon. Laquelle des situations suivantes doit inquiéter le plus l'auditeur interne ?
   a. Il a dénombré moins d'écarts qu'attendu dans l'échantillon.
   b. Les écarts constatés sont de même nature que ceux observés lors du dernier audit du service.
   c. Les écarts constatés semblent avoir pour origine une mauvaise compréhension des instructions par un collaborateur.
   d. Les écarts constatés peuvent avoir été causés intentionnellement.

Copyright © 2015 Eyrolles.

9. Si, tous les autres facteurs spécifiés dans le plan d'EUM demeurant constants, on ramenait l'anomalie tolérable définie de 200 000 à 100 000 et le risque d'acceptation à tort fixé de 10 % à 5 %, quelle serait l'incidence sur la taille de l'échantillon ?
   a. Elle augmenterait.
   b. Elle diminuerait.
   c. Elle resterait identique.
   d. Elle varierait de 5 %.

10. Un auditeur interne veut tester le solde des créances d'exploitation d'un client sur la base d'un échantillon afin d'identifier des éléments surévalués. Parmi les propositions suivantes, laquelle serait la raison la moins valide de décider de recourir à un EUM plutôt qu'à un échantillonnage de variables classique ?
   a. L'EUM est généralement perçu comme plus facile à utiliser que l'échantillonnage de variables classique.
   b. L'auditeur interne s'attend à ne trouver aucune anomalie et, dans cette situation, l'EUM nécessite généralement un échantillon de taille plus restreinte que l'échantillonnage de variables classique.
   c. L'EUM stratifie automatiquement la population.
   d. Le recours à l'EUM élimine la nécessité d'un jugement professionnel pour déterminer la taille adéquate de l'échantillon et évaluer les résultats.

Copyright © 2015 Eyrolles.

Thèmes de discussion

1. Le responsable de l'audit interne de l'organisation HVR vous demande d'expliquer ce qui distingue fondamentalement l'échantillonnage statistique de l'échantillonnage non statistique de manière à l'aider à prendre une décision éclairée sur la nature de la formation à l'échantillonnage qui sera la plus bénéfique aux membres du service d'audit interne. Expliquez-lui en quoi les deux approches diffèrent sur les aspects suivants.
   a. Détermination de la taille de l'échantillon.
   b. Sélection de l'échantillon.
   c. Évaluation des résultats d'échantillonnage.

2. Vous étudiez l'échantillonnage en audit avec un ami. Celui-ci a du mal à comprendre les différents aspects du risque associé à l'échantillonnage d'attributs et a établi la liste de questions suivantes dont il souhaite discuter avec vous. Répondez à chacune de ses questions.
   a. Qu'est-ce que :
   - le risque d'audit ?
   - le risque inhérent ?
   - le risque de non-contrôle ?
   - le risque maîtrisable ?
   - le risque résiduel ?

   b. Qu'est-ce que le risque d'échantillonnage ? Comment le maîtrise-t-on ?
   c. Quels sont les deux aspects du risque d'échantillonnage qui intéressent l'auditeur interne lorsqu'il teste des contrôles ? Décrivez brièvement chacun de ces aspects.
   d. Qu'est-ce que le risque discrétionnaire ? Comment le maîtrise-t-on ?

3. Chaque mois, l'organisation AVF traite en moyenne 400 pièces justificatives (*vouchers*) correspondant à des dettes d'exploitation. Chaque lot de pièces justificatives contient la copie du chèque émis et les pièces connexes, telles que factures fournisseurs, bordereaux de réception et bons de commande. L'auditeur interne prévoit d'examiner un échantillon de pièces justificatives répertoriées dans le journal des pièces justificatives, en vue d'évaluer, au moyen d'un échantillonnage d'attributs, l'efficacité de divers contrôles. Les attributs qui revêtent un intérêt particulier sont notamment :
   - la concordance entre le montant figurant sur la pièce justificative et le montant de la facture ;
   - l'annulation de la pièce justificative (*voucher*) après le règlement.

   Par expérience, l'auditeur anticipe un taux d'écarts de 2 % pour le premier attribut et de 1 % pour le second. Il choisit un taux d'écarts acceptable de 7 % pour le premier et de 6 % pour le second. Il fixe à 5 % le risque de sous-estimer le risque de non-contrôle.

Copyright © 2015 Eyrolles.

Supposons que les tests ont permis à l'auditeur de mettre au jour deux cas dans lesquels les montants des pièces justificatives ne correspondaient pas au montant de la facture et deux cas dans lesquels elles n'ont pas été supprimées après le règlement.

a. Complétez le tableau suivant (Note : Pour la taille de l'échantillon utilisé, arrondissez à la dizaine supérieure) :

	Attribut 1	Attribut 2
Risque de sous-estimer le risque de non-contrôle		
Taux d'écarts acceptable		
Taux d'écarts attendu de la population		
Taille de l'échantillon, d'après la table		
Taille de l'échantillon utilisé		
Nombre d'écarts détectés		
Taux d'écarts de l'échantillon		
Plafond d'écarts tolérés		

b. Évaluez les résultats de l'échantillon pour les deux attributs. Votre réponse doit comporter :

- Une conclusion statistique pour chaque attribut.
- La décision d'audit que vous prendriez à partir des résultats quantitatifs de l'échantillon pour chacun des attributs.[3]

4. Les auditeurs internes utilisent l'EUM pour obtenir des conclusions concernant des valeurs monétaires.

a. Indiquez dans quelle situation l'application de l'EUM est la plus appropriée.

b. Décrivez la méthode de sélection de l'échantillon d'un EUM.

c. Identifiez les facteurs ayant une incidence sur la taille de l'échantillon d'un EUM. Précisez l'incidence de chaque facteur sur la taille de l'échantillon.

d. Expliquez quels sont les avantages et les inconvénients que l'auditeur interne doit prendre en compte lorsqu'il choisit la meilleure méthode à appliquer entre l'EUM et l'échantillonnage de variables classique.

Copyright © 2015 Eyrolles.

ÉTUDE DE CAS

[4] Ira Icandoit fait partie de l'équipe d'audit interne d'une petite entreprise manufacturière située dans l'Ouest. Ira a récemment achevé un cursus de formation continue sur l'échantillonnage statistique, et il est ravi de ses nouvelles connaissances. Il décide de les mettre en pratique au cours d'une mission d'audit qui vient de lui être assignée. Il utilise un échantillonnage d'attributs pour tester les contrôles appliqués aux transactions d'achat de l'organisation.

Ira estime qu'un taux d'écarts acceptable de 10 % et un risque de 5 % de sous-estimer le risque de non-contrôle sont des niveaux adéquats pour les tests qu'il envisage. Il n'a aucune idée du nombre d'écarts qui pourraient effectivement exister dans la population ; par prudence, il définit donc un taux d'écarts attendu de 2 %. Il sélectionne un échantillon de 100 éléments.

Jugeant que les éléments les plus gros méritent davantage d'attention que les petits, Ira en sélectionne 75 d'une valeur supérieure ou égale à 2 500 et 25 d'une valeur inférieure. Il pense qu'il serait plus approprié de choisir des transactions effectuées vers la fin de l'exercice ; aussi sélectionne-t-il de manière aléatoire au sein des deux derniers mois les éléments à tester.

Ira est soulagé de ne constater que six écarts par rapport aux contrôles prescrits. L'un d'entre eux est une facture manquante d'un fournisseur ; il appelle donc ce dernier pour s'assurer que la transaction était valide. La conversation téléphonique le convainc que la transaction est effectivement valide. Trois des écarts concernent l'absence de signature de la part du manager habilité. Celui-ci explique qu'il n'a pas signé ces factures parce qu'il n'était pas au bureau à la date à laquelle elles ont été établies. Il les examine et affirme à Ira qu'elles ne posent pas de problème particulier. Les deux autres écarts portent sur des erreurs de montants. L'une était une erreur dans le calcul du montant de la facture, et l'autre une erreur de classification entre les postes de dépenses, qui n'a pas affecté le résultat net. Ira considère que ces deux erreurs de montant sont les deux seuls véritables écarts par rapport au contrôle prescrit. Il estime que le plafond d'écarts tolérés est de 7 %, avec un risque de 5 % de sous-estimer le risque de non-contrôle.

Sur la base de ces résultats, Ira conclut que les transactions d'achat pour l'exercice sont peu susceptibles de contenir davantage d'écarts que le taux acceptable. Par conséquent, il conclut que les contrôles portant sur ces transactions ont été efficaces et que le management peut s'y fier.

Identifiez et expliquez toute déficience que vous remarquez dans l'échantillonnage d'attributs effectué par Ira.

Copyright © 2015 Eyrolles.



Copyright © 2015 Eyrolles.



Copyright © 2015 Eyrolles.

CHAPITRE 12
INTRODUCTION AU PROCESSUS D'AUDIT

Objectifs pédagogiques

- Comprendre les différentes missions réalisées par les auditeurs internes.
- Comprendre les principales activités liées à la planification et à l'accomplissement d'une mission d'assurance et rendre compte des résultats de la mission.
- Expliquer en quoi le déroulement de la mission de conseil diffère du déroulement de la mission d'assurance.

Les onze premiers chapitres du présent manuel, qui forment ensemble la section « Concepts fondamentaux d'audit interne », sont consacrés aux concepts fondamentaux que les auditeurs internes doivent connaître et comprendre. Une bonne maîtrise de ces concepts est nécessaire, mais pas suffisante pour appréhender l'audit interne. L'auditeur doit également comprendre le processus de l'audit interne, à savoir la manière dont les missions d'assurance et de conseil menées par l'audit interne sont planifiées et exécutées, ainsi que la manière dont leurs résultats sont communiqués.

Le présent chapitre est le premier de quatre chapitres relatifs à la conduite des missions d'audit interne. Nous commençons ce chapitre par une brève description des catégories de missions que les auditeurs internes doivent exécuter. Nous décrivons ensuite le déroulement de la mission d'assurance de l'audit interne. Nous concluons ce chapitre en analysant en quoi les missions de conseil diffèrent des missions d'assurance, ainsi que l'effet de ces différences sur le déroulement de la mission de conseil. Au chapitre 13, *Le déroulement de la mission d'assurance*, nous expliquons en détail comment mener le déroulement de la mission d'assurance, tandis qu'au chapitre 14, *La communication des résultats d'une mission d'assurance et les procédures de suivi,* nous couvrons la communication des résultats des missions d'assurance. Enfin, au chapitre 15, *La mission de conseil*, nous portons notre attention sur le déroulement de la mission de conseil.

Il importe de souligner que, tout au long de ce chapitre et de ceux qui suivent, nous évoquons très souvent la « fonction d'audit interne », l'« audit interne », l'« auditeur interne » et l'« équipe d'audit interne ». Même s'il existe de subtiles différences entre ces termes, suivant les circonstances décrites ou le contexte dans lequel ils sont utilisés, nous désignons ainsi, de manière générale, les activités mises en œuvre par l'audit interne sous la supervision du responsable de

ENCADRÉ 12-1

DISPOSITIONS DU CRIPP PERTINENTES RELATIVES AU CHAPITRE 12

Norme 1220 – Conscience professionnelle
Norme 2000 – Gestion de l'audit interne
Norme 2200 – Planification de la mission
Norme 2201 – Considérations relatives à la planification
Norme 2210 – Objectifs de la mission
Norme 2220 – Champ de la mission
Norme 2230 – Ressources affectées à la mission
Norme 2240 – Programme de travail de la mission
Norme 2300 – Accomplissement de la mission
Norme 2310 – Identification des informations
Norme 2320 – Analyse et évaluation
Norme 2330 – Documentation des informations
Norme 2340 – Supervision de la mission
Norme 2400 – Communication des résultats
Norme 2410 – Contenu de la communication
Norme 2420 – Qualité de la communication
Norme 2421 – Erreurs et omissions
Norme 2431 – Indication de non-conformité
Norme 2440 – Diffusion des résultats
Norme 2500 – Surveillance des actions de progrès
Norme 2600 – Communication relative à l'acceptation des risques

Modalité Pratique d'Application 2200-1 :	Planification de la mission
Modalité Pratique d'Application 2210-1 :	Objectifs de la mission
Modalité Pratique d'Application 2210.A1-1 :	Évaluation des risques dans la planification de la mission
Modalité Pratique d'Application 2230-1 :	Ressources affectées à la mission
Modalité Pratique d'Application 2240-1 :	Programme de travail de la mission
Modalité Pratique d'Application 2320-2 :	Analyse causale
Modalité Pratique d'Application 2330-1 :	Documentation des informations
Modalité Pratique d'Application 2330.A1-1 :	Contrôle des dossiers d'audit
Modalité Pratique d'Application 2330.A2-1 :	Conservation des dossiers
Modalité Pratique d'Application 2340-1 :	Supervision de la mission
Modalité Pratique d'Application 2410-1 :	Contenu de la communication
Modalité Pratique d'Application 2420-1 :	Qualité de la communication
Modalité Pratique d'Application 2440-1 :	Diffusion des résultats de la mission
Modalité Pratique d'Application 2500-1 :	Surveillance des actions de progrès
Modalité Pratique d'Application 2500.A1-1 :	Processus de suivi de la mission

l'audit interne et sous la surveillance du comité d'audit. Comme nous l'expliquons en détail dans le chapitre 9, *La gestion de l'audit interne*, la Norme 2000, Gestion de l'audit interne, indique que « le responsable de l'audit interne doit gérer efficacement cette activité de façon à garantir qu'elle apporte une valeur ajoutée à l'organisation ».

Copyright © 2015 Eyrolles.

Commentaire du traducteur

Le lecteur pourra également s'appuyer sur d'autres normes et lignes directrices du CRIPP, notamment en ce qui concerne l'objectivité individuelle, la compétence et les travaux d'autres prestataires de services d'assurance.

CATÉGORIES DE MISSIONS D'AUDIT INTERNE

Comme le précise le chapitre 1, *Introduction à l'audit interne*, les auditeurs internes mènent deux types d'activités, l'assurance et le conseil. Ces deux types d'activités sont définis dans le glossaire des *Normes internationales pour la pratique professionnelle de l'audit interne* (les *Normes*), au sein du Cadre de référence international des pratiques professionnelles de l'audit interne (CRIPP), de la manière suivante.

- **Activités d'assurance –** Il s'agit d'un examen objectif d'éléments probants, effectué en vue de fournir à l'organisation une évaluation indépendante des processus de gouvernement d'entreprise, de management des risques et de contrôle. Par exemple, des audits financiers, de performance, de conformité, de sécurité des systèmes et de *due diligence*.
- **Activités de conseil –** Il s'agit des conseils et services y afférents rendus au client donneur d'ordre, dont la nature et le champ sont convenus au préalable avec lui. Ces activités ont pour objectifs de créer de la valeur ajoutée et d'améliorer les processus de gouvernement d'entreprise, de management des risques et de contrôle d'une organisation sans que l'auditeur interne n'assume aucune responsabilité de management. Quelques exemples : avis, conseil, assistance et formation.

L'encadré 12-2 présente des exemples de missions d'assurance et de conseil réalisées par les auditeurs internes. Comme l'indique cet encadré, les activités d'assurance et de conseil des auditeurs internes peuvent être conçues pour couvrir directement les performances opérationnelles, de reporting et/ou de conformité. Elles peuvent également viser les contrôles destinés à donner l'assurance raisonnable que les objectifs de performance sont atteints. Les missions centrées sur l'adéquation de la conception et le fonctionnement effectif des *contrôles* relatifs aux opérations, au reporting et à la conformité sont beaucoup plus fréquentes que les missions centrées sur les *performances* réalisées. Comme indiqué dans le chapitre 15, *La mission de conseil*, les missions d'audit peuvent être des missions d'assurance ou des missions de conseil et, dans certaines circonstances, peuvent être regroupées en une seule mission. C'est pourquoi les exemples présentés dans l'encadré 12-2, qui illustrent chaque type de mission, peuvent tout aussi bien intégrer des éléments de l'autre type de mission.

Missions centrées sur les performances

Missions couvrant directement les performances opérationnelles, de reporting et/ou de conformité.

Missions centrées sur les contrôles

Missions visant l'adéquation de la conception et le fonctionnement effectif des contrôles mis en place pour donner l'assurance raisonnable que les objectifs de performance sont atteints.

Copyright © 2015 Eyrolles.

ENCADRÉ 12-2

EXEMPLES DE MISSIONS D'AUDIT INTERNE D'ASSURANCE ET DE CONSEIL

Exemples de missions d'assurance

- Évaluer l'adéquation de la conception et le fonctionnement effectif des contrôles à l'échelle de l'entité. Les contrôles à l'échelle de l'entité peuvent être, par exemple :
  - des contrôles sur le risque de contournement par le management ;
  - des contrôles sur le processus d'évaluation des risques de l'organisation à l'échelle de l'entité ;
  - des contrôles visant à surveiller les résultats des opérations ;
  - des contrôles sur le processus du reporting financier en fin d'exercice.
- Évaluer l'adéquation de la conception et le fonctionnement effectif des contrôles des processus opérationnels. Les contrôles des processus peuvent être, par exemple :
  - des contrôles sur l'efficacité et l'efficience des opérations ;
  - des contrôles sur la fiabilité du reporting financier et/ou de gestion ;
  - des contrôles sur la conformité aux lois et règlements applicables.
- Évaluer l'adéquation de la conception et le fonctionnement effectif des contrôles des SI. Les contrôles des SI peuvent être, par exemple :
  - des contrôles généraux à l'échelle de l'entité tels que les contrôles d'accès au système et les contrôles de la gestion du changement ;
  - des contrôles applicatifs intégrés dans les programmes applicatifs spécifiques.
- Évaluer directement les performances des processus opérationnels. Les performances des processus peuvent être, par exemple :
  - l'efficacité et l'efficience opérationnelles exprimées par des indicateurs tels que les indices de satisfaction des clients, le temps de cycle, la rotation du personnel, etc. ;
  - la fiabilité du reporting financier, telle qu'exprimée par le nombre et le montant des écritures de correction en fin d'exercice ;
  - la conformité aux lois et règlements applicables, telle qu'exprimée par des indicateurs comme le nombre d'accidents déclarés ou les rejets à l'environnement.

Exemples de missions de conseil

- Exécuter des activités de conseil, par exemple :
  - des conseils à la direction générale concernant les conséquences pour le risque et les contrôles de la mise en œuvre d'une solution de SI avancée ;
  - des conseils aux propriétaires de processus sur la manière de rationaliser ces derniers afin de dégager des gains d'efficience ;
  - des conseils aux managers à tous les niveaux de l'organisation sur la manière de documenter et de regrouper leurs évaluations des risques et des contrôles.
- Faciliter les auto-évaluations comme :
  - l'évaluation par la direction générale des risques opérationnels qui menacent l'organisation dans son ensemble ;
  - l'évaluation, par les propriétaires de processus, des risques qui menacent leurs activités.
- Mener des formations en interne, par exemple :
  - renseigner la direction générale et le comité d'audit sur les nouvelles lignes directrices qui font autorité sur la gouvernance, la gestion des risques et le contrôle ;
  - informer les propriétaires de processus et les collaborateurs sur les concepts fondamentaux que sont la gouvernance, la gestion des risques et le contrôle.

Copyright © 2015 Eyrolles.

PRÉSENTATION DU DÉROULEMENT DE LA MISSION D'ASSURANCE

L'encadré 12-3 décrit le déroulement de la mission d'assurance centrée sur les contrôles, qui comporte trois phases fondamentales : la planification, l'exécution de la mission et la communication des résultats. Ces trois phases y sont décrites comme des étapes distinctes et séquentielles. Dans les faits, il en va néanmoins différemment, étant donné que le début et la fin de chaque phase ne sont pas clairement délimités. Il est souvent difficile de dire où s'achève la planification et où commence l'exécution. Généralement, la planification se poursuit tout au long de la mission, car des ajustements sont nécessaires à mesure que de nouvelles preuves sont mises au jour. L'exécution de la mission, elle, débute pendant la planification, puisque l'équipe d'audit interne applique des procédures destinées à collecter les informations qui lui permettront de planifier la mission. Et la communication des résultats de l'audit a aussi lieu tout au long de la mission : l'équipe d'audit interne signale des aspects importants à l'audité périodiquement, et non pas seulement dans le rapport définitif de la mission, à l'issue du processus.

L'encadré 12-3 propose un cadre de référence permettant d'analyser les différentes activités qui composent une mission d'audit. Comme indiqué plus haut, même si, au cours d'une mission d'assurance, plusieurs membres de la fonction d'audit interne mènent à bien les activités spécifiques nécessaires pour planifier, exécuter cette mission et en communiquer les résultats, c'est le responsable de l'audit interne qui exerce la responsabilité ultime des travaux d'audit effectués. Chacune des activités présentées dans l'encadré, sous les rubriques « Planifier », « Exécuter » et « Communiquer », est brièvement décrite ci-après. Les deux premières phases du déroulement des missions d'assurance sont détaillées dans le chapitre 13, *Le déroulement de la mission d'assurance*, et la troisième dans le chapitre 14, *La communication des résultats d'une mission d'assurance et les procédures de suivi*. Il convient de noter qu'une mission d'assurance centrée sur les performances comprendra habituellement bon nombre des activités qui sont énumérées dans l'encadré 12-3, mais pas toutes. Les activités précises et la manière dont elles sont menées dépendront des objectifs de la mission centrée sur les performances.

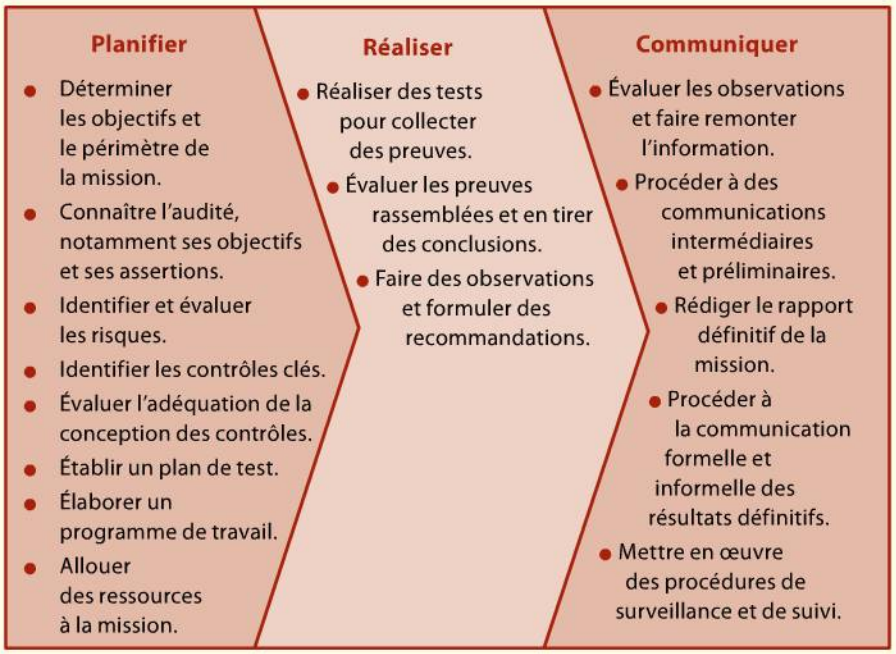
Planification des missions d'assurance

La réussite de tout projet passe par une planification efficace. Il existe en anglais une expression, parfois appelée les « six P », qui illustre ce principe : « *Proper Prior Planning Prevents Poor Performance* » (une bonne planification préalable empêche de piètres performances). Bien qu'il puisse être tentant de commencer

Copyright © 2015 Eyrolles.

ENCADRÉ 12-3

LE DÉROULEMENT DE LA MISSION D'ASSURANCE



immédiatement les tests d'audit, une méthode de planification structurée et rigoureuse contribuera à l'exécution efficace et efficiente de la mission. Si le temps et les efforts consacrés à la planification sont insuffisants, il est probable que la mission n'atteindra pas ses objectifs ou qu'elle les atteindra de façon inefficiente. Ce chapitre et les suivants visent à faire comprendre au lecteur que bâcler la planification revient à planifier l'échec de la mission. Les paragraphes ci-après expliquent en quoi consiste la planification d'une mission.

Déterminer les objectifs et le périmètre de la mission. Une première étape importante consiste à déterminer les objectifs de la mission (ce que celle-ci vise) et son périmètre (ce sur quoi elle portera et ne portera pas). À ce titre, il convient de déterminer les centres d'intérêt de l'audit interne au regard des différentes catégories d'objectifs (liés à la stratégie, aux opérations, au reporting et/ou à la conformité). La mission se concentrera-t-elle, par exemple, sur l'efficacité et l'efficience des opérations de l'audité, sur le reporting financier de l'audité, ou sur ces deux éléments ? Un autre aspect fondamental réside dans les prestations requises de la part de l'équipe d'audit interne. Ainsi, on peut attendre de l'équipe qu'elle réserve au niveau de management approprié la communication des différentes observations sur les contrôles effectués au cours de la mission, ou qu'elle exprime une opinion globale sur les contrôles portant sur le domaine ou sur le processus analysé. Le troisième aspect clé concerne les « limites » de la mission.

Copyright © 2015 Eyrolles.

Par exemple, si l'audit porte sur un processus opérationnel ou un sous-processus, où commence ce processus ou sous-processus et où finit-il ? Si l'audit porte sur une catégorie précise d'unités opérationnelles géographiquement distinctes, telles que des succursales de service ou des usines, sur quels sites l'équipe d'audit interne se rendra-t-elle et quelle partie de chaque unité opérationnelle la mission couvrira-t-elle ?

Connaître l'audité, notamment ses objectifs et ses assertions. Il est quasiment impossible d'auditer avec efficacité un domaine que l'on ne comprend pas. La réussite de toute mission dépend, dans une large mesure, de la connaissance de l'audité par l'équipe d'audit. Les auditeurs internes doivent en premier lieu cerner les objectifs et les assertions de l'audité. Les objectifs de l'audité décrivent *ce que ce dernier cherche à réaliser*. Les assertions sont des déclarations *a posteriori* sur *ce qui a été réalisé*. Les objectifs et les assertions de l'audité devraient être exprimés de manière explicite, même s'ils sont souvent implicites.

Objectifs de l'audité
Ce que l'audité cherche à réaliser.

Assertions de l'audité
Déclarations *a posteriori* sur ce qui a été réalisé.

> **Exemple.** Il existe pour le département « service après-vente » d'une organisation un objectif écrit qui requiert de répondre aux demandes des clients sous 48 heures. Cet objectif contient implicitement l'assertion selon laquelle le service après-vente a mis en œuvre les contrôles nécessaires pour donner l'assurance raisonnable que l'objectif est atteint. Le rapport sur les performances affiché dans le couloir du département affirme explicitement que le département a atteint cet objectif pour 92 % des demandes reçues au cours des trois derniers mois.

Pour l'audité, des objectifs clairs et mesurables constituent des objectifs de performance pertinents et les assertions reflètent le niveau de performance atteint. Pour l'auditeur interne, les objectifs et les assertions de l'audité forment un cadre de référence servant à définir les objectifs de la mission (*ce à quoi l'auditeur interne souhaite aboutir*). En fin de compte, la relation directe entre d'une part les objectifs et, d'autre part, les assertions de l'audité et les objectifs de la mission d'audit fixe le cadre dans lequel les auditeurs internes pourront aider l'audité à atteindre ses objectifs, ce qui permettra à son tour à toute l'organisation d'atteindre les siens.

À titre d'illustration, supposons que l'audit porte sur un processus opérationnel. L'équipe d'audit interne doit également prendre en compte d'autres aspects de ce processus :

- comment le management déploie les ressources et assigne les responsabilités afin que les objectifs du processus considéré soient atteints ;
- les risques opérationnels qui menacent le processus ;
- les contrôles clés définis et mis en œuvre en vue de maîtriser ces risques ;

Copyright © 2015 Eyrolles.

- les relations entre le processus considéré et les processus connexes ;
- ce que produit le processus (biens et/ou services par exemple) ;
- les activités qui participent à cette production ;
- les collaborateurs affectés au processus, les responsabilités qui leur ont été assignées, les pouvoirs qui leur ont été délégués et le dispositif par lequel ils doivent rendre compte ;
- les ressources matérielles et immatérielles mises en œuvre dans le cadre du processus ;
- tout changement récent, changement en cours et/ou changement attendu concernant le processus. Il convient de noter que les changements importants ont des répercussions sur les risques liés au processus et, par conséquent, sur l'adéquation de la conception et le fonctionnement effectif des contrôles.

Risque inhérent

Combinaison de facteurs de risque internes et externes à leur état d'origine, en l'absence de contrôle.

Identifier et évaluer les risques. L'équipe d'audit interne doit identifier et évaluer les risques opérationnels qui menacent la réalisation des objectifs de l'audité et, *in fine*, de l'organisation. À ce stade de la mission, elle concentre son attention sur le *risque inhérent*, c'est-à-dire sur le risque encouru par l'audité en l'absence de toute mesure que le management pourrait prendre pour réduire ou gérer les risques identifiés. L'évaluation des risques consiste à estimer leur impact (si ces risques devaient se matérialiser) et leur probabilité d'occurrence. Le fait de considérer les risques en termes de causes et d'effets permet à l'auditeur interne d'évaluer l'ampleur du problème potentiel et sa probabilité de survenue. Supposons par exemple le risque suivant : le traitement inefficace des factures fournisseurs à régler (la cause) peut empêcher de bénéficier de ristournes, entraîner des retards de paiement et mécontenter les fournisseurs concernés (les effets).

L'analyse des effets potentiels (c'est-à-dire l'impossibilité de bénéficier de ristournes, les retards de paiement et le mécontentement des fournisseurs) permet à l'auditeur interne d'estimer l'ampleur du problème potentiel et de déterminer s'il faut prêter davantage attention au risque. L'analyse de la cause potentielle (c'est-à-dire les inefficacités), ainsi que de ses raisons, aide l'auditeur interne à évaluer la probabilité de matérialisation du risque.

Contrôle clé (ou contrôle primaire)

Activité destinée à réduire les risques associés à un objectif critique de l'organisation.

L'équipe d'audit interne doit également mettre en balance les niveaux de risque évalués et les seuils de tolérance au risque définis par le management, pour déterminer si la gestion du risque est appropriée. Les niveaux de risque qui, d'après son évaluation, correspondent au seuil de tolérance peuvent être *acceptés*. Ceux qui dépassent les seuils de tolérance doivent être ramenés à un niveau acceptable. Les modalités de traitement consistent à *éviter les risques* (y compris en se séparant des activités qui les ont induits), à *partager les risques* en en transférant une partie à des tiers (par exemple, à un assureur) ou à *réduire les risques* en mettant en

Copyright © 2015 Eyrolles.

œuvre des contrôles destinés à limiter leur impact, leur probabilité d'occurrence ou les deux.

Identifier les contrôles clés. À ce stade de la planification de la mission, l'auditeur interne doit identifier les contrôles qui sont les plus cruciaux pour ramener les risques opérationnels à un niveau acceptable et, ainsi, donner l'assurance que les objectifs fixés sont atteints. Les contrôles sont détaillés dans le chapitre 6, *Le contrôle interne*, et analysés à nouveau dans le chapitre 13, *Le déroulement de la mission d'assurance*.

Évaluer l'adéquation de la conception des contrôles. L'équipe d'audit interne doit ensuite se prononcer sur la capacité des contrôles clés identifiés à ramener les risques, individuellement et collectivement, à un niveau acceptable, dans l'hypothèse où ces contrôles ont été appliqués et se déroulent comme prévu. À ce stade, les auditeurs internes doivent admettre que la relation entre risques et contrôles n'est pas biunivoque : tel contrôle peut contribuer à maîtriser plusieurs risques, et plusieurs contrôles sont parfois nécessaires pour maîtriser efficacement un risque.

Établir un plan de test. L'équipe d'audit interne doit concevoir la mission de façon à rassembler des preuves suffisantes et adéquates pour atteindre les objectifs de la mission. Pour établir un plan de test, il faut déterminer la nature, le calendrier d'application et l'étendue des procédures d'audit nécessaires à la collecte des preuves d'audit requises. Les plans de test peuvent comporter des tests directs des contrôles, des tests des performances, qui apportent des preuves indirectes sur le fonctionnement effectif des contrôles, ou les deux. Un plan destiné à tester des contrôles déjà appliqués doit permettre la collecte et l'évaluation de preuves suffisantes et adéquates, de façon à déterminer si les contrôles qui sont conçus de manière adéquate fonctionnent de manière effective.

Élaborer un programme de travail. Le programme de travail est un outil de planification extrêmement important. Il énumère les procédures d'audit nécessaires à la réalisation des objectifs de la mission. Au cours de la mission, les auditeurs internes cochent les procédures afin d'indiquer que le travail a été effectué, ce qui permet à leurs superviseurs d'examiner celui-ci et de piloter le travail qui reste à faire. À la fin de la mission, le programme achevé sert à documenter le travail effectué et montre quels ont été les intervenants et quand le travail a été effectué.

Allouer des ressources à la mission. La dernière étape de la planification consiste à allouer les ressources nécessaires pour mener à bien la mission (c'est-à-dire avec efficacité et efficience). Il faut pour cela déterminer les compétences d'audit requises, estimer le délai de réalisation de la mission, assigner celle-ci aux auditeurs internes appropriés et programmer le travail de manière à ce qu'il soit effectué rapidement.

Programme de travail de la mission

Document énumérant les procédures à mettre en œuvre, conçu pour réaliser le plan de mission.

Copyright © 2015 Eyrolles.

Exécution des missions d'assurance

Réaliser des tests pour collecter des preuves. L'exécution de la mission consiste à appliquer des procédures d'audit spécifiques, destinées à recueillir des preuves : demande de renseignements, observation d'opérations, examen de documents, analyse de la vraisemblance des informations, par exemple. Pour rassembler des preuves, il importe également de formaliser les travaux réalisés et leurs résultats obtenus. Ce processus de documentation est étudié au chapitre 10, *Les preuves d'audit et les papiers de travail*. Le chapitre 13, *Le déroulement de la mission d'assurance*, est quant à lui axé sur la conduite et la documentation des tests visant à déterminer si les contrôles ont été conçus de manière adéquate et fonctionnent de manière effective.

Évaluer les preuves d'audit rassemblées et en tirer des conclusions. Il faut une certaine capacité de jugement professionnel pour évaluer les preuves d'audit collectées, afin de se prononcer, par exemple, sur l'adéquation de la conception et le fonctionnement effectif des contrôles. L'équipe d'audit interne doit *in fine* tirer des conclusions logiques (c'est-à-dire rendre un avis en connaissance de cause) en se fondant sur les preuves qui ont été réunies. Le chapitre 13, *Le déroulement de la mission d'assurance*, montre comment un auditeur interne documente les conclusions qui se dégagent des résultats des tests. Le chapitre 14, *La communication des résultats d'une mission d'assurance et les procédures de suivi*, explique de quelle façon un auditeur interne formule et documente ses conclusions sur l'ensemble de la mission.

Faire des observations et formuler des recommandations. Les observations (ou *constats*, ou *constatations*) sont définies dans la MPA 2410-1, Contenu de la communication, comme « des exposés pertinents des faits » qui « sont le résultat d'un processus de comparaison d'un référentiel (la situation normale) et d'un fait (la situation actuelle) ». Les observations bien rédigées rapportent les éléments suivants :

- les *référentiels*, qui sont les normes, mesures ou exigences requises, utilisées pour évaluer et vérifier « ce qui devrait être » (la situation normale) ;
- les *faits*, qui sont les preuves factuelles identifiées par l'auditeur interne au cours de son examen, c'est-à-dire « ce qui est » (la situation actuelle) ;
- les *conséquences*, qui sont les effets négatifs, réels ou potentiels, qui résultent du fait que les situations diffèrent du référentiel. La MPA 2410-1 appelle aussi cet élément l'« impact » ;
- les *causes* sont les raisons de la différence entre les situations attendues et existantes, différence qui a des conséquences négatives.

Copyright © 2015 Eyrolles.

Si ce qui existe réellement correspond à ce qui devrait exister, il n'y a pas de différence, et donc pas de conséquences, ni de causes, à traiter.

« Les recommandations sont fondées sur les observations et conclusions de l'auditeur interne » (MPA 2410-1). Les recommandations de l'audit (ou *actions correctives proposées*) peuvent être documentées dans le cadre des observations ou séparément. Elles visent à combler l'écart entre les référentiels et les faits. Les recommandations d'actions correctives sont pertinentes si elles traitent des causes de cet écart, si elles proposent des solutions de long terme plutôt que des remèdes provisoires et si elles sont économiquement réalisables. Les recommandations qui traitent des symptômes et non des causes d'un problème ont généralement peu d'utilité. Le chapitre 14, *La communication des résultats d'une mission d'assurance et les procédures de suivi*, donne davantage d'informations sur l'analyse causale, de même que la MPA 2320-2, Analyse causale.

Observation

Conclusion, déduction ou jugement découlant des résultats de tests effectués par l'auditeur interne. Également appelé constat ou constatation.

Communication des résultats des missions d'assurance

La communication des résultats de l'audit est une composante essentielle de toute mission d'audit interne. Indépendamment de son contenu et de sa forme, qui peuvent varier, « la communication doit être exacte, objective, claire, concise, constructive, complète et émise en temps utile » (Norme 2420, Qualité de la communication).

Évaluer les observations et faire remonter l'information. Lorsque l'équipe d'audit interne a fait plusieurs observations, elle doit évaluer chacune d'entre elles en suivant un processus d'évaluation et de remontée de l'information, et en déterminer les répercussions sur les résultats qui seront communiqués concernant le domaine (le processus) examiné. L'encadré 12-4 illustre un mode de traitement pour des observations qui ne présentent pas toutes la même importance au sein d'une organisation. Le chapitre 14, *La communication des résultats…*, comporte une description détaillée du processus d'évaluation des observations et de remontée de l'information.

Procéder à des communications intermédiaires et préliminaires. Comme indiqué plus haut, la communication dans le cadre d'un audit interne intervient tout au long de la mission, et non pas seulement à la fin. Des problèmes se posent souvent en cours de mission, requérant l'attention immédiate ou à court terme du management. S'ils sont notifiés en temps opportun, le management peut les traiter et les régler plus tôt, parfois avant que la mission ne soit terminée. D'autres informations provisoires peuvent également être communiquées à l'audité durant la mission, par exemple des changements apportés au périmètre de l'audit et les avancées de la mission.

Copyright © 2015 Eyrolles.

Il importe que l'équipe d'audit interne donne au management la possibilité de clarifier des points et d'exprimer son opinion sur les conclusions et recommandations des auditeurs internes. De plus, ce qui est écrit est parfois interprété différemment de ce qui est dit, et les déclarations écrites comme orales peuvent être mal interprétées. L'examen des versions préalables du rapport avec le management permet ainsi de s'assurer qu'elles correspondent à ce que les auditeurs internes ont dit et écrit.

ENCADRÉ 12-4

TYPES D'OBSERVATIONS ET MESURES À PRENDRE

Types d'observations	Mesures à prendre
Observation non pertinente : un examen poussé révèle finalement que les informations sur lesquelles se fonde l'observation ne sont pas exactes ou ne sont pas pertinentes.	Mettre à jour les documents consignant les travaux effectués et l'observation, afin d'y intégrer les nouvelles informations et d'étayer la conclusion appropriée.
Observation : l'observation n'a pas à être signalée en raison de contrôles de maîtrise et/ou elle constitue une amélioration proposée pour un processus et n'a pas d'impact significatif sur le plan financier, opérationnel ou de la conformité.	Documenter les travaux effectués. Expliquer dans les papiers de travail pourquoi l'observation n'a pas à être signalée.
Observation à signaler : l'observation porte sur un risque significatif, que les contrôles en place ne ramènent pas à un niveau acceptable.	Mettre à jour les papiers de travail pour y inclure le plan d'actions du management qui a été convenu. Observer l'exécution de ce plan. Intégrer l'observation dans le rapport de la mission uniquement.
Observation significative : l'observation est jugée suffisamment importante pour être communiquée au comité d'audit.	Mettre à jour les papiers de travail pour y inclure le plan d'actions du management qui a été convenu. Observer l'exécution de ce plan. Intégrer l'observation dans le résumé du rapport de la mission.

Rédiger le rapport définitif de la mission. À ce stade, l'équipe d'audit interne est prête à agréger et à synthétiser toutes les preuves rassemblées au cours de la mission. Il n'y a pas de méthode unique imposée pour faire part des résultats globaux de la mission. Cette communication peut, par exemple, consister à :

- recenser et à hiérarchiser les observations relatives aux contrôles, mais sans aller jusqu'à rendre une conclusion globale ou à donner une assurance, à quelque niveau que ce soit, quant à l'efficacité des contrôles de l'audité ;
- rendre une conclusion appelée « assurance de forme négative » (ou « assurance modérée »). Les auditeurs internes expriment une assurance de forme négative lorsqu'ils concluent que rien de ce qu'ils ont pu observer ne laisse à penser que les contrôles de l'audité sont conçus de manière inadéquate ou ne fonctionnent pas de manière effective ;

Copyright © 2015 Eyrolles.

- rendre une conclusion appelée « assurance de forme affirmative » (ou « assurance raisonnable »). Les auditeurs internes expriment une assurance de forme affirmative lorsqu'ils concluent que, selon eux, les contrôles de l'audité sont conçus de manière adéquate et fonctionnent de manière effective.

Procéder à la communication formelle et informelle des résultats définitifs. Plusieurs *Normes* de l'IIA ont directement trait à l'élaboration et à l'émission du rapport d'audit final, notamment :

Norme 2410 – Contenu de la communication. La communication doit inclure les objectifs et le périmètre de la mission, ainsi que les conclusions, recommandations et plans d'actions.

2410.A1 – La communication finale des résultats de la mission doit, lorsqu'il y a lieu, contenir l'opinion globale des auditeurs internes et/ou leurs conclusions.

2410.A2 – Les auditeurs internes sont encouragés à faire état des forces relevées, lors de la communication des résultats de la mission.

2410.A3 – Lorsque les résultats de la mission sont communiqués à des destinataires ne faisant pas partie de l'organisation, les documents communiqués doivent préciser les restrictions à observer en matière de diffusion et d'exploitation des résultats.

Norme 2440 – Diffusion des résultats. Le responsable de l'audit interne doit diffuser les résultats aux destinataires appropriés.

2440.A1 – Le responsable de l'audit interne est chargé de communiquer les résultats définitifs aux destinataires à même de garantir que ces résultats recevront l'attention nécessaire.

2440.A2 – Sauf indication contraire de la loi, de la réglementation ou des statuts, le responsable de l'audit doit accomplir les tâches suivantes avant de diffuser les résultats à des destinataires ne faisant pas partie de l'organisation :

- évaluer les risques potentiels pour l'organisation ;
- consulter la direction générale et/ou, selon les cas, un conseil juridique ;
- maîtriser la diffusion en imposant des restrictions quant à l'utilisation des résultats.

Par ailleurs, la MPA 2410-1, Contenu de la communication, indique que tous les rapports définitifs contiennent, au minimum, « les objectifs, le périmètre et les résultats de l'audit ». Les objectifs, ce sont les objectifs de la mission, c'est-à-dire les motifs de la mission et les résultats escomptés. Le périmètre, ce sont les activités incluses dans la mission, la nature et l'étendue des procédures d'audit, ainsi que la période couverte. Le périmètre peut également,

Copyright © 2015 Eyrolles.

si nécessaire, préciser les activités connexes qui ne font pas partie de la mission, afin de délimiter l'intervention. Les résultats comprennent les observations, les conclusions, les opinions, les recommandations et les plans d'actions. Les rapports définitifs peuvent également contenir les réponses de l'audité aux conclusions, opinions et recommandations de l'équipe d'audit interne.

Les observations qu'il convient d'inclure dans le rapport définitif et formel de la mission sont celles qui doivent être communiquées impérativement pour étayer les conclusions et recommandations de l'équipe d'audit interne ou pour empêcher que ces conclusions et recommandations ne soient mal interprétées. Les observations moins importantes peuvent être communiquées de façon informelle. Les conclusions et opinions sont le résultat de l'évaluation des observations par l'équipe d'audit interne. Les recommandations, qui se fondent sur les observations et conclusions, sont les actions proposées dans l'optique de corriger des conditions existantes ou d'améliorer des opérations. Les plans d'actions sont les mesures que le management accepte de prendre pour faire suite aux observations, conclusions et recommandations de l'équipe d'audit interne.

Le responsable de l'audit interne, ou un autre auditeur interne de rang élevé qu'il désigne, doit examiner et valider le rapport final avant qu'il ne soit transmis au management de l'audité.

Le responsable de l'audit interne, ou son représentant désigné, doit déterminer auprès de qui, outre le management du domaine ou du processus audité, le rapport d'audit final sera diffusé. Les destinataires appropriés sont les membres de l'organisation à même de garantir que ce rapport recevra l'attention nécessaire. Il s'agit des personnes qui sont en mesure d'engager ou de faire engager des actions correctives. Des notes de synthèse mettant en évidence les résultats de la mission importants pour l'ensemble de l'organisation peuvent être préférables lorsque l'on s'adresse à la direction générale, au comité d'audit et au Conseil.

Il convient de noter que, d'après l'interprétation de la Norme 2440, Diffusion des résultats, même si le responsable de l'audit interne autorise quelqu'un d'autre à revoir et à approuver le rapport définitif, et à décider à qui il sera diffusé, « il/elle garde l'entière responsabilité » de ces fonctions.

Mettre en œuvre des procédures de surveillance et de suivi. Il ressort de l'encadré 12-3 que les missions d'assurance ne se terminent pas avec l'élaboration d'un rapport. Conformément à la Norme 2500, Surveillance des actions de progrès, « le responsable de l'audit interne doit mettre en place et tenir à jour un système permettant de *surveiller* la suite donnée aux résultats communiqués au management ». La Norme 2500.A1 spécifie, elle, que « le responsable de l'audit interne doit mettre en place un processus

Copyright © 2015 Eyrolles.

de *suivi* permettant de surveiller et de garantir que des mesures ont été effectivement mises en œuvre par le management ou que la direction générale a accepté de prendre le risque de ne rien faire ».

Il est très important que l'audit interne détermine si, en réponse à ses observations et recommandations, le management a effectivement engagé des actions correctives qui remédient aux dysfonctionnements en temps opportun. La charte d'audit interne doit définir la responsabilité de la fonction d'audit interne en ce qui concerne le suivi. Le responsable de l'audit interne doit déterminer la nature, le calendrier d'application et l'étendue des procédures de suivi appropriées pour la mission concernée. Les responsabilités de surveillance et de suivi que la fonction d'audit interne doit exercer sont analysées plus en détail dans la MPA 2500-1, Surveillance des actions de progrès, et dans la MPA 2500.A1-1, Processus de suivi de la mission.

Surveillance des actions de progrès

Processus de suivi mis en place par le responsable de l'audit interne, permettant de surveiller et de garantir que des mesures ont été effectivement mises en œuvre par le management ou que la direction générale a accepté de prendre le risque de ne rien faire.

LE DÉROULEMENT DE LA MISSION DE CONSEIL

Les missions de conseil conduites par l'audit interne diffèrent des missions d'assurance à plus d'un titre :

- si la nature et le périmètre d'une mission d'assurance sont déterminés par la fonction d'audit interne, lors d'une mission de conseil, la nature et le périmètre doivent être définis d'un commun accord avec le client de la mission ;
- par conséquent, les missions de conseil sont d'une nature beaucoup plus discrétionnaire que les missions d'assurance. Comme le précise le glossaire des *Normes*, les activités de conseil englobent « avis, conseil, assistance et formation ».

Le déroulement de la mission de conseil comporte les mêmes étapes que celui de la mission d'assurance décrit à l'encadré 12-3. Cependant, chaque étape n'est pas forcément nécessaire pour toutes les missions de conseil, et beaucoup d'entre elles peuvent être menées différemment. Comme l'indiquent les normes citées plus haut, les trois grandes phases de la mission – planification, accomplissement et communication des résultats – restent les mêmes.

Planification de la mission. « Les auditeurs internes doivent concevoir et documenter un plan pour chaque mission. Ce plan de mission précise les objectifs, le champ d'intervention, la date et la durée de la mission, ainsi que les ressources allouées » (Norme 2200, Planification de la mission). « Les auditeurs internes doivent établir avec le client donneur d'ordre un accord sur les objectifs et le champ de la mission de conseil, les responsabilités de chacun et plus généralement sur les attentes du client donneur d'ordre » (Norme 2201.C1). « Les auditeurs internes doivent s'assurer que le champ d'intervention permet de répondre aux objectifs convenus » (Norme 2220.C1). « Le programme de travail d'une mission

Copyright © 2015 Eyrolles.

de conseil peut varier, dans sa forme et son contenu, selon la nature de la mission » (Norme 2240.C1).

Accomplissement de la mission. « Les auditeurs internes doivent identifier, analyser, évaluer et documenter les informations nécessaires pour atteindre les objectifs de la mission » (Norme 2300, Accomplissement de la mission). Le type d'informations identifiées, analysées, évaluées et documentées varie en fonction de la nature de la mission, tout comme la nature, le calendrier d'application et l'étendue des procédures d'audit interne exécutées.

Communication des résultats. « Les auditeurs internes doivent communiquer les résultats de la mission [de conseil] » (Norme 2400, Communication des résultats). « La communication doit inclure les objectifs et le champ de la mission, ainsi que les conclusions, recommandations et plans d'actions. » (Norme 2410, Contenu de la communication). Cependant, « la communication sur l'avancement et les résultats d'une mission de conseil variera dans sa forme et son contenu en fonction de la nature de la mission et des besoins du client donneur d'ordre » (Norme 2410.C1). Par exemple, les prestations pour une mission de conseil dans laquelle le client a demandé à la fonction d'audit interne de formuler des conseils sur certains aspects différeront des prestations livrées lors des missions d'assistance et de formation.

RÉSUMÉ

Les auditeurs internes exécutent deux catégories d'activités : les activités d'assurance et les activités de conseil, qui peuvent être centrées sur les contrôles et/ou sur les performances. Pour ces deux catégories d'activités, le déroulement de la mission comprend trois grandes phases (planification, accomplissement et communication des résultats). L'encadré 12-3 décrit les principales étapes d'une mission d'assurance centrée sur les contrôles. La nature et le périmètre des missions d'assurance sont déterminés de manière unilatérale par la fonction d'audit interne, et le processus a tendance à être relativement uniforme d'une mission à l'autre. En revanche, pour chaque mission de conseil, la nature et le périmètre sont déterminés conjointement par l'audit interne et le client, et les étapes du processus varient d'une mission à l'autre.

Le présent chapitre est le premier de quatre chapitres relatifs à la conduite des missions d'audit interne. Le chapitre 13, *Le déroulement de la mission d'assurance*, décrit en détail les phases de planification et d'accomplissement, et le chapitre 14, *La communication des résultats d'une mission d'assurance et les procédures de suivi,* couvre la phase de communication des résultats. Enfin, le chapitre 15, *La mission de conseil*, contient une analyse détaillée des activités de conseil et du déroulement de la mission de conseil.

Copyright © 2015 Eyrolles.

Questions de révision



1. Quels sont les deux types d'activités réalisées par les auditeurs internes ? Donnez trois exemples pour chaque type de mission.

2. Quelles sont les trois phases du déroulement de la mission d'assurance ?

3. Quelles sont les différentes étapes de la phase de planification d'une mission d'assurance ?

4. Quelle est la relation entre les objectifs de l'audité et les assertions de l'audité ?

5. Que signifie l'expression « risque inhérent » ?

6. Pourquoi est-il utile qu'un auditeur interne exprime les risques en termes de causes et d'effets ?

7. Quelles sont les différentes modalités de traitement des risques ?

8. À quoi cela sert-il d'avoir un programme de travail bien écrit ?

9. Quelles démarches l'allocation des ressources à la mission suppose-t-elle ?

10. Quelles sont les différentes étapes de la phase d'exécution d'une mission d'assurance ?

11. Quels sont les éléments contenus dans les observations correctement rédigées ?

12. Quelles sont les caractéristiques des recommandations pertinentes ?

13. Quelles sont les principales caractéristiques qualitatives de la communication des résultats d'une mission d'audit interne ?

14. Quelles sont les différentes étapes de la phase de communication des résultats d'une mission d'assurance ?

15. Quelle est la différence entre une « assurance de forme négative » et une « assurance de forme positive » ?

16. Quelles sont les informations que doit contenir le rapport définitif d'une mission d'assurance ?

17. En quoi les missions de conseil de l'audit interne diffèrent-elles des missions d'assurance ?

Copyright © 2015 Eyrolles.

Questions à choix multiples

Sélectionnez la meilleure réponse pour chacune des questions suivantes.

1. Les tâches effectuées par l'audit interne au cours d'une mission d'assurance doivent permettre de répondre aux questions suivantes :
   I. Qu'est-ce qui explique ces résultats ?
   II. Comment les performances peuvent-elles être améliorées ?
   III. Quels sont les résultats actuels ?

   L'ordre chronologique dans lequel il faut répondre à ces questions est le suivant :
   a. III, I, II.
   b. I, III, II.
   c. III, II, I.
   d. II, III, I.

2. Au cours de la phase de planification d'une mission d'assurance, l'auditeur interne obtient des informations sur les opérations de l'audité en vue, entre autres :
   a. De développer un certain scepticisme professionnel concernant les critères de qualité retenus par le management.
   b. De formuler des suggestions constructives à l'intention du management concernant les améliorations à apporter aux contrôles internes.
   c. D'évaluer s'il convient de faire part à la direction générale et au comité d'audit des anomalies figurant dans les rapports de performance de l'audité.
   d. De comprendre les objectifs, les risques et les contrôles de l'audité.

3. Parmi les affirmations suivantes, laquelle n'illustre pas le concept de risque opérationnel inhérent ?
   a. Les liquidités sont plus exposées au vol qu'un stock de feuilles de métal.
   b. Un cadenas cassé sur une porte permet aux collaborateurs d'entrer dans une zone dans laquelle ils ne sont pas autorisés à pénétrer.
   c. Les transactions supposant des calculs complexes sont davantage susceptibles de contenir des erreurs que les transactions ne requérant que des calculs simples.
   d. Le progrès technologique peut rendre un produit donné obsolète.

4. Une évaluation complète du risque suppose l'analyse des causes et des effets. Parmi les affirmations suivantes sur l'analyse des causes et des effets, laquelle est fausse ?
   a. Il ne faut analyser les causes et les effets d'un risque donné qu'une fois que l'auditeur interne a obtenu des preuves de l'existence d'un problème.
   b. Analyser les causes et les effets d'un risque donné permet de se faire une idée de la meilleure manière de gérer ce risque.

Copyright © 2015 Eyrolles.

c. Analyser les effets d'un risque donné permet de se faire une idée de la taille relative du risque et de l'importance relative de l'objectif menacé par ce risque.
d. Analyser les causes fondamentales d'un risque donné aide l'auditeur interne à formuler des recommandations en vue de ramener le risque à un niveau acceptable.

5. Les auditeurs internes cherchent à comprendre les contrôles et réalisent des tests sur les contrôles dans l'objectif :
   a. De détecter les erreurs importantes dans les soldes des comptes.
   b. De ramener le risque de contrôle à un niveau acceptable.
   c. D'évaluer l'adéquation de la conception et le fonctionnement effectif des contrôles.
   d. D'évaluer les risques inhérents associés aux transactions.

6. Si l'évaluation par un auditeur interne de la conception des contrôles internes indique que ces contrôles sont conçus de manière adéquate, il faut ensuite :
   a. Tester le fonctionnement effectif des contrôles.
   b. Établir un diagramme de flux décrivant le système de contrôle interne.
   c. Conclure que le risque résiduel est faible.
   d. Conclure que le risque de contrôle est élevé.

7. Les observations d'audit interne dont il est fait état découlent d'un processus comparant « ce qui devrait être » à « ce qui est ». Lorsque, pour l'audit d'une fonction de trésorerie, on définit « ce qui devrait être », quel serait, parmi les critères suivants, le moins utile pour évaluer les opérations actuelles ?
   a. Les bonnes pratiques de la fonction de trésorerie dans le secteur.
   b. Les règles et procédures de l'organisation définissant la délégation de pouvoir et l'assignation des responsabilités.
   c. Les objectifs de performance établis par la direction générale.
   d. Les opérations de la fonction de trésorerie telles que documentées au cours du précédent audit.

8. Il arrive que les auditeurs internes expriment des opinions qui viennent s'ajouter aux observations énoncées dans leurs rapports. La conscience professionnelle impose que les opinions des auditeurs internes soient :
   a. Fondées sur des preuves suffisantes et adéquates.
   b. Limitées à l'efficacité des dispositifs de contrôle interne.
   c. Exprimées uniquement si le management ou le comité d'audit le demandent.
   d. Fondées sur l'expérience et exemptes d'erreurs de jugement.

Copyright © 2015 Eyrolles.

9. Parmi les déclarations suivantes, laquelle décrit le mieux la responsabilité de la fonction d'audit interne pour les activités faisant suite à une mission d'assurance ?
   a. La fonction d'audit interne doit déterminer si les actions correctives ont été mises en œuvre et produisent les résultats attendus, ou si la direction générale assume le risque associé à l'absence d'actions.
   b. La fonction d'audit interne doit déterminer si le management a engagé des actions correctives mais elle n'est pas habilitée à déterminer si ces actions produisent les résultats attendus. En effet, cette tâche incombe au management.
   c. Le responsable de l'audit interne ne doit planifier les activités de suivi que si la direction générale ou le comité d'audit le lui ont demandé. Sinon, ces activités sont discrétionnaires.
   d. Les activités de suivi ne sont pas nécessaires si l'audité s'est engagé par écrit à mettre en application les recommandations formulées par les auditeurs internes.

10. Les auditeurs internes réalisent à la fois des missions d'assurance et de conseil. Parmi les missions suivantes, laquelle serait classée dans les missions de conseil ?
   a. Évaluer directement la conformité de l'organisation aux lois et règlements.
   b. Évaluer l'adéquation de la conception des activités de pilotage à l'échelle de l'entité dans l'organisation.
   c. Faciliter l'évaluation par la direction générale des risques qui menacent l'organisation.
   d. Aider l'auditeur externe dans le cadre de sa mission d'audit des états financiers.

Copyright © 2015 Eyrolles.

Thèmes de discussion

1. Rappelez la définition du risque inhérent. Pourquoi est-ce important que les auditeurs internes s'attachent au risque inhérent pendant la phase de planification d'une mission d'assurance ?

2. Le COSO définit le risque comme la possibilité qu'un événement se produise et ait une incidence défavorable sur la réalisation des objectifs. Voici un exemple d'objectif et d'événement :

Objectif	Événement
Protéger les ressources et les citoyens de la ville	Un accident à l'intersection de quatre voies

   a. Citez trois conséquences négatives potentielles de l'événement.

   b. Citez trois facteurs de risque inhérent qui rendent l'événement plus ou moins probable.

   c. Les autorités de la ville doivent décider comment traiter ce risque. Elles peuvent notamment choisir (1) d'éviter le risque ou (2) de ramener le risque à un niveau acceptable.

      1. Expliquez comment la ville peut éviter le risque.
      2. Citez *deux* manières dont la ville peut réduire le risque.

3. Lisez les deux affirmations ci-dessous.
   - Évaluer l'adéquation de la conception des contrôles est nécessaire mais pas suffisant si l'objectif d'une mission d'assurance est de parvenir à une conclusion sur l'efficacité générale des contrôles.
   - Si un auditeur interne détermine qu'un contrôle n'est pas conçu de manière adéquate, il n'y a aucune raison de tester le fonctionnement effectif du contrôle.

   Êtes-vous d'accord avec chacune de ces affirmations ? Expliquez pourquoi.

Copyright © 2015 Eyrolles.

4. Réfléchissez aux manières suivantes d'exprimer les résultats généraux d'une mission d'assurance, décrites dans ce chapitre.
   - Recenser et hiérarchiser les observations, mais sans aller jusqu'à donner une assurance, à quelque niveau que ce soit.
   - Rendre une conclusion appelée « assurance de forme négative » (ou « assurance modérée »).
   - Rendre une conclusion appelée « assurance de forme positive » (ou « assurance raisonnable »).

   a. Quel niveau d'assurance requiert les preuves d'audit les plus probantes ? Pourquoi ?

   b. De quels autres facteurs, le cas échéant, un responsable de l'audit interne peut-il tenir compte lorsqu'il décide laquelle de ces trois options est la plus appropriée à une mission d'assurance donnée ?

5. Les auditeurs internes mènent deux types d'activités, l'assurance et le conseil.

   a. Quelles sont les différences au niveau de la finalité de ces deux catégories d'activités ?

   b. Par ailleurs, en quoi les missions de conseil diffèrent-elles des missions d'assurance ?

Copyright © 2015 Eyrolles.

ÉTUDE DE CAS

[1] La direction générale de l'organisation AFR Manufacturing a demandé à son équipe d'auditeurs internes de conduire un audit de la sécurité opérationnelle des perceuses à colonne pour pièces métalliques de l'unité de production. Plus précisément, les auditeurs internes doivent déterminer dans quelle mesure le matériel et les opérateurs des perceuses se conforment aux règles de sécurité de l'organisation.

On a dénombré cinq blessures avec arrêt de travail chez les opérateurs de ces perceuses au cours des six derniers mois. Ces arrêts de travail représentent en tout 37 heures. Le management estime que la mise hors service des perceuses, ainsi que le recul de la productivité qui en résulte, ont amputé le chiffre d'affaires d'environ 265 000. Outre ces blessures, deux autres opérateurs ont souffert d'une perte d'audition sensible pendant ces six mois.

Les auditeurs internes apprennent que les règles de sécurité de l'organisation comprennent les dispositions énumérées ci-après.

IV. Les opérateurs sont tenus de porter des lunettes de sécurité, des bouchons d'oreille et des gants de protection.

V. Les perceuses doivent être dotées d'un capot de sécurité en plastique transparent ainsi que d'un protecteur qui permet d'amener en toute sécurité les pièces de métal.

VI. Les perceuses sont actionnées par un mouvement du genou droit de l'opérateur.

Les auditeurs internes observent que le matériel est relativement en mauvais état et que rien ne prouve qu'il bénéficie d'une maintenance régulière. Les pointes émoussées ne sont pas remplacées et les pointes cassées continuent d'être utilisées, car il n'y a pas de pointes neuves en stock. Sur deux des 10 perceuses, le capot de protection a disparu. Cinq des dix opérateurs portent des bouchons d'oreille de protection au moment où les auditeurs visitent l'usine, et six portent des lunettes. Les auditeurs constatent que sur quatre des machines, les manettes activées par le genou se coincent, parfois, en position marche ou arrêt. Les auditeurs ont une impression générale de négligence de la part de la direction de la production, des opérateurs et des collaborateurs de la maintenance.

1. Sur la base du scénario présenté ci-dessus :
   a. énoncez clairement l'objectif de la mission de l'audit interne ;
   b. rédigez une ou plusieurs observations d'audit interne mentionnant le fait, les référentiels, la/les conséquence(s) et la/les cause(s) .

2. Référez-vous à l'encadré 12-4. À quel niveau placeriez-vous la ou les observations que vous avez rédigées en A.2. ci-dessus ? Expliquez clairement pourquoi.

3. Rédigez une note à l'attention de la direction générale dans laquelle vous décrivez une mission de conseil que la fonction d'audit interne pourrait mener compte tenu des résultats de l'audit de la sécurité opérationnelle.

Copyright © 2015 Eyrolles.


Copyright © 2015 Cytolles



CHAPITRE 13
LE DÉROULEMENT DE LA MISSION D'ASSURANCE

Objectifs pédagogiques

- Décrire comment la finalité d'une mission d'assurance influe sur les objectifs de l'audit.
- Déterminer les objectifs et le périmètre de la mission.
- Décrire les différentes catégories et sources d'information qui permettent à l'auditeur interne de comprendre le processus de réalisation d'une mission d'assurance.
- Documenter les flux de processus simples en présentant les principales étapes du processus, les interfaces et les services concernés.
- Évaluer les risques au niveau du processus.
- Faire la distinction entre les contrôles clés et les contrôles qui ne doivent pas être considérés comme clés.
- Décrire comment évaluer l'adéquation de la conception des contrôles au niveau des processus.
- Concevoir différentes catégories de méthodes de test, selon la spécificité du processus et les objectifs de la mission.
- Élaborer un programme de travail général destiné à encadrer le déroulement de la mission.
- Préciser les ressources qui devront être affectées à la mission ainsi que le calendrier de cette dernière.
- Réaliser différents types de tests afin de recueillir des preuves et de documenter ces tests.
- Évaluer les preuves résultant des procédures d'assurance afin de tirer des conclusions reposant sur les résultats des tests.
- Faire des observations et formuler des recommandations.

Ce chapitre décrit les différentes étapes du déroulement d'une mission d'assurance axée sur les contrôles. Plus précisément, le lecteur pourra y prendre connaissance des principales étapes de la planification et de l'exécution d'une

Copyright © 2015 Eyrolles.

ENCADRÉ 13-1

DISPOSITIONS DU CRIPP PERTINENTES RELATIVES AU CHAPITRE 13

Norme 2200 – Planification de la mission
Norme 2201 – Considérations relatives à la planification
Norme 2210 – Objectifs de la mission
Norme 2220 – Champ de la mission
Norme 2230 – Ressources affectées à la mission
Norme 2240 – Programme de travail de la mission
Norme 2300 – Accomplissement de la mission
Norme 2310 – Identification des informations
Norme 2320 – Analyse et évaluation
Norme 2330 – Documentation des informations
Norme 2340 – Supervision de la mission

Modalité Pratique d'Application 2200-1 :	Planification de la mission
Modalité Pratique d'Application 2210-1 :	Objectifs de la mission
Modalité Pratique d'Application 2210.A1-1 :	Évaluation des risques dans la planification de la mission
Modalité Pratique d'Application 2230-1 :	Ressources affectées à la mission
Modalité Pratique d'Application 2240-1 :	Programme de travail de la mission
Modalité Pratique d'Application 2330-1 :	Documentation des informations
Modalité Pratique d'Application 2330.A1-1 :	Contrôle des dossiers d'audit
Modalité Pratique d'Application 2330.A2-1 :	Conservation des dossiers
Modalité Pratique d'Application 2340-1 :	Supervision de la mission

mission d'assurance, énumérées à l'encadré 13-2, déjà présenté dans le chapitre précédent (encadré 12-2).

Mission d'assurance
Examen objectif d'éléments probants, effectué en vue de fournir à l'organisation une évaluation indépendante des processus de gouvernement d'entreprise, de management des risques et de contrôle.

La première section de ce chapitre s'attache à la planification. Cet aspect est traité de manière approfondie, car une planification efficace fait partie intégrante du succès d'une mission. S'il respecte ces étapes, l'auditeur aura la relative assurance que sa mission sera :

- complète ;
- en accord avec les objectifs de l'organisation ;
- en accord avec la charte d'audit interne.

Après avoir bien étudié cette section, le lecteur sera convaincu de l'importance primordiale que revêt la planification : « Un échec de la planification, c'est la planification de l'échec. »

La deuxième section de ce chapitre est consacrée à l'exécution du programme de tests conçu pendant la phase de planification. Si l'exécution des tests d'audit prend normalement davantage de temps que la planification de la mission, cette section est plus courte que celle consacrée à la planification, car les étapes à étudier sont relativement peu nombreuses et l'auditeur doit simplement les répéter afin de tester les différentes assertions relatives

Copyright © 2015 Eyrolles.

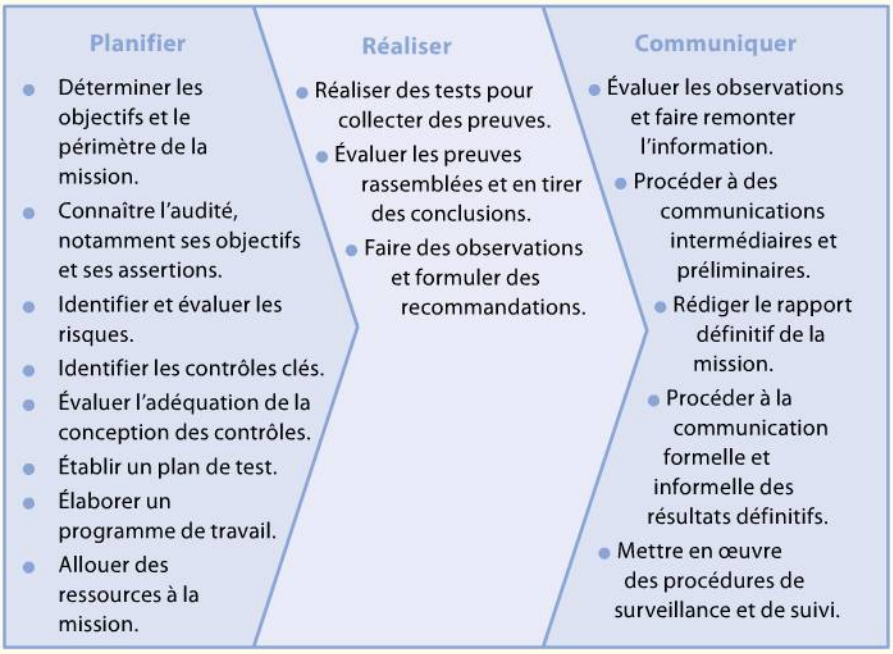
aux contrôles. L'exécution de la mission d'assurance est traitée au chapitre 12, *Introduction au processus d'audit*. De plus, les techniques d'évaluation et de compte rendu des observations d'audit sont décrites au chapitre 14, *La communication des résultats d'une mission d'assurance et les procédures de suivi*. La section consacrée à l'exécution se concentre donc sur l'application de ces concepts, plutôt que sur leur énoncé. Grâce aux informations contenues dans ce chapitre, l'auditeur dispose de connaissances solides sur la manière de planifier et de conduire la quasi-totalité des missions d'assurance.

L'ensemble de ce chapitre est ponctué d'exemples pour nombre des principales étapes, qui illustrent la façon dont celles-ci peuvent être mises en œuvre et consignées dans une documentation. Ces exemples concernent le processus relatif aux Comptes fournisseurs (CF) et aux décaissements d'une organisation fictive, **Books 2 Buy**. Ce processus de décaissement a été retenu, car il existe dans la plupart des organisations, quels que soient leur taille ou leur secteur. L'encadré 13-3 présente **Books 2 Buy** de manière succincte. Ces données permettent de rendre ces exemples plus réalistes.

La planification est la première phase d'une mission d'assurance ; elle s'articule en plusieurs étapes. L'encadré 13-4 présente une liste de ces étapes, qui seront chacune examinées plus en détail dans les sections suivantes.

ENCADRÉ 13-2

LE DÉROULEMENT DE LA MISSION D'ASSURANCE



Copyright © 2015 Eyrolles.

DÉTERMINER LES OBJECTIFS ET LE PÉRIMÈTRE DE LA MISSION

Motivations d'une mission

Comme examiné au chapitre 12, il existe plusieurs catégories de missions d'assurance, et plusieurs raisons peuvent justifier de mener l'une de ces missions. Le type de mission et ses motivations peuvent influer de manière significative sur la façon dont la mission est exécutée. Il importe donc de comprendre ce qui motive l'exécution de la mission avant d'en commencer la planification.

Plusieurs raisons justifient de procéder à une mission d'assurance, dont voici une liste non exhaustive :

- La mission a été inscrite dans le plan d'audit interne en raison des risques inhérents repérés lors de l'évaluation des risques opérationnels, des risques détectés lors du dernier audit ou d'autres facteurs pertinents.

ENCADRÉ 13-3

DONNÉES RELATIVES À BOOKS 2 BUY, EXEMPLE ILLUSTRANT LE CHAPITRE 13

- Books 2 Buy est un éditeur de manuels scolaires qui propose des outils pédagogiques pour l'enseignement primaire (K-8), le secondaire et le post-secondaire.
- Cette société est cotée en bourse, et basée à Dallas, au Texas. Elle compte des clients aux États-Unis, au Canada, en Angleterre, en Afrique du Sud, au Japon, en Australie et en Nouvelle-Zélande.
- Books 2 Buy dispose en interne d'une équipe de professionnels de l'édition et sous-traite la rédaction des manuels à des universitaires de renom et autres professionnels.
- Toutes les activités d'impression et de reliure sont sous-traitées, ce qui représente l'un des principaux postes de coût de l'organisation.
- L'organisation loue des locaux pour ses centres de distribution, qui sont répartis dans tous les pays où elle opère.
- Books 2 Buy dégage un chiffre d'affaires annuel total de 550 millions, ses dépenses de liquidités se montent à environ 480 millions, ses dépenses hors liquidités (par exemple les amortissements) à environ 25 millions et ses dépenses d'investissement à long terme à environ 40 millions.
- En moyenne, ses 480 millions de dépenses annuelles de liquidités se répartissent comme suit :

	% des décaissements	% du montant
Virements	10 %	60 %
Chèques générés par ordinateur	88 %	38 %
Chèques établis manuellement	2 %	2 %

Si les décaissements peuvent être libellés dans des monnaies différentes, tous sont traités depuis une fonction centralisée des décaissements située à Chartres.

Copyright © 2015 Eyrolles.

Pour ces missions, l'auditeur interne doit comprendre les risques opérationnels qui ont incité à inscrire la mission dans le plan d'audit, puis concevoir un plan de mission qui permettra d'apporter des assurances concernant l'adéquation de la conception et le fonctionnement effectif des contrôles instaurés pour maîtriser ces risques.

- Des missions de nature réglementaire. L'objectif peut porter notamment sur la conformité réglementaire des états financiers et leur fiabilité dans le cadre de la section 404 de la loi *Sarbanes-Oxley*.

Commentaire du traducteur

La mission peut porter plus généralement sur l'appréciation du dispositif de contrôle interne et de gestion des risques afin de répondre aux d'autres exigences telles que celles de Solvabilité II (Directive 2009/138/CE du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice) ou de la loi de sécurité financière en France.

Dans le cas d'audit de conformité réglementaire, l'auditeur interne doit veiller à ce que la mission soit conçue de manière à tester les aspects énoncés par les textes applicables (par exemple donner une assurance quant à l'adéquation de la conception et au fonctionnement effectif du contrôle interne relatif au reporting financier).

- Des missions *a posteriori* suite à l'identification de fraude ou d'anomalie significative. Cela peut être un événement récent (par exemple une catastrophe naturelle, une fraude interne ou la faillite d'un client) qui a mis à l'épreuve le processus dans des circonstances inhabituelles. Le management souhaite alors une analyse *a posteriori* afin de déterminer l'efficacité du processus de contrôle interne. Pour ce type de mission, l'auditeur interne devra adapter ses tests et leurs évaluations en fonction de l'événement générateur.
- Des missions qui permettent d'accompagner l'organisation dans ses évolutions et ses adaptations. Le management souhaite que l'on confirme rapidement que ces évolutions n'affectent pas la pertinence du dispositif de contrôle interne. Pour ce type de mission, la fonction d'audit interne doit procéder à un audit complet des contrôles ou peut décider de limiter son audit aux contrôles qui ont changé.

Commentaire du traducteur

L'IFACI a publié un ouvrage qui s'intitule, Les outils de l'audit interne, *comprenant 40 fiches qui présentent les différentes étapes du processus de déroulement d'une mission d'audit interne.*

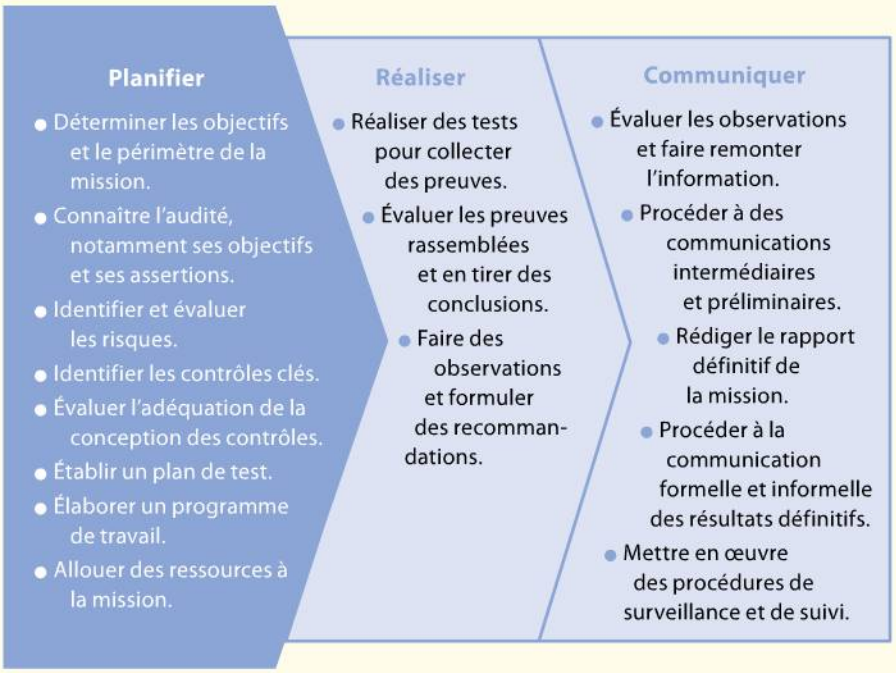
Finalité de la mission

– Plan d'audit.
– Obligation de conformité.
– Analyse *a posteriori* (*post mortem*).
– Changements significatifs.

Copyright © 2015 Eyrolles.

ENCADRÉ 13-4

LE DÉROULEMENT DE LA MISSION D'ASSURANCE



D'autres types de facteurs peuvent motiver la réalisation d'une mission. L'essentiel pour l'équipe d'audit est qu'elle comprenne bien les raisons ou les facteurs qui justifient la réalisation de la mission. Par exemple, le management peut vouloir évaluer les performances d'un processus donné par rapport aux attentes, plutôt que de rechercher une assurance concernant les différentes assertions évoquées plus haut. En effet, selon la finalité de la mission, l'orientation du programme de travail, les tests réalisés seront différents. Comprendre les enjeux d'une mission, quels qu'ils soient, permet de gérer au mieux l'organisation des tâches lors de la mission en fonction d'objectifs prioritaires.

Exemple Books 2 Buy. Si la mission consacrée au processus de décaissement a été inscrite dans le plan annuel d'audit interne, c'est en raison des risques inhérents identifiés lors du processus d'évaluation des risques opérationnels (voir chapitre 5, *Les processus et les risques*, pour plus de détails sur le processus d'évaluation des risques opérationnels).

Objectifs de la mission

Ce que vise à accomplir un audit.

Définir les objectifs de la mission

Une fois que les motivations de la mission d'assurance sont comprises, il convient de définir les objectifs affichés de la mission. Ces objectifs, qui sont normalement mentionnés dans le rapport

Copyright © 2015 Eyrolles.

définitif de la mission d'assurance, précisent clairement ce à quoi la mission essaie d'aboutir. Si les objectifs peuvent être énoncés de diverses manières, il faut que les assurances que la mission entend apporter soient claires. Par exemple, la formulation des objectifs peut commencer par des expressions telles que :

- évaluer l'adéquation de la conception de…
- déterminer le fonctionnement effectif de…
- évaluer la conformité avec…
- déterminer l'efficacité et l'efficience de…
- évaluer l'exactitude de…
- évaluer la réalisation de…
- évaluer les performances de…

La définition des objectifs au début de la mission constitue une étape critique. Si ces objectifs ne sont pas arrêtés formellement, l'équipe d'audit interne risque de ne pas être en phase avec les motivations de la mission, et donc de procéder à des démarches inappropriées ou inutiles.

> **Exemple Books 2 Buy.** La mission a pour objectif d'évaluer l'adéquation de la conception et le fonctionnement effectif des contrôles mis en place pour maîtriser les risques liés au processus de décaissement.

Périmètre de la mission

Périmètre (ou champ)

Ce qui est ou non inclus dans une mission.

Sous-processus

Composante ou portion discrète et reconnaissable d'un processus.

Une fois que les objectifs ont été définis, il convient de déterminer le périmètre de la mission. Dans la mesure où une mission ne couvre pas forcément tout ce qui peut être audité et qui se rapporte aux objectifs de la mission, il convient de préciser clairement ce qui est ou non inclus dans la mission. Ces énoncés du périmètre de la mission peuvent comporter les éléments suivants.

- **Délimitation du processus.** Si certains processus sont restreints et autonomes, d'autres couvrent un périmètre très large et peuvent être interconnectés avec d'autres processus. Il importe donc de définir à quel stade du processus la mission commence (par exemple, les intrants initiaux découlant des transactions ou d'autres processus) et à quel stade elle se termine (par exemple, les rapports, les états financiers ou les extrants vers d'autres processus).
- **Sites dans le périmètre et hors du périmètre de la mission.** Pour les processus qui s'étendent sur plusieurs sites, il convient de préciser les sites qui sont concernés par la mission.

Copyright © 2015 Eyrolles.

- **Sous-processus.** Certains processus étendus sont composés d'un ensemble de sous-processus (ainsi, le processus de décaissement peut comprendre les sous-processus suivants : rapprochement et autorisation des factures, saisie des décaissements et traitement des paiements).
- **Composantes.** Certaines parties d'un processus peuvent être volontairement omises. Par exemple, si l'application informatique soutenant un processus a fait l'objet d'un audit assez récemment, on peut inclure dans le périmètre les contrôles manuels associés à ce processus, mais en exclure les procédures automatisées.
- **Période auditée.** Une mission peut couvrir une année civile, les douze derniers mois, une période s'arrêtant à une date précise (par exemple, au 31 décembre) ou toute autre période.

Les décisions concernant le périmètre de la mission requièrent l'expertise de l'auditeur interne. Ce dernier doit veiller à ce que le périmètre soit suffisant pour pouvoir répondre aux objectifs de la mission. En formulant précisément l'énoncé du périmètre de la mission, l'équipe d'audit interne pourra mieux cibler ses tests spécifiques. En outre, les destinataires du rapport d'audit seront mieux à même d'interpréter les constats lorsque les objectifs de la mission ont été bien précisés.

Exemple Books 2 Buy. Les éléments suivants seront inclus dans le périmètre de la mission.

- Les procédures liées au décaissement, depuis la réception d'une facture ou d'un document analogue prouvant la création d'une dette jusqu'au décaissement de fonds et à l'enregistrement de ce décaissement dans le grand livre général.
- Les trois types de décaissement (virements, chèques générés par informatique et chèques établis manuellement).
- Les décaissements en euros et dans d'autres monnaies.
- Les décaissements qui ont été traités au cours des 12 derniers mois.

Résultats et prestations attendus

Avant de passer à l'étape de planification, il reste une dernière tâche à exécuter. Si les objectifs et le périmètre ont été définis, il n'est pas inutile d'appliquer l'une des *Sept habitudes des gens efficaces* : « Commencer en gardant à l'esprit la fin »[1]. Il existe deux « fins » importantes à prendre en compte, qui facilitent la validation des objectifs de la mission et du périmètre définis :

- les résultats potentiels des tests à effectuer pendant la mission ;
- les attentes de l'audité en ce qui concerne la communication des résultats de la mission.

Copyright © 2015 Eyrolles.

Chacune est décrite plus en détail ci-après.

- **Résultats potentiels des tests à effectuer pendant la mission.** S'il est capable d'anticiper les différentes catégories d'anomalies susceptibles d'être identifiées dans les tests lors d'une mission donnée, l'auditeur interne peut plus facilement planifier ces tests et apporter une assurance raisonnable que ces anomalies sont détectées. Les anomalies les plus fréquentes sont :
  - erreurs dans les états financiers ou mauvaises classifications dans les comptes, les soldes ou la communication financière ;
  - déficiences des contrôles, signalant que certains contrôles ne produisent pas les effets escomptés, à savoir maîtriser les risques pour les ramener au niveau souhaité ;
  - insuffisances dans la réalisation des objectifs, dues à des déficiences dans les contrôles ou à un fonctionnement inadéquat de ceux-ci ;
  - inefficacités, dues au fait que les ressources ne sont pas affectées de manière optimale ;
  - non-conformité, lorsque les lois, règlements ou règles applicables ne sont pas respectés de manière systématique.
- **Attentes de l'audité en ce qui concerne la communication des résultats de la mission.** Comprendre la forme et le contenu du rapport final aide l'auditeur interne à collecter toutes les informations requises au cours de la mission. Les catégories habituelles de communications sont les suivantes :
  - les rapports internes globaux sont en général largement diffusés, et il faut donc que les preuves soient suffisantes et adéquates pour étayer les conclusions et recommandations d'amélioration ;
  - les notes internes, parfois diffusées de manière plus restreinte, décrivent les travaux effectués et étayent les conclusions et recommandations uniquement dans les proportions nécessaires pour que les lecteurs visés puissent comprendre les déficiences sous-jacentes ;
  - les rapports destinés à des tiers doivent partir du principe que ces derniers connaissent moins bien les règles et procédures propres à l'organisation que les auteurs internes et ont donc besoin d'informations plus détaillées pour comprendre la nature des observations et recommandations, ainsi que le contexte dans lequel elles s'inscrivent ;
  - parfois, un niveau de confidentialité élevé est nécessaire pour certaines missions. Il convient d'aborder ces questions en amont, avec les responsables du processus, si l'on veut que la prestation attendue respecte le niveau de confidentialité requis.

Audité

Filiale, unité opérationnelle, service, groupe ou autre subdivision en place dans une organisation qui fait l'objet d'une mission d'assurance.

Copyright © 2015 Eyrolles.

Exemple Books 2 Buy. Toutes les anomalies potentielles évoquées sont susceptibles de survenir lors de cette mission, et l'équipe d'audit interne doit donc concevoir les tests en conséquence. Le document livrable *in fine* est un rapport d'audit interne global standard (pour des exemples de livrables envisageables, voir le chapitre 14, *La communication des résultats d'une mission d'assurance et les procédures de suivi).*

COMPRENDRE L'AUDITÉ

Lorsque l'équipe d'audit interne planifie une mission, elle doit d'abord comprendre l'audité (expression employée, dans ce chapitre, comme synonyme de « processus » ou de « domaine » couvert par le périmètre de la mission). Si l'auditeur n'a pas une vision complète du domaine qu'il doit auditer, son plan d'audit est incomplet ou les ressources d'audit interne sont affectées à mauvais escient. Bien comprendre le processus constitue donc une étape très importante.

Détermination des objectifs de l'audité

Objectifs de l'audité

Ce que l'audité cherche à réaliser.

Pour comprendre le processus, il faut d'abord en déterminer les principaux objectifs. L'auditeur interne sait ainsi pourquoi le processus existe, ce qui se révèle important au moment d'identifier et d'évaluer les risques et les contrôles au niveau de ce processus. Il convient de noter que cette étape de la mission correspond à la section « Fixation des objectifs » de l'ouvrage « Le Management des risques de l'entreprise, Cadre de référence – Techniques d'application » publié par le *Committee of Sponsoring Organizations of the Treadway Commission* (COSO). Cet ouvrage est traité plus en détail au chapitre 4, *La gestion des risques*, ainsi que dans d'autres sections de ce manuel.

Un processus donné peut avoir différentes catégories d'objectifs. Leur description peut suivre la classification en quatre catégories, opérée par le cadre de référence relatif au management des risques de l'entreprise élaboré par le COSO. Plus précisément, les objectifs au niveau des processus peuvent être présentés comme suit (voir aussi les exemples pour le processus de décaissement).

- Les objectifs liés aux opérations sont les plus courants au niveau des processus dont ils définissent généralement la raison d'être. Ils se focalisent sur le pilotage et la réalisation des activités et sont de ce fait orientés vers l'exactitude, le caractère opportun, l'exhaustivité ou le contrôle de certains critères. De plus, les objectifs liés aux opérations visent essentiellement à s'assurer de l'efficacité et de l'efficience des activités et de la sauvegarde des actifs.

Copyright © 2015 Eyrolles.

Exemple Books 2 Buy. Un processus de décaissement peut répondre aux objectifs suivants :

- payer la somme exacte figurant sur les factures afin d'éviter le report de régularisations sur des factures ultérieures ou les pénalités pour paiement insuffisant des dettes à court terme ;
- payer les factures en temps opportun afin de bénéficier de remises (le cas échéant) ou d'éviter des pénalités de retard ;
- enregistrer tous les décaissements précisément dans les fichiers comptables et pour la période comptable correspondante ;
- suivre en fonction d'indicateurs de rentabilité pour permettre une maîtrise des coûts ;
- veiller à ce que chaque décaissement représente des obligations « *a payé en toute bonne foi* ».

- Les objectifs liés au reporting au niveau du processus sont conçus pour répondre aux besoins de reporting interne ou externe de l'organisation.

  Exemple Books 2 Buy. Les informations émanant du processus de décaissement peuvent être utilisées pour :

  - la communication interne d'informations sur les flux de trésorerie, qui aident le trésorier à préparer les prévisions hebdomadaires de ces flux ;
  - étayer les informations sur la liquidité mentionnées dans les déclarations obligatoires aux autorités.

- Les objectifs liés à la conformité au niveau du processus peuvent porter sur la conformité aux lois et règlements externes (définition du COSO), à la politique interne ou aux contrats (incluse dans la définition de l'IIA au même titre que les lois et règlements externes).

  Exemple Books 2 Buy. Les objectifs liés à la conformité des décaissements peuvent être les suivants :

  - veiller à ce que les décaissements respectent la réglementation bancaire et les lois anti-blanchiment de capitaux ;
  - veiller à ce que les décaissements soient autorisés conformément à la politique de délégation de pouvoir de l'organisation.

- Les objectifs stratégiques au niveau du processus sont ceux qui visent spécifiquement à servir les objectifs stratégiques de l'organisation. S'ils ne sont pas toujours évidents pour les personnes qui exécutent les tâches au niveau du processus, ils sont importants, car ils créent un lien entre les activités quotidiennes et les stratégies qui conduisent l'organisation au succès. Il convient de noter que la présente analyse des objectifs stratégiques s'écarte de la définition qu'en donne le COSO dans le *Référentiel intégré de contrôle interne – Principes de mise en œuvre et de pilotage*, qui est traitée au chapitre 6, *Le contrôle*

Catégories d'objectifs d'après le COSO

– Objectifs liés aux opérations.
– Objectifs liés au reporting.
– Objectifs liés à la conformité.
– Objectifs liés à la stratégie.

Copyright © 2015 Eyrolles.

interne. Les objectifs stratégiques au sens du COSO n'existent qu'à l'échelle de l'entité. Cependant, lorsqu'il effectue une mission d'assurance, l'auditeur interne a besoin d'appréhender le processus comme une composante de l'organisation dans son ensemble, et notamment certains processus dont les objectifs sont stratégiques par nature.

Exemple Books 2 Buy. Dans une organisation ayant adopté une stratégie spécifique pour la trésorerie ou la liquidité, une fonction de décaissement peut viser les objectifs suivants :

- payer les factures en respectant les directives relatives aux flux de trésorerie édictées par le service de la trésorerie, afin de préserver la liquidité courante de l'organisation.

- D'autres objectifs peuvent également être établis pour un processus spécifique à un service.

  Exemple Books 2 Buy. Si le management chargé du décaissement voulait développer la transversalité des compétences de ses collaborateurs, l'objectif suivant pourrait être retenu :

  - assurer une formation polyvalente de chaque collaborateur, de manière à ce que des binômes soient capables d'exécuter toutes les tâches importantes pour le service.

Le propriétaire du processus ou les collaborateurs concernés peuvent être en mesure de donner une liste d'objectifs relatifs au processus. Cependant, bien souvent, ces objectifs n'auront pas été énoncés formellement. Dans un tel cas, l'auditeur interne doit animer des discussions avec les personnes concernées par le processus afin d'en déterminer les principaux objectifs. Les questions suivantes pourront se révéler utiles durant ces discussions, ou pour faciliter les séances de réflexion collective entre les membres de l'équipe d'audit interne si les personnes concernées par le processus ne sont pas disponibles.

- Pourquoi ce processus existe-t-il, à savoir quelle est sa finalité première ?
- Parmi les objectifs stratégiques de l'organisation, lesquels sont affectés ou influencés par ce processus, et comment ?
- Quelles initiatives le processus entreprend-il ou devrait-il entreprendre pour aider l'organisation à atteindre ses objectifs stratégiques ?
- Qu'est-ce que le processus apporte à l'organisation et dont l'absence compromettrait le succès de cette dernière ?
- À la fin de la journée, de la semaine, du mois ou de l'année, qu'est-ce qui donne aux collaborateurs un sentiment d'accomplissement dans leur travail ?
- Quelles sont les réalisations qui valent aux collaborateurs la reconnaissance du management ou des clients internes ?

Copyright © 2015 Eyrolles.

Dès lors qu'il comprend bien les objectifs du processus, l'auditeur interne est prêt à rassembler des informations sur le mode opératoire du processus.

Compilation des informations

Il existe de multiples façons de rassembler des informations sur un processus. L'auditeur interne doit étudier les différentes catégories et sources d'informations pertinentes et aisément disponibles. De plus, l'analyse des données et les contrôles à l'échelle de l'entité lui permettront de se faire une idée plus précise d'un processus.

Catégories et sources d'informations pertinentes

Pour comprendre un processus, il convient de commencer par étudier la documentation qui existe déjà. Par exemple, on peut se procurer les documents énumérés ci-dessous auprès des propriétaires des processus ou d'autres personnes qui le connaissent bien. Ces documents peuvent en effet contenir des informations utiles sur le fonctionnement du processus.

- La politique relative au processus.
- Les manuels de procédures.
- Les organigrammes ou informations analogues précisant le nombre de collaborateurs et les principales relations hiérarchiques.
- Le descriptif des postes des personnes prenant part au processus.
- Des cartographies des processus ou des diagrammes décrivant les flux généraux du processus.
- Des descriptions narratives des principales tâches ou parties du processus.
- Des copies des principaux contrats avec les clients, fournisseurs, prestataires extérieurs, etc.
- Des informations pertinentes concernant les lois et règlements applicables au processus.
- D'autres documents qui ont été élaborés pour faciliter le reporting sur l'efficacité du système de contrôle interne.

Ces informations peuvent apporter à l'auditeur interne une grande partie des éléments dont il a besoin pour comprendre le processus. Cependant, il reste souvent nécessaire de discuter de certains aspects avec les personnes qui participent directement au processus. Si la documentation disponible n'est pas suffisamment

Copyright © 2015 Eyrolles.

détaillée, l'auditeur doit leur poser de nombreuses questions, par exemple :

- Quelles sont les principales tâches que vous êtes chargé d'exécuter ?
- De quels éléments (information, documentation, etc.) avez-vous besoin pour exécuter ces tâches ?
- Que faites-vous précisément avec ces éléments ?
- Quelles sont les données de sortie de chacune de vos tâches ?
- De quelles autres personnes ou de quels autres services dépendez-vous pour exécuter ces tâches ?
- Quelles autres personnes ou quels autres services ont besoin que vous exécutiez ces tâches efficacement et en temps opportun ?
- Quels systèmes d'information utilisez-vous pour exécuter ces tâches ?
- Combien de temps vous faut-il pour mener à bien chaque tâche ?
- Quels types d'anomalies ou d'erreurs rencontrez-vous habituellement ?
- Comment traitez-vous ces anomalies ou ces erreurs ?
- Quels autres obstacles ou difficultés rencontrez-vous habituellement lorsque vous exécutez ces tâches ?
- Que faites-vous pour surmonter ces obstacles ou ces difficultés ?
- Comment faites-vous *in fine* pour vous assurer que vous exécutez les tâches correctement ?

Rassembler des informations concernant :

– les données d'entrée ;
– le traitement ;
– les données de sortie.

Ces questions, ainsi que d'autres, peuvent apporter à l'auditeur interne l'information dont il a besoin pour bien comprendre le processus. Il peut recueillir ces informations au moyen d'entretiens individuels, ou en procédant à un test de cheminement, ce qui suppose de suivre une transaction à chaque étape du processus. Indépendamment de l'approche retenue, il importe de comprendre les principales tâches de manière suffisamment détaillée, car cette compréhension structure les étapes ultérieures de la planification.

Procédures analytiques

Procédures analytiques

Examen et évaluation des informations existantes, financières ou extrafinancières, afin de déterminer si elles correspondent aux résultats attendus.

Comme indiqué ci-dessus, la compréhension des tâches intervenant dans un processus constitue une étape importante dans la planification de la mission. Cependant, ces tâches décrivent la manière dont le processus doit fonctionner, mais ne donnent guère d'indication sur l'efficacité de leur exécution. Les procédures analytiques sont l'un des moyens par lesquels l'auditeur interne peut procéder à des évaluations de haut niveau qui peuvent mettre en évidence les activités méritant une attention plus soutenue et, le cas échéant, des tests plus détaillés.

Copyright © 2015 Eyrolles.

Les procédures analytiques supposent d'examiner et d'évaluer les informations existantes, financières ou extrafinancières, afin de déterminer si elles correspondent aux résultats attendus.

Exemple Books 2 Buy. Pour l'audit des décaissements, cette analyse peut inclure tout ou partie des éléments suivants :

- des comparaisons des informations financières concernant des périodes antérieures, par exemple l'évolution des soldes des comptes fournisseurs d'un trimestre à l'autre ;
- des analyses de ratios, par exemple le ratio de liquidité générale (l'actif à court terme sur le passif à court terme) et la rotation des comptes fournisseurs (coût de la marchandise vendue sur les comptes fournisseurs) ;
- des comparaisons des informations financières et extrafinancières avec les informations budgétées. Par exemple, on pourra comparer le solde de trésorerie effectif par rapport au solde de trésorerie prévisionnel.

Analyse des données à l'aide des techniques d'audit informatisées

L'analyse des données suppose de compiler et d'analyser de gros volumes de données, habituellement en recourant à la technologie. Cette technique est décrite plus en détail au chapitre 10, *Les preuves d'audit et les papiers de travail*. Si la majeure partie de l'analyse des données sert à tester l'efficacité d'un processus, certains tests peuvent apporter des informations utiles pendant la planification, par exemple des informations sur la population des transactions, ce qui facilitera le choix de la méthode d'audit interne.

Exemple Books 2 Buy. Lors d'un audit du processus de décaissement, l'équipe d'audit interne peut, pendant la phase de planification, effectuer les tests d'analyse sur les données suivantes :

- le nombre ou le pourcentage des paiements qui sont effectués bien avant ou après la date d'échéance, ce qui donne une idée du soin apporté à la gestion des flux de trésorerie ;
- le nombre des chèques établis manuellement, qui donne une idée des déficiences dans la conception des processus ou des possibilités de contourner les contrôles en place ;
- la stratification des comptes fournisseurs, qui donne une idée de la proportion des paiements de petit montant, ce qui indique la possibilité de mettre en place des forfaits ou industrialiser le processus ;
- la distribution des premiers chiffres des montants payés (analyse selon la loi de Benford) : une distribution ne suivant pas la loi de Benford peut indiquer des pratiques de

Techniques d'audit informatisées

Techniques d'audit assistées par ordinateur, comme les logiciels d'audit généralisés, les logiciels utilitaires, les données de test, les outils de traçage logique et de cartographie de logiciels d'application, et les systèmes experts d'audit, qui aident l'auditeur interne à tester directement les contrôles intégrés dans les systèmes d'information informatisés et les données contenues dans les fichiers informatiques.

Copyright © 2015 Eyrolles.

décaissement inhabituelles (par exemple, un processus de facturation décentralisé), ce qui peut influer sur le choix de la méthode d'audit interne. La loi de Benford estime le nombre de fois que chacun des 10 chiffres (zéro à neuf) apparaîtra au début des nombres dans une population présentant certaines caractéristiques ;

- la présence de deux paiements du même montant pour le même fournisseur, qui peut indiquer la possibilité qu'une facture a été réglée deux fois ou permettre de savoir qui sont les fournisseurs qui reçoivent de manière récurrente des paiements pour des montants analogues.

Toute information complémentaire que l'auditeur interne pourra recevoir sur une population, pendant la planification, permettra de concevoir des tests d'audit d'une plus grande efficacité.

Contrôle à l'échelle de l'entité

Contrôle au niveau de toute une entité et qui, par conséquent, n'est ni lié ni associé à un processus en particulier.

Analyse des contrôles à l'échelle de l'entité

S'il importe de comprendre les tâches et les contrôles au niveau du processus, il convient également de comprendre comment les contrôles à l'échelle de l'entité peuvent influer sur l'exécution du processus. Des déficiences dans les contrôles à l'échelle de l'entité peuvent perturber la fiabilité des contrôles au niveau du processus. Par exemple, si, à l'échelle de l'organisation, la politique a tendance à être informelle et appliquée sans cohérence, alors les politiques spécifiques au processus audité ne seront pas aussi importantes pour la compréhension du processus. De même, si l'organisation ne s'emploie pas à attirer, former et perfectionner des collaborateurs compétents dans des domaines essentiels nécessitant des capacités de décision ou de jugement poussées, il faudra peut-être modifier la méthode de test, car on ne pourra guère compter sur la capacité des collaborateurs à exécuter des tâches complexes ou faisant intervenir un degré de discernement élevé.

Habituellement, on évalue périodiquement les contrôles à l'échelle de l'entité dans toute l'organisation (par exemple chaque année). Il n'est donc normalement pas nécessaire d'évaluer l'efficacité des contrôles à l'échelle de l'entité lors de chaque mission. Cependant, comme l'indique le paragraphe précédent, l'auditeur interne doit tenir compte des résultats de cette évaluation lorsqu'il planifie ses missions afin de choisir la méthode de test la plus pertinente et efficiente.

Documentation des flux de processus

Comme nous l'avons vu ci-dessus, il est possible de collecter plusieurs sortes d'informations auprès de sources très diverses. Pour montrer qu'il comprend comment le processus fonctionne, l'auditeur interne doit élaborer une documentation sur les principales

Copyright © 2015 Eyrolles.

étapes. Cette documentation des flux du processus facilite l'examen des papiers de travail par le superviseur de l'auditeur interne, notamment. Les méthodes les plus courantes pour la documentation des flux de processus sont les diagrammes de flux (de niveau général ou détaillé) et les notes narratives. Avant de décrire brièvement ces méthodes, il est important de comprendre les différences subtiles qui existent entre ces modes de documentation des flux de processus.

- **Les cartographies des processus**, telles que décrites dans le chapitre 5, *Les processus et les risques*, visent à décrire globalement les données d'entrée, les activités, les flux de travail et les interactions avec d'autres processus et données de sortie. Elles offrent un cadre de référence pour comprendre les activités et les sous-processus.
- **Les diagrammes de flux** comportent des informations complémentaires, décrivant fréquemment les systèmes et applications informatiques, les flux de documents, le détail des risques et des contrôles, les étapes manuelles et les étapes automatisées, la durée des différentes étapes du processus, les propriétaires des principales étapes, ainsi que toute autre information susceptible d'aider l'évaluateur à comprendre le processus et son flux.
- **Les notes narratives** donnent des informations concernant le flux de processus, uniquement au moyen de mots : elles n'essaient pas d'employer des symboles pour décrire les flux. Il est habituel de combiner les diagrammes de flux à des informations supplémentaires sous forme narrative afin de créer un format de documentation hybride.

Cartographie des processus

Schéma décrivant globalement les données d'entrée, les activités, les flux de travail et les interactions avec d'autres processus et données de sortie.

Les cartographies des processus ont tendance à être plus utiles au niveau des activités, comme le montre le chapitre 5, tandis que les diagrammes de flux et la documentation hybride fournissent le niveau d'information nécessaire pour comprendre les processus détaillés. Une brève description de ces techniques habituellement utilisées au niveau des processus est exposée ci-après.

Diagramme de flux

Graphique complémentaire de la cartographie des processus, qui inclut les systèmes et applications informatiques, les flux de documents, le détail des risques et des contrôles, les étapes manuelles et les étapes automatisées, la durée, ainsi que les propriétaires des principales étapes.

Diagramme de flux macro

Un diagramme de flux macro vise à décrire globalement les données d'entrée, les activités, les flux de travail et les données de sortie. Il permet de comprendre l'ensemble des activités, des systèmes, des rapports et des interfaces avec les autres processus ou sous-processus. Cette compréhension forme une sorte de cadre de référence pour l'identification des principaux sous-processus et systèmes qu'il convient d'envisager d'intégrer dans le périmètre de la mission. Les diagrammes de flux se présentent habituellement comme une cartographie des processus, mais contiennent des informations supplémentaires, si elles sont nécessaires à la compréhension des flux du processus. Les symboles les plus fréquents dans

Copyright © 2015 Eyrolles.

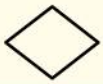
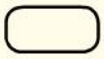
ces diagrammes sont présentés à l'encadré 13-5. Ils s'appuient sur ceux utilisés pour les cartographies des processus, comme indiqué au chapitre 5.

Exemple Books 2 Buy. L'encadré 13-6 présente un diagramme de flux macro décrivant le processus de décaissement.

L'auditeur interne peut utiliser un simple diagramme de flux macro pour confirmer, avec le propriétaire du processus, qu'il cerne bien l'ensemble du processus. Il lui est ainsi plus facile de déterminer quels domaines ou sous-processus entrent dans le périmètre de la mission. Ce schéma synthétise les diagrammes de flux détaillés.

ENCADRÉ 13-5

SYMBOLES COURANTS DANS LES DIAGRAMMES DE FLUX

	**Processus ou opération** – Processus, sous-processus ou activité.
	**Décision** – Indique une alternative (par exemple, oui/non ou accepter/rejeter), chaque choix engendrant différents flux d'activités et/ou de documents.
	**Document** – Sortie papier d'un document source ou d'un rapport.
	**Ligne de liaison** – Sens dans lequel vont les activités, les flux de travail, les flux d'information, les documents et les transferts.
	**Système ou application informatique** – Technologie informatique servant à stocker des données, faire tourner une application ou effectuer d'autres fonctions informatisées.
	**Renvoi sur la page** – Sert à relier différentes parties d'un diagramme sur la même page sans utiliser de lignes de liaison.
	**Renvoi hors page** – Sert à relier des parties d'un diagramme présenté sur différentes pages.
	**Terminateur** – Marque de début ou de fin d'un flux.
	**Annotation** – Note explicative en un point spécifique d'un diagramme.

Diagrammes de flux détaillés

Si un diagramme de flux macro peut constituer un point de départ important, il n'apporte toutefois ni la profondeur ni le niveau de détail suffisant pour faciliter le jugement de l'auditeur interne concernant la conception du processus. Un diagramme de flux détaillé consigne des entrées, tâches, actions, systèmes, documents

Copyright © 2015 Eyrolles.

et sorties plus spécifiques. Les diagrammes détaillés donnent une description plus pointue des flux du processus, mais aussi des informations supplémentaires qui permettent de mieux comprendre le processus. Ils peuvent par exemple inclure certains ou tous les éléments suivants.

- Les principaux risques, qui peuvent être figurés par un symbole identifiant les points du processus qui pourraient subir un dysfonctionnement et empêcher le processus de fonctionner comme prévu.
- Les contrôles clés, qui peuvent être figurés par un symbole identifiant les tâches, les actions ou les décisions qui sont considérées comme critiques pour la conception adéquate du processus.
- Les personnes ou les postes exécutant des tâches principales ou prenant les décisions principales.
- La période où les tâches, actions ou décisions principales interviennent.
- Le temps qu'il faut pour exécuter une tâche ou prendre une décision (qui peut être indiqué sur le diagramme de flux si cette information sert à évaluer l'efficience du processus).

  Exemple Books 2 Buy. L'encadré 13-7 présente un diagramme de flux détaillé. Cet exemple décrit le sous-processus du traitement des factures dans le processus de décaissement chez Books 2 Buy. Le sous-processus du traitement des factures est présenté dans le diagramme de flux macro illustré dans l'encadré 13-6.

Les diagrammes de flux détaillés constituent un moyen efficace de présenter un volume important d'informations sous un format intuitif et compréhensible. Le niveau d'information qui y figure doit être suffisant pour faciliter le jugement de l'auditeur interne concernant l'identification des contrôles clés, l'adéquation du processus dans son ensemble et les écarts entre le niveau effectif et le niveau souhaité pour des contrôles spécifiques.

Notes narratives

Justification d'une note narrative

– Processus simple.
– Tâches compliquées.
– Demande expresse du propriétaire du processus.
– Plus grande efficience.

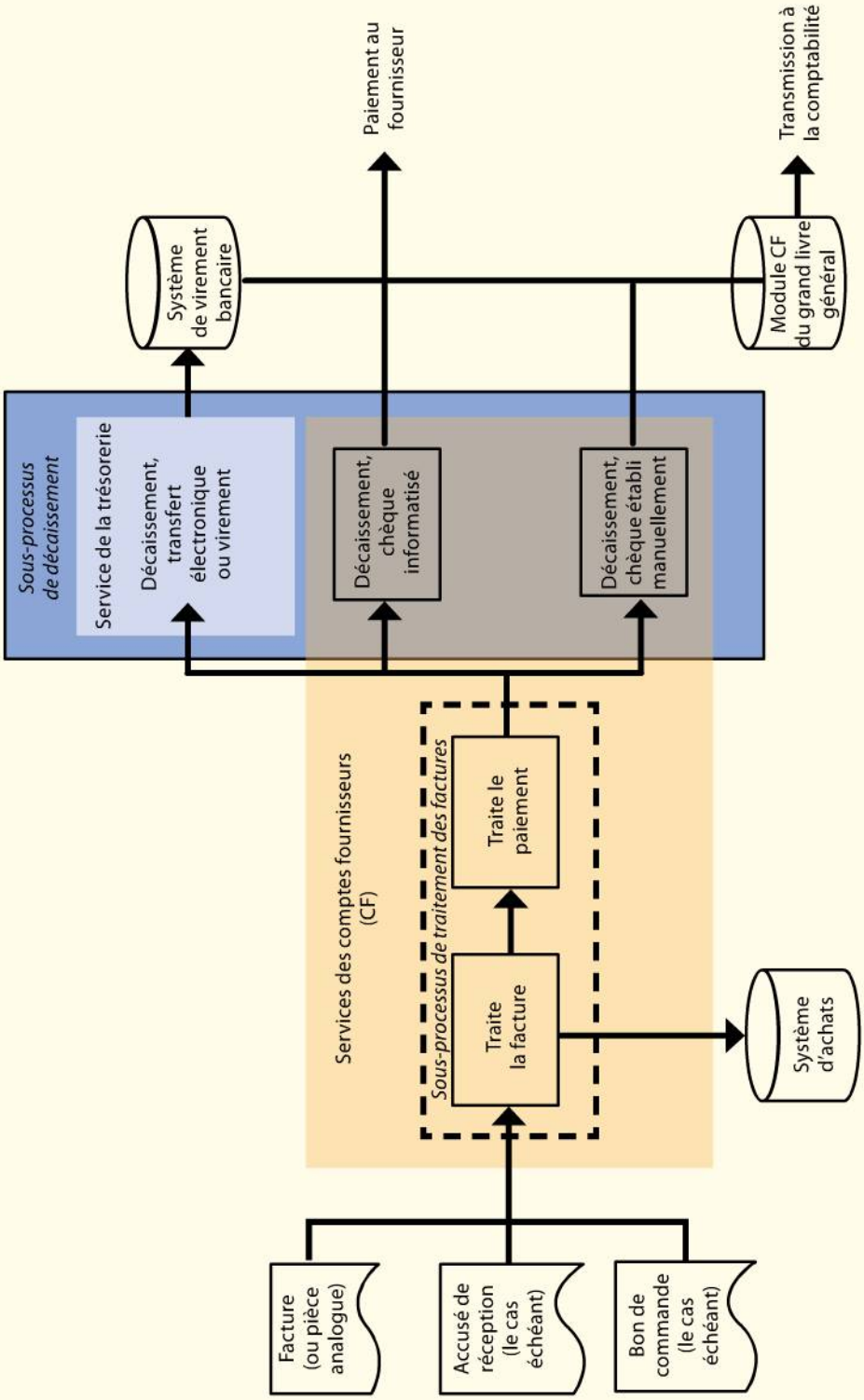
Dans certaines situations, l'auditeur interne peut estimer qu'il est plus approprié de documenter sa compréhension du processus par des notes narratives, et non par des diagrammes de flux. Ce type de situations présente habituellement une ou plusieurs des caractéristiques suivantes :

- le processus est simple et la représentation au moyen d'un diagramme n'apporte pas grand-chose de plus ;
- les étapes sont compliquées, si bien qu'il est difficile de les décrire efficacement dans l'espace limité qu'offre une icône sur un diagramme ;

Copyright © 2015 Eyrolles.

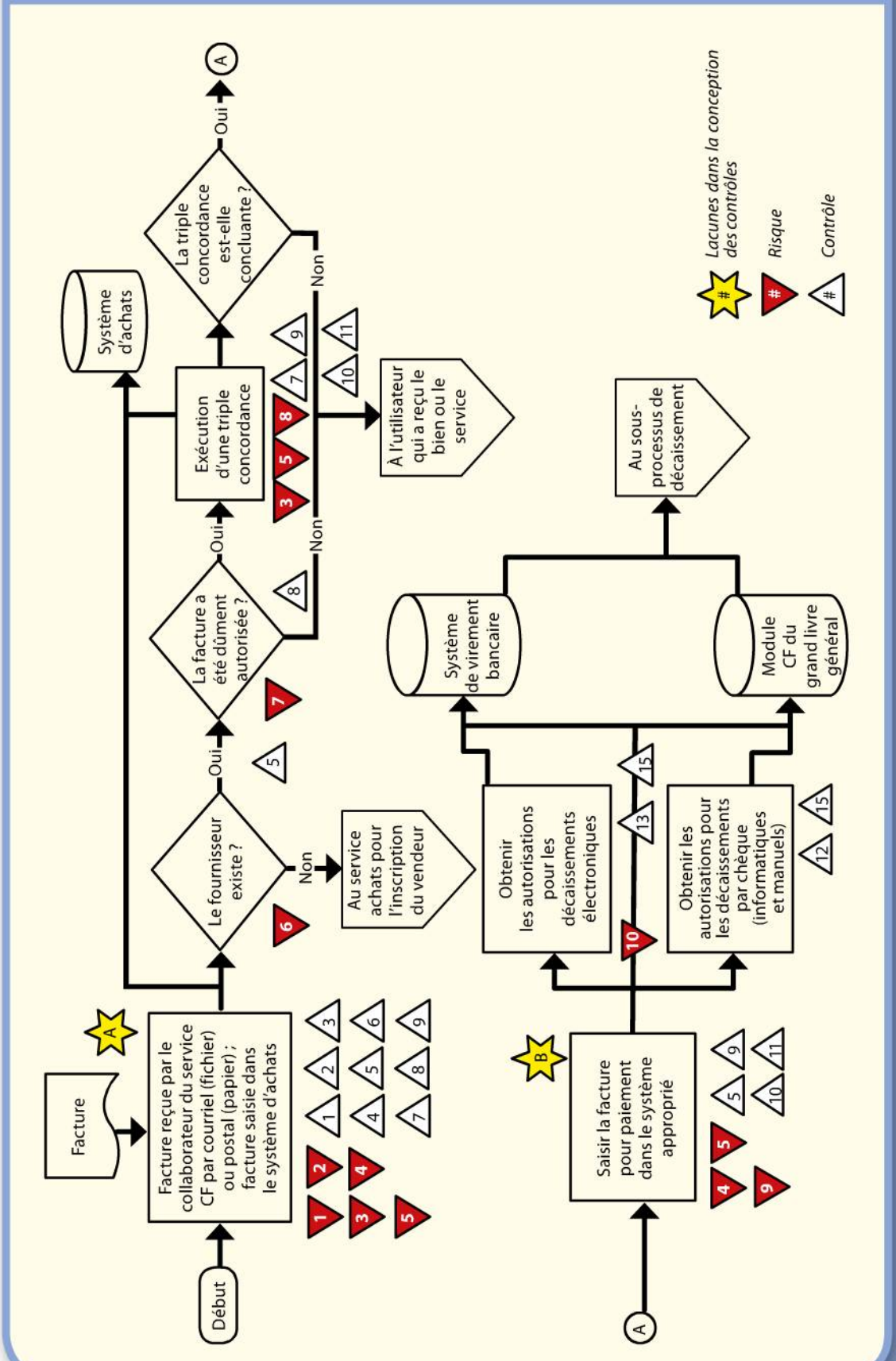
ENCADRÉ 13-6

DIAGRAMME DE FLUX MACRO DU PROCESSUS DE DÉCAISSEMENT



Copyright © 2015 Eyrolles.

DIAGRAMME DÉTAILLÉ
SOUS-PROCESSUS DE TRAITEMENT DES FACTURES



Copyright © 2015 Eyrolles.

ENCADRÉ 13-7
suite

DIAGRAMME DÉTAILLÉ, *SUITE*
RISQUES ET CONTRÔLES ASSOCIÉS AU TRAITEMENT DES FACTURES

1. La facture n'est pas reçue en temps opportun par le service CF, et les états financiers ne tiennent pas correctement compte de cet engagement.
2. La facture n'est pas traitée en temps opportun par le service CF, ce qui fait que l'organisation passe à côté de remises, voire doit supporter des pénalités de retard.
3. L'information concernant la facture n'est pas saisie correctement dans le système d'achats, ce qui se traduit par des paiements erronés ou indus.
4. Des factures sont saisies deux fois et traitées deux fois en vue du paiement, si bien que la même facture est payée deux fois.
5. Les collaborateurs du service CF disposent indûment de l'accès aux différents systèmes, ce qui leur permet de saisir des fournisseurs fictifs, de créer de faux bons de commande ou de procéder à des paiements non autorisés.
6. Le traitement attribue les paiements au mauvais fournisseur ou à un fournisseur inexistant : par conséquent, les paiements au bon fournisseur prennent du retard, l'organisation doit se faire rembourser les montants versés indûment au mauvais fournisseur ou des paiements frauduleux sont effectués.
7. Des paiements sont traités pour des factures qui n'ont pas encore été autorisées, si bien que le paiement intervient avant la réception de la marchandise ou du service.
8. Le traitement porte sur des factures qui ne correspondent pas aux bons de commande, aux bordereaux de réception ou aux autres pièces pertinentes, si bien que l'on saisit un engagement dans le système et que l'on paie un montant incorrect.
9. Des paiements sont effectués avant la date d'échéance, ce qui se traduit par une gestion inefficace de la trésorerie.
10. Des paiements sont effectués sans autorisation, ce qui se traduit par l'adoption d'une méthode de paiement coûteuse ou inefficace, ou qui ne répond pas aux impératifs de flux de trésorerie de l'organisation.

△1 Dans le cadre du processus de clôture de fin de mois, le manager du service CF sollicite des informations concernant des factures non traitées et prévoit d'établir le compte de charges à payer en conséquence.

△2 Une fois que la facture validée est saisie, le système comptabilise automatiquement le crédit dans le CF et le débit dans le compte de charges ou de bilan approprié.

△3 Les bons de commande permanents sont examinés une fois par mois par le manager du service des achats, qui cherche à en déterminer le statut.

△4 Le collaborateur du service CF sort un rapport à la fin de chaque semaine afin de faire apparaître les factures qui sont saisies mais qui ne sont pas validées. Pour les factures en cours depuis plus d'une semaine, un rappel est envoyé à l'utilisateur.

△5 Le système d'achats requiert que tous les champs de factures soient complétés avant d'autoriser le traitement. Une facture ne peut pas être saisie avant un rapprochement avec un fournisseur agréé.

△6 Le système d'achats alerte le collaborateur du service CF si la référence du fournisseur, le numéro de facture et le montant de la facture correspondent à une facture déjà saisie.

△7 Le système d'achats confirme une correspondance entre les quantités et les prix figurant sur une facture, le bon de commande et les bordereaux de réception. En l'absence de correspondance, la facture est mise en attente.

Copyright © 2015 Eyrolles.

8 Les seuils/plafonds d'autorisation des factures sont confirmés avec les chefs de service chaque année et actualisés si nécessaire.

9 Un nom d'utilisateur et un mot de passe sont nécessaires pour l'accès à tous les systèmes. Le choix des mots de passe est soumis à des règles et ces mots de passe doivent être changés tous les 90 jours.

10 Les droits d'accès aux systèmes sont examinés deux fois par an avec les chefs de service afin que les capacités d'accès correspondent aux responsabilités de chacun.

11 Les collaborateurs du service CF ne peuvent pas accéder au fichier maître des fournisseurs, ni apporter des changements aux informations relatives aux bons de commande et aux bordereaux de réception qui sont déjà saisis.

12 Seul le manager du service CF peut lancer le traitement d'un lot de chèques informatisés.

13 Seuls les collaborateurs du service de la trésorerie sont en droit de traiter les virements bancaires.

14 Le système d'achats fait l'interface avec le module CF du grand livre général et le système de virement bancaire.

15 Les chèques informatisés de plus de 50 000 requièrent la signature manuelle du trésorier.
Les chèques informatisés de plus de 100 000 requièrent la signature manuelle du directeur financier.
Les chèques manuels doivent être signés par le trésorier et le directeur financier. Le trésorier doit autoriser les virements bancaires de plus de 100 000.

A Il n'y a pas de vérification auprès des utilisateurs pour déterminer si des produits ou des services ont été reçus mais n'ont pas encore été facturés (observation de mission portée dans le papier de travail Z-1).

B Si le système d'achat alerte le collaborateur du service CF d'un risque de doublon de facture, il n'empêche pas ce collaborateur de continuer de traiter la facture en question (observation de mission portée dans le papier de travail Z-2).

- le propriétaire du processus souhaite que le résultat vienne alimenter la documentation relative à d'autres processus et préfère des notes narratives à des diagrammes de flux ;
- les notes narratives constituent une méthode plus efficiente de documenter le processus.

Elles doivent contenir les mêmes catégories d'informations que celles présentes sur les diagrammes de flux. Si les sections spécifiques de ces notes peuvent varier suivant le processus, une note doit normalement contenir les éléments énumérés ci-après.

1. Description générale du processus.
2. Principales données d'entrée :
   a. documents ou communications provenant de sources extérieures (par exemple factures ou chèques) ;
   b. données de sortie des autres processus ou sous-processus ;
   c. informations provenant de sources extérieures ;
   d. données provenant des systèmes internes.

Copyright © 2015 Eyrolles.

3. Principales étapes du processus :
   a. Les activités qui permettent de manier, vérifier, changer ou piloter les entrées ;
   b. Les analyses qui sont effectuées ;
   c. Les décisions qui sont prises ou jugements qui sont formulés ;
   d. Les applications informatiques qui sont actualisées ;
   e. Les nouveaux documents ou informations qui sont créés ;
   f. Les principales personnes qui exécutent les tâches ;
   g. Le temps écoulé pour des tâches ou des ensembles de tâches.
4. Principaux éléments sortants :
   a. les documents à envoyer à des parties extérieures (par exemple factures, chèques ou relevés) ;
   b. les rapports à usage interne ;
   c. les entrées dans les autres processus ou sous-processus ;
   d. les données à stocker électroniquement ;
   e. les copies papier de la documentation à stocker en interne.
5. Risques qui menacent le processus.
6. Contrôles clés (voir ci-dessous la section de ce chapitre consacrée à l'identification des contrôles clés).

Que l'auditeur utilise des diagrammes de flux, des notes narratives ou une combinaison des deux, la documentation des flux de processus lui permet de mieux comprendre les éléments qui seront critiques lors des étapes suivantes de la planification de la mission. Il doit donc consacrer suffisamment de temps à cette compréhension pour pouvoir évaluer l'adéquation de la conception du processus.

Il importe de se souvenir que, dans une mission d'assurance, les diagrammes de flux et les notes narratives servent à dépeindre la situation telle qu'elle est, et non telle qu'elle devrait être ou qu'on voudrait qu'elle soit. Les audits ont pour objectif commun d'évaluer l'adéquation de la conception et le fonctionnement effectif d'un processus. La documentation de la situation telle qu'elle est aide l'auditeur interne à évaluer la qualité de la conception actuelle du processus. L'audité n'obtient la situation souhaitée qu'une fois qu'il a remédié aux éventuelles déficiences identifiées par l'auditeur interne.

Identifier les indicateurs clés de performance

Après avoir bien compris les flux du processus, l'auditeur interne doit aussi comprendre comment le management pilote les performances au niveau du processus. Il n'est pas rare que des indicateurs clés de performance (ou KPI, pour *Key Performance Indicator*) soient vérifiés périodiquement afin de donner aux propriétaires du processus des informations sur le fonctionnement du processus.

Copyright © 2015 Eyrolles.

L'observation de ces indicateurs clés de performance peut être semblable aux procédures analytiques déployées par l'auditeur interne et décrites dans la section précédente, voire très différente. Les bons indicateurs clés de performance doivent réunir plusieurs caractéristiques. Ils doivent être :

- **pertinents,** c'est-à-dire qu'ils mesurent ce qui est important (par exemple l'exactitude des décaissements), et non ce qui est quantifiable (par exemple le montant des décaissements traités) ;
- **mesurables,** c'est-à-dire qu'il existe des informations quantifiables permettant de déterminer le bon fonctionnement du processus (par exemple, des informations inexactes sur les décaissements sont suivies et compilées pour vérifier l'exactitude des décaissements) ;
- **disponibles,** c'est-à-dire que les informations nécessaires sont disponibles au bon moment et pour les bonnes personnes, ce qui permet de mesurer rapidement les performances du processus (par exemple, les statistiques sur les décaissements sont disponibles pour le manager du service des comptes fournisseurs à la clôture de chaque cycle de paiement) ;
- **alignés** sur les principaux objectifs du processus (par exemple, l'information sur les doublons de paiement est retenue parce que l'objectif est d'éviter tous les doublons) ;
- **expliqués** aux personnes qui prennent part au processus, afin qu'elles comprennent ce qu'on mesure et l'importance d'atteindre les niveaux de performance requis (par exemple, les collaborateurs du service des comptes fournisseurs peuvent rapidement prendre connaissance des statistiques et corriger leurs performances en conséquence).

Indicateur clé de performance

Donnée chiffrée ou toute autre forme de mesure permettant de déterminer si un processus ou une tâche donnés respectent les seuils de tolérance fixés.

Qu'ils soient formels ou informels, les indicateurs clés de performance peuvent définir la tolérance du propriétaire du processus concernant les écarts par rapport aux performances requises. Le management détermine le niveau d'erreur qu'il est prêt à accepter lorsque le processus ne fonctionne pas comme prévu. S'il connaît ces seuils de tolérance, l'auditeur interne peut évaluer plus facilement les résultats des tests d'audit. Ainsi, si l'auditeur interne trouve un taux d'erreur de deux pour cent dans un test et connaît le niveau d'erreur acceptable, il pourra déterminer si ce taux d'erreur est significatif.

Exemple Books 2 Buy. Voici des exemples d'indicateurs clés de performance pour le processus de décaissement :

- 100 % des décaissements sont exacts (par exemple, le montant versé correspond à celui figurant sur la facture) ;
- 98 % des décaissements sont payés à la date d'échéance. En aucun cas, l'organisation ne doit avoir à payer d'intérêts ou de pénalités de retard ;

Copyright © 2015 Eyrolles.

- il n'y a pas de paiements en double ;
- 90 % des créances fournisseurs assorties d'une remise de 1 % en cas de paiement rapide sont payées suffisamment tôt pour donner droit à la remise.

Fraude

Tout acte illégal caractérisé par la tromperie, la dissimulation ou la violation de la confiance sans qu'il y ait eu violence ou menace de violence. Les fraudes sont perpétrées par des personnes et des organisations afin d'obtenir de l'argent, des biens ou des services, ou de s'assurer un avantage personnel ou commercial.

Évaluation des risques de fraude au niveau des processus

Enfin, il est important de comprendre les risques de fraude potentiels au niveau des processus. Comme l'indique la section suivante, la plupart des risques reposent sur l'incertitude d'événements susceptibles de survenir en raison de la nature inhérente du processus. La probabilité inhérente que certains risques se concrétisent augmente si une personne a l'intention de commettre une fraude et/ou si plusieurs personnes ont l'intention de participer au processus. Avant de commencer le processus formel d'évaluation des risques lors d'une mission, il importe donc d'évaluer les scénarios de fraude potentiels dans le processus. Cette démarche comporte les trois étapes suivantes.

1. **Identifier les scénarios de fraude potentiels.** Organiser des séances de réflexion collective avec les personnes participant au processus est une méthode efficace pour déterminer les moyens par lesquels des personnes, opérant seules ou en collusion avec d'autres, pourraient contourner le processus.

   Exemple Books 2 Buy. Exemples de fraudes potentielles sur les décaissements :

   - un collaborateur crée un fournisseur fictif avec sa propre adresse, soumet pour traitement une facture libellée au nom de ce fournisseur et envoie le paiement sur son propre compte ;
   - un collaborateur du service des comptes fournisseurs traite un paiement deux fois et, en collusion avec le fournisseur, s'arrange pour partager le produit du deuxième paiement avec une personne travaillant chez le fournisseur en question ;
   - un collaborateur de la trésorerie ouvre un compte bancaire à un nom analogue à celui d'un fournisseur certifié et réalise des transferts de fonds vers ce compte.

2. **Comprendre l'impact potentiel de la fraude.** Il convient de déterminer quel pourrait être l'impact potentiel de chaque scénario de fraude. Par exemple, une organisation peut :

   - essuyer un préjudice financier direct (en raison d'un détournement d'actifs) ;
   - déclarer des états financiers ne reflétant pas la réalité (en raison d'un reporting financier frauduleux) ;
   - souffrir d'une atteinte à sa réputation si la fraude a un impact très négatif sur la gouvernance de l'organisation.

Copyright © 2015 Eyrolles.

3. **Déterminer s'il faut tester les risques de fraude spécifiques.** À partir des deux premières étapes, l'auditeur interne peut évaluer, en fonction du risque inhérent de fraude dans le processus, s'il doit élaborer des tests spécifiques afin de déterminer la vulnérabilité à la fraude.

Cette étape n'a pas pour objet systématique d'identifier l'occurrence d'une fraude, mais plutôt d'évaluer la possibilité qu'un scénario de fraude se produise. Si l'auditeur interne peut raisonnablement penser que ces scénarios vont se produire, il doit envisager d'élaborer des tests qui permettront d'identifier l'occurrence ou le potentiel pour les scénarios de fraude. Voir le chapitre 8, *Les risques de fraude et d'actes illégaux*, pour un examen détaillé de la fraude.

REPÉRER ET ÉVALUER LES RISQUES

Identifier les scénarios de risque au niveau des processus

Une organisation instaure des processus afin d'exécuter son plan d'activité (*business plan*) et de réaliser ses objectifs. Ces processus peuvent être des microprocessus et extrêmement ciblés, ou transversaux. Des risques sont associés à tous les processus, quels que soient leur ampleur, leur emplacement et leur cible. La première tâche de l'évaluation des risques au niveau des processus consiste à repérer les scénarios de risque qui sont inhérents aux processus. Les scénarios de risque sont des événements potentiels de la vie réelle qui peuvent entraver la réalisation des objectifs.

Risque

Possibilité qu'un événement survienne et ait un impact défavorable sur la réalisation des objectifs.

Les risques présentés à l'encadré 13-7 peuvent passer inaperçus tant que l'auditeur interne n'a pas achevé cette tâche de la planification. Il est fréquent que les activités « Comprendre l'audité » et « Repérer et évaluer les risques » soient menées à bien de manière itérative.

L'identification des scénarios de risques a pour objectif de répondre à la question suivante : que peut-il se passer qui risque d'empêcher la réalisation des objectifs au niveau du processus ? Pour répondre à cette question, les auditeurs internes doivent réfléchir collectivement aux scénarios de risque possibles. Voici comment ils peuvent procéder.

1. Choisir un seul objectif au niveau d'un processus. Cet exercice fonctionne mieux si l'on prend chaque objectif, l'un après l'autre.
2. Réfléchir collectivement aux obstacles (événements, problèmes, circonstances, etc.) susceptibles de menacer la réalisation de l'objectif. En voici quelques exemples :
   a. événements extérieurs auxquels l'organisation n'est pas préparée ou auxquels elle ne réagit pas assez rapidement ou de manière appropriée ;
   b. procédures conçues de manière inadéquate ou mal documentées ;

Copyright © 2015 Eyrolles.

c. dysfonctionnements dans les procédures existantes ;
d. absence de collaborateurs disposant des qualifications requises pour effectuer efficacement la mission ;
e. mauvaise communication entre des domaines qui sont interconnectés ;
f. comportement de collaborateurs qui violent intentionnellement les politiques ou agissent volontairement de manière contraire à la déontologie ;
g. applications informatiques conçues de manière inadéquate ou obsolètes ;
h. informations tardives inexactes ou inadéquates pour la prise de décision ;
i. absence de mesures des performances.

3. Poursuivre l'exercice sur les objectifs restants au niveau du processus.
4. Étant donné que certains scénarios de risque sont communs à tous les objectifs au niveau du processus, il convient de les classer et de combiner les scénarios analogues. La raison de ce regroupement apparaît de manière plus évidente lors de l'activité suivante, pendant laquelle les risques au niveau des processus sont définis.

Cet exercice de réflexion collective est optimisé si toutes les personnes prenant part au processus y sont associées. Elles peuvent être à même de repérer les scénarios de risque grâce à leur expérience. Cependant, les auditeurs internes chevronnés doivent être capables de conduire cet exercice sans l'aide des personnes participant au processus.

Pour que la séance de réflexion collective soit efficace, les auditeurs internes peuvent rédiger différents scénarios sur des notes adhésives puis les afficher sur un grand tableau. Une fois que cette étape de réflexion collective est terminée, les notes peuvent être (1) classées par objectif, ce qui permet de balayer complètement chaque objectif, et (2) classées par catégories de scénarios, ce qui facilite la définition des risques.

Exemple Books 2 Buy. Voici quelques-uns des scénarios de risque qui peuvent se produire dans un processus de décaissement :

- les factures ne sont pas traitées assez rapidement pour autoriser un paiement en temps voulu ;
- un paiement est effectué en double, car une facture a été saisie deux fois, une fois à partir d'une facture validée et la seconde à partir d'un relevé envoyé par le fournisseur ;
- un collaborateur du service des comptes fournisseurs saisit par erreur un montant erroné dans le système, si bien que le montant payé est incorrect ;

Copyright © 2015 Eyrolles.

- en raison de la rotation des collaborateurs au sein du service des comptes fournisseurs, des retards de saisie entraînent des retards de paiement ;
- des personnes non autorisées modifient les modalités de paiement dans le système, ce qui se traduit par des paiements en retard ou erronés.

Définir les risques au niveau du processus

Comme indiqué ci-dessus, l'identification des risques au niveau du processus se fonde sur des scénarios de risque analogues. Ces scénarios représentent des événements précis de la vie réelle susceptibles de compromettre la réalisation des objectifs. Les risques correspondent à la description large des causes et des effets de ces événements. L'activité suivante de l'évaluation des risques au niveau des processus consiste donc à définir les risques pertinents.

On peut définir les risques de bien des manières. L'approche optimale dépend de la culture et de « la façon dont on parle du risque » dans l'organisation. Cependant, indépendamment des méthodes retenues par chaque organisation, il importe de rester cohérent. En effet, un manque de cohérence pourrait compliquer la définition des risques dans toute l'organisation.

L'une des méthodes les plus fréquentes et les plus efficaces de définition des risques repose sur un protocole de type « cause et effet ». Avec cette approche, les risques commencent avec une « cause » (par exemple manquement à…, absence de…, incapacité à…) et continuent avec l'effet (par exemple, préjudice financier, blessure corporelle, corruption de données, atteinte à la réputation).

Exemple Books 2 Buy. Voici un échantillon des risques que peut présenter le processus de décaissement.

- **Attentes.** L'absence de politiques, procédures et autres formes de communication de la direction générale bien conçues et bien articulées peut conduire des collaborateurs à exercer leurs responsabilités à l'encontre des attentes et des souhaits de la direction générale.
- **Double paiement.** Lorsqu'on ne repère pas que des factures ont été saisies plusieurs fois, l'organisation risque de payer des fournisseurs plusieurs fois, sans que cela soit détecté, et risque d'avoir des difficultés à recouvrer les trop-payés.
- **Retard.** L'incapacité à traiter les paiements dans les délais peut entraîner des amendes ou des pénalités de retard ou empêcher l'organisation de bénéficier de remises.
- **Accès aux systèmes.** L'absence de pratiques efficaces visant la sécurité logique peut permettre à des personnes

Copyright © 2015 Eyrolles.

non autorisées d'accéder à des données importantes relatives aux décaissements, de les manipuler ou de les effacer.

- **Ressources humaines.** L'incapacité à embaucher, former, affecter au poste adéquat et retenir des collaborateurs compétents peut se traduire par un fonctionnement sous-optimal du processus de décaissement, avec à la clé des paiements erronés ou tardifs.

Une fois que les risques sont définis, il convient de les mettre en relation avec les objectifs au niveau du processus, afin de vérifier s'il y a corrélation entre chacun des risques et les objectifs. Comme nous le verrons plus loin dans ce document, l'évaluation des risques suppose de prendre en considération leur impact sur la capacité à atteindre les objectifs.

La dernière tâche consiste à confirmer que les définitions sont formulées dans « un langage compréhensible par les collaborateurs du processus concerné ». Puisque ces derniers sont chargés de gérer les risques au niveau du processus, il faut qu'ils aient une conception uniforme et cohérente de ces risques. Les auditeurs internes doivent donc expliquer les définitions des risques au management et aux collaborateurs intervenant au niveau des processus et en discuter avec eux afin de confirmer que la liste des risques est complète et que ces définitions ont du sens. Si cette tâche est menée avec succès, elle facilitera la suivante, qui consiste à évaluer l'impact et la probabilité d'occurrence des risques.

Évaluer l'impact et la probabilité d'occurrence des risques

Une fois que les risques sont repérés et définis, l'auditeur interne est prêt à les évaluer. Lors de cette activité, il s'attache à déterminer l'impact potentiel et la probabilité de chaque risque. Cette évaluation a pour objet de faciliter l'identification des principaux risques qui menace la réalisation des objectifs au niveau du processus. Ces risques requièrent une attention accrue de la part de l'auditeur lors d'une mission d'assurance.

L'évaluation des risques au niveau du processus se déroule généralement en trois temps :

1. La première étape consiste à déterminer l'impact des différentes conséquences associées à chaque risque. Les conseils suivants peuvent se révéler utiles à ce stade :
   - Il ne faut pas oublier que, par définition, le risque représente une incertitude, et que plusieurs conséquences sont donc possibles. L'auditeur interne doit donc essayer d'éviter de se focaliser sur une seule conséquence possible au risque d'ignorer celles dont la probabilité ou l'impact est plus fort.

Évaluation des risques

Identification et analyse (généralement en termes d'impact et de probabilité d'occurrence) des risques susceptibles d'affecter la réalisation des objectifs d'une organisation, de façon à déterminer comment ces risques doivent être gérés.

Impact

Gravité des conséquences d'un événement (risque). Se mesure en termes d'impacts financiers, juridiques, de réputation ou autres.

Copyright © 2015 Eyrolles.

- On mesure habituellement le risque au regard de son impact financier, le plus fréquent et le plus facile à quantifier. Cependant, le risque peut avoir d'autres conséquences qui ne se mesurent pas en termes financiers et qui peuvent se révéler plus graves que l'impact financier. Ainsi, les atteintes à la santé ou à la sécurité d'un collaborateur, ou à la réputation de l'organisation à la suite d'une mauvaise publicité, peuvent être considérées comme des conséquences plus graves que l'impact financier direct de ces risques.
- L'impact doit s'attacher à l'exposition potentielle sur une période donnée, généralement d'un an. Étant donné qu'un risque peut se présenter plusieurs fois sur la même période, il importe d'éviter de se concentrer sur l'impact d'une seule occurrence. Lorsqu'on estime l'impact sur une période donnée, on prend en compte l'exposition envisageable la plus extrême.
- Pour estimer l'impact d'un risque, il n'est pas nécessaire de parvenir à un degré élevé de précision. Une échelle générique (par exemple, élevé/intermédiaire/faible) suffit en général. Cependant, il demeure important de définir les niveaux de cette échelle. Par exemple, un impact élevé peut se définir comme un impact financier supérieur à 1 million, l'impact intermédiaire se situe entre 250 000 et 1 million et l'impact faible est inférieur à 250 000.

2. La deuxième étape consiste à estimer la probabilité que chacun de ces impacts se produise. Les astuces suivantes peuvent se révéler utiles à ce stade :
   - Comme indiqué plus haut, les risques peuvent avoir diverses conséquences, assorties de probabilités d'occurrence différentes. Il importe de s'attacher à la conséquence du risque déterminée lors de l'étape précédente.
   - De même que les risques peuvent avoir de nombreuses conséquences différentes, ils peuvent aussi être dus à de multiples causes. Toutes ces causes n'ont pas la même probabilité d'occurrence. Lorsqu'on évalue la probabilité d'occurrence d'un risque, il importe donc d'étudier la ou les cause(s) sous-jacente(s) de la conséquence choisie.
   - Comme pour la détermination de l'impact du risque, il n'est pas nécessaire d'obtenir un degré de précision élevé lorsqu'on estime la probabilité d'un risque. Une échelle générique (par exemple, élevé/intermédiaire/faible) suffit en général. Par exemple, une probabilité élevée peut indiquer que l'impact du risque a plus de 50 % de chances de se produire, une probabilité intermédiaire indique que l'impact est possible (et est compris par exemple entre 10 % et 50 %) et une probabilité faible peut indiquer que l'impact est peu probable (probabilité inférieure à 10 %, par exemple).

Probabilité

Possibilité qu'un événement (risque) survienne.

Copyright © 2015 Eyrolles.

- Lorsqu'on évalue la probabilité, il importe de s'attacher à la probabilité inhérente, c'est-à-dire sans considération des contrôles éventuellement mis en place par le management. Puisque l'auditeur interne maîtrise déjà le processus, il peut être tentant d'estimer la probabilité sur la base de l'effet de ces contrôles. Or, lorsqu'ils planifient la mission, les auditeurs internes ne doivent pas partir du principe que ces contrôles fonctionnent de manière effective, sous peine de sous-estimer les risques y afférents et de négliger de tester ces contrôles.

3. La dernière étape consiste à combiner l'évaluation de l'impact et de la probabilité à une évaluation unique du risque. Le meilleur moyen consiste à élaborer une matrice de risques qui présente les interrelations entre l'impact et la probabilité de chaque risque. Par exemple, la matrice de risques présentée à l'encadré 13-8 montre l'utilisation que l'on peut faire d'une échelle « élevé/intermédiaire/faible » pour l'évaluation aussi bien de l'impact que de la probabilité. Lorsque l'on examine cette matrice de risques, on remarque qu'un chiffre est inscrit dans chaque case pour indiquer le niveau global du risque. Chacun des risques est placé dans l'une des cases, qui correspondent aux catégories suivantes :
   - les cases 8 ou 9 (fond rouge) regroupent les risques considérés comme élevés ;
   - les cases 5, 6 ou 7 (fond jaune) regroupent les risques considérés comme intermédiaires ;
   - les cases 1, 2, 3 ou 4 (fond blanc) regroupent les risques considérés comme faibles.

Classiquement, les risques élevés et intermédiaires doivent être inclus dans toute mission d'audit interne. Les risques faibles peuvent y être inclus ou non, suivant la charte d'audit interne, les objectifs de la mission et les considérations de ressources. L'encadré 13-9 donne un exemple de matrice de risques du processus de décaissement qui peut être pertinente pour l'exemple **Books 2 Buy**.

ENCADRÉ 13-8

EXEMPLE DE MATRICE DE RISQUES

IMPACT				
	Élevé	7	8	9
	Intermédiaire	4	5	6
	Faible	1	2	3
		Faible	**Intermédiaire**	**Élevé**
		PROBABILITÉ		

Copyright © 2015 Eyrolles.

L'utilisation d'une matrice ou de tout autre mode de représentation graphique des résultats de l'évaluation des risques facilitera l'examen global des jugements formés par les responsables de l'audit interne et les propriétaires du processus lors de l'évaluation des risques. Ces examens, et particulièrement ceux menés par le propriétaire du processus, permettent de valider les jugements de l'auditeur interne.

Comprendre la tolérance au risque du management

Tolérance au risque

Niveau de risque et d'écart acceptable entre les objectifs et la performance réelle ; elle doit être en adéquation avec l'appétence pour le risque de l'organisation.

Appétence pour le risque

Niveau de risque global qu'une organisation est prête à accepter en vue de la réalisation de ses objectifs.

Traditionnellement, les jugements formulés par l'équipe d'audit interne constituent la seule source d'évaluation des risques. Cette situation reflète le rôle de l'auditeur interne dans la gouvernance de l'organisation. Cependant, le management des risques de l'entreprise repose sur le principe selon lequel le management doit définir un seuil de tolérance au risque opérationnel qui correspond à l'appétence de l'organisation pour le risque. Ce principe s'applique aussi au niveau des processus.

Il importe donc que l'auditeur interne valide le caractère raisonnable des seuils d'impact élevés, intermédiaires et faibles qui ont été utilisés. Il est possible que le management ait un seuil de tolérance au risque différent pour le processus en question. Rappelons, comme nous l'avons vu dans le chapitre 4, *La gestion des risques*, que l'appétence pour le risque désigne le niveau de risque global qu'une organisation est prête à accepter, alors que la tolérance au risque désigne le niveau de risque et d'écart acceptable entre les objectifs et la performance réelle. La tolérance au risque doit être en adéquation avec l'appétence pour le risque de l'organisation. Pour cerner les seuils de tolérance du management, il convient de suivre les trois étapes suivantes.

1. **Identifier les conséquences possibles des risques.** Comme nous l'avons déjà précisé, un risque est, par définition, associé à tout un éventail de conséquences possibles. Si ces conséquences sont souvent mesurées en termes financiers, certaines ne se prêtent pas à un tel mode d'évaluation ou sont plus graves que le seul impact financier. Ainsi, une atteinte à la sécurité des collaborateurs sera plus grave que les amendes ou les pénalités infligées en cas de violation de la réglementation sur la sécurité. De même, l'incapacité à protéger des renseignements confidentiels sur les clients peut avoir un impact plus grave que le coût supporté pour la récupération ou pour la protection de ces données.
2. **Comprendre les seuils de tolérance établis.** Une fois que les différentes conséquences du risque sont déterminées, l'auditeur interne peut engager des discussions avec les responsables du processus afin de se renseigner sur les seuils de tolérance déjà arrêtés. Ces niveaux peuvent transparaître dans la documentation des indicateurs clés de performance, des objectifs de performance individuels ou dans toute autre communication.

Copyright © 2015 Eyrolles.

3. **Évaluer les seuils de tolérance qui n'ont pas été établis.** Si les seuils de tolérance établis ne couvrent pas toutes les conséquences possibles des risques, l'auditeur doit en discuter avec les responsables du processus afin de définir des seuils de tolérance appropriés. Voici quelques questions à poser pour faciliter cette discussion :
   - Quel degré de variabilité vous-même ou la direction générale pouvez-vous tolérer concernant la réalisation des objectifs du processus ?
   - Quels types de conséquences considéreriez-vous comme inacceptables ?
   - Quels exemples ou scénarios de risque préféreriez-vous éviter d'avoir à traiter ?

ENCADRÉ 13-9

EXEMPLE DE MATRICE DE RISQUES

IMPACT				
	Élevé	7 Risque relatif aux attentes	8 Risque de double paiement Risque pour la sécurité des systèmes	9
	Intermédiaire	4	5 Risque lié aux ressources humaines	6 Risque de retard
	Faible	1	2	3
		Faible	**Intermédiaire**	**Élevé**
		PROBABILITÉ		

Le risque relatif aux attentes est considéré comme un risque à *impact fort*, car, en l'absence d'orientation et de supervision suffisantes de la part de la direction générale, des décaissements conséquents indus ou frauduleux pourraient être effectués. La probabilité de ce risque est considérée comme *faible*, car il existe de nombreux exemples de bonnes règles et procédures efficaces régissant les activités de décaissements, et la direction générale n'est pas censée ignorer un domaine aussi important.

Le risque de retard est considéré comme un risque à *impact intermédiaire*, car les pénalités et les intérêts de retard ne sont pas très importants, bien qu'il soit préoccupant d'entretenir de mauvaises relations avec ses fournisseurs. La probabilité de ce risque est considérée comme *élevée*, car on dépend d'un grand nombre de personnes lorsqu'on veut engager un processus de décaissement et, avec des délais de règlement généralement serrés, le processus peut prendre du retard pour plusieurs raisons, ce qui peut entraîner des retards de paiement.

Le risque lié aux ressources humaines est considéré comme un risque à *impact intermédiaire*, car le fait de ne pas recruter, former et conserver de collaborateurs compétents au sein du service des comptes fournisseurs peut entraîner un nombre plus élevé que souhaitable de paiements erronés ou en retard. La probabilité de ce risque est considérée comme *intermédiaire*, car les compétences nécessaires ne sont pas forcément difficiles à trouver sur le marché.

Le risque associé à l'accès aux systèmes est considéré comme un risque à *impact fort*, car un accès non autorisé peut se traduire par des changements susceptibles de dissimuler des décaissements indus. La probabilité de ce risque est considérée comme *intermédiaire*, car ces décaissements indus peuvent être détectés par d'autres moyens.

Le risque de double paiement est considéré comme un risque à *impact fort*, car un seul paiement en double peut se révéler conséquent et peut entraîner un préjudice pécuniaire s'il n'est pas détecté. La probabilité de ce risque est considérée comme *intermédiaire*, car il est assez fréquent que des factures soient présentées deux fois à une organisation. Cependant, la plupart des fournisseurs sont honnêtes, si bien qu'il est moins probable que des doubles paiements importants passent inaperçus sur la durée.

Copyright © 2015 Eyrolles.

Il est important de comprendre les seuils de tolérance du management, mais cette étape ne doit pas forcément se substituer au jugement de l'auditeur interne. Il ne faut pas oublier que la fonction d'audit interne est d'être au service de nombreuses parties prenantes. Sa responsabilité fiduciaire vis-à-vis des autres ne doit pas être subordonnée si l'auditeur interne estime que les responsables du processus ont un seuil de tolérance au risque supérieur à celui des autres parties prenantes. Cependant, la capacité à bien cerner les seuils de tolérance au risque des responsables du processus aide l'auditeur interne à finaliser son jugement sur l'évaluation des risques, et l'auditeur interne peut alors plus facilement estimer l'importance des constats d'audit ultérieurs.

IDENTIFIER LES CONTRÔLES CLÉS

Un processus peut être composé de plusieurs actions, et toutes peuvent jouer un rôle dans l'obtention du résultat final, mais rares sont celles qui sont vraiment critiques au point que leur absence compromettrait la réalisation du résultat souhaité. Ces actions critiques sont appelées *contrôles clés*. Le chapitre 6, *Le contrôle interne*, donne une définition du contrôle interne et propose une discussion détaillée à ce sujet. Il ne faut pas non plus oublier, comme nous l'avons vu au début de ce chapitre, que les contrôles à l'échelle de l'entité peuvent se répercuter sur le fonctionnement des contrôles au niveau des processus. L'auditeur interne doit donc tenir compte de l'impact que produisent les contrôles à l'échelle de l'entité sur le processus qu'il examine avant de se lancer dans l'identification des contrôles clés au niveau du processus.

Contrôle clé (ou contrôle primaire)

Activité destinée à réduire les risques associés à un objectif critique de l'organisation.

Pour mener à bien cette activité de la planification de la mission, il importe de bien déterminer les différentes catégories de contrôles à classer parmi les contrôles clés au niveau du processus. Bien qu'elle ne soit pas exhaustive, la liste ci-après énumère des exemples de catégories de contrôles courantes.

- **La validation** consiste à obtenir une autorisation pour l'exécution d'une transaction, l'autorisation devant être donnée par une personne qui en a le pouvoir (par exemple autorisation d'une sortie de bilan).
- **Le calcul** implique de compter ou de recompter un montant qui résulte d'autres données obtenues dans le processus (par exemple, utiliser des données historiques sur les sorties de bilan afin de calculer une provision pour créances douteuses, ou vérifier un calcul d'amortissement pour vérifier que le montant calculé par le système est raisonnable).
- **La documentation** vise à préserver les informations sources ou à consigner dans un document le raisonnement qui a présidé à un jugement afin de pouvoir s'y référer ultérieurement (par

Copyright © 2015 Eyrolles.

exemple, scanner les bordereaux de réception, les factures et les chèques concernant un paiement, ou rédiger une note, jointe aux dossiers, qui explique les jugements opérés pour déterminer des charges à payer).

- **L'examen** consiste à vérifier un attribut, c'est-à-dire un élément de données, un événement ou une preuve documentaire étayant l'existence ou la survenue (par exemple, la preuve que les marchandises payées ont bien été reçues).
- **Le rapprochement** suppose d'établir des comparaisons entre deux attributs différents pour vérifier qu'ils correspondent (par exemple, que le montant d'un paiement correspond au montant figurant sur la facture).
- **Le pilotage** consiste à vérifier le respect des procédures en place (par exemple, vérifier que la personne chargée de valider les factures ne dépasse pas les limites qui lui sont fixées).
- **La restriction** consiste à ne pas autoriser une action inacceptable (par exemple, interdire la spéculation sur les fluctuations des taux d'intérêt, ou interdire aux personnes non autorisées d'accéder à certaines données au sein de systèmes sensibles).
- **La séparation des tâches** se focalise sur la séparation des activités incompatibles dont la concomitance pourrait ouvrir la voie à une action indésirable (par exemple, séparer le pouvoir de signer les chèques de celui d'autoriser les factures).
- **La supervision** apporte une orientation et une surveillance afin que les actions et les tâches soient exécutées comme prévu (par exemple, le superviseur valide un lot avant traitement informatique).

Comme indiqué précédemment, l'identification des contrôles au niveau des processus commence généralement avec les deux étapes de planification préalables : « Comprendre l'entité auditée » et « Repérer et évaluer les risques ». Il est important à ce stade de pouvoir identifier les contrôles clés.

L'auditeur interne ne peut s'appuyer sur aucune checklist ni sur aucune formule qui lui apporterait des informations incontestables lui permettant de distinguer les contrôles clés des autres. Ce processus fait plutôt intervenir le jugement et l'auditeur interne peut l'optimiser en répondant à la question suivante : s'ils ne sont pas exécutés comme prévu, lesquels de ces contrôles pourraient entraver la réalisation des objectifs au niveau du processus ? Les contrôles qui permettent de maîtriser les risques élevés ou intermédiaires, tels que décrits à l'encadré 13-8, sont probablement des contrôles clés. Les aspects suivants sont importants lorsqu'il s'agit de déterminer quels sont les contrôles clés.

Copyright © 2015 Eyrolles.

- L'auditeur interne doit bien comprendre les objectifs attachés au processus.
- Il doit évaluer les conséquences d'une mauvaise exécution des contrôles, afin de déterminer si une déficience du contrôle pourrait significativement entraver la réalisation des objectifs.
- Il doit envisager d'autres contrôles compensatoires, qui peuvent indiquer que le fonctionnement d'un contrôle clé donné n'est pas aussi critique qu'on l'avait cru dans un premier temps.
- Il lui faut aussi tenir compte de l'effet d'un contrôle sur les autres contrôles. Ainsi, il peut apparaître que l'exécution d'un contrôle n'entrave pas significativement la réalisation d'un objectif, mais pourrait avoir un impact sur l'exécution des autres contrôles, ce qui pourrait compromettre la réalisation d'un objectif.
- L'auditeur doit aussi prendre en compte l'impact des contrôles à l'échelle de l'entité. En effet, des déficiences au niveau de ces contrôles peuvent amoindrir l'efficacité des contrôles au niveau des processus. À l'inverse, des faiblesses identifiées au niveau des contrôles du processus peuvent être contrebalancées par l'efficacité des contrôles à l'échelle de l'entité.
- Il convient en outre de modifier ou d'éliminer les contrôles redondants ou ceux qui ne sont pas rentables. Ces contrôles ne sont probablement pas des contrôles clés.

La dernière activité de cette étape de planification de la mission consiste à relier les contrôles au niveau du processus aux risques du même processus. La réalisation des objectifs est tributaire de divers scénarios de risque, et certains contrôles ne font que maîtriser certains risques. En fin de compte, si l'on juge qu'un contrôle est inopérant, il risque d'avoir un impact sur un ou plusieurs risques. La documentation de ce lien peut prendre la forme d'une matrice simple, appelée matrice de risques et de contrôles, dont un exemple est présenté à l'encadré 13-10.

Nous verrons ultérieurement comment utiliser cette matrice dans le cadre du programme d'audit.

ÉVALUER L'ADÉQUATION DE LA CONCEPTION DES CONTRÔLES

L'étape suivante de la planification d'une mission consiste à évaluer l'adéquation de la conception des processus. Pour l'essentiel, il s'agit de déterminer si les contrôles clés sont conçus de manière adéquate pour ramener à un niveau acceptable les différents risques liés aux processus. Il convient de répondre aux questions suivantes lorsque l'on évalue l'adéquation de la conception des processus.

Copyright © 2015 Eyrolles.

- L'auditeur interne comprend-il ce qu'est un « niveau de risque acceptable », d'après les seuils de tolérance au risque du management induit par le processus ?
- Les contrôles clés, considérés individuellement ou globalement, permettent-ils de ramener à un niveau acceptable les risques liés aux processus ?
- Existe-t-il d'autres contrôles compensatoires qui concernent d'autres processus et permettent de réduire davantage les risques pour les ramener à des niveaux suffisamment faibles ?
- Peut-on considérer que les contrôles clés, s'ils fonctionnent de manière effective, soutiennent la réalisation des objectifs au niveau des processus ?
- Dans la limite de ce qui est approprié, la conception des processus répond-elle aux principes d'efficacité et d'efficience des opérations, de fiabilité du reporting, de conformité aux lois et règlements applicables et de réalisation des objectifs stratégiques ?
- Quelles lacunes éventuelles entravent les processus ?
- Quelles sont les lacunes particulières qui existent dans la conception du processus ?
- Quels en sont les conséquences ou les effets possibles ?
- Pourquoi ces lacunes existent-elles, c'est-à-dire quelles en sont les causes (par exemple, des procédures inadéquates, des politiques peu claires, l'absence d'interfaces ou la non-séparation des tâches) ?

ENCADRÉ 13-10

EXEMPLE DE MATRICE DE RISQUES ET DE CONTRÔLES

Risque au niveau du processus	Contrôle clé	Adéquation de la conception
Risque A – Définition (objectifs au niveau du processus)	• Contrôle A • Contrôle B • Contrôle C	Les contrôles clés mentionnés sont conçus de manière adéquate pour ramener ce risque à un niveau acceptable.
Risque B – Définition (objectifs au niveau du processus)	• Contrôle A • Contrôle D	Les contrôles clés mentionnés **ne** sont **pas** conçus de manière adéquate pour ramener ce risque à un niveau acceptable (décrire la faiblesse de conception).
Risque C – Définition (objectifs au niveau du processus)	• Contrôle C • Contrôle E • Contrôle F	Les contrôles clés mentionnés sont conçus de manière adéquate pour ramener ce risque à un niveau acceptable.

Lorsque l'auditeur interne a fini d'évaluer l'adéquation de la conception, tous les points identifiés doivent faire l'objet d'une discussion avec le management et être documentés en tant qu'observations

Copyright © 2015 Eyrolles.

d'audit préliminaires. Notons que la matrice présentée dans l'encadré 13-10 comporte une colonne intitulée « Adéquation de la conception », dans laquelle l'auditeur interne peut émettre un jugement. Comme indiqué dans cet encadré, ce jugement correspond généralement à l'une des formulations suivantes :

- les contrôles clés mentionnés sont conçus de manière adéquate pour ramener ce risque à un niveau acceptable ;
- les contrôles clés mentionnés ne sont pas conçus de manière adéquate pour ramener ce risque à un niveau acceptable (décrire la faiblesse de conception).

Une fois que l'auditeur interne a évalué l'adéquation de la conception des contrôles pour chaque processus, il peut évaluer la conception globale du dispositif de contrôle.

- La conception est adéquate, il n'existe pas de lacunes importantes. Globalement, le processus et les systèmes d'information paraissent conçus de manière adéquate pour ramener les risques à un niveau acceptable.
- La conception est adéquate, mais il existe des lacunes. Globalement, le processus et les systèmes d'information paraissent conçus de manière adéquate pour ramener les risques à un niveau acceptable. Néanmoins, l'existence d'une ou de plusieurs lacunes peut engendrer une certaine exposition, que le propriétaire du processus peut estimer inacceptable.
- La conception est inadéquate, il existe des lacunes importantes. Globalement, la conception du processus ne paraît pas adéquate pour ramener les risques à un niveau acceptable. Des lacunes importantes engendrent un degré d'exposition inacceptable, qui empêchera la réalisation des objectifs au niveau des processus.

Ces observations distinctes et l'évaluation générale influeront sur la nature, l'étendue et le calendrier des tests à effectuer.

Adéquation de la conception

Caractéristique des activités de contrôle permettant d'affirmer que le management les a planifiées et organisées (conçues) de manière à donner une assurance raisonnable quant à la possibilité de ramener les risques à un niveau acceptable.

ÉTABLIR UN PLAN DES TESTS

Lorsque l'auditeur interne a parfaitement compris comment fonctionnent les processus et qu'il en a évalué la conception, l'étape suivante consiste à établir un plan des tests. Celui-ci doit être élaboré de façon à permettre de recueillir des preuves (ou éléments probants) suffisantes et adéquates pour étayer une évaluation portant sur le fonctionnement effectif des contrôles clés. Cette évaluation et l'évaluation de l'adéquation de la conception des processus apportent à l'auditeur interne une assurance raisonnable que les objectifs au niveau des processus seront atteints.

Copyright © 2015 Eyrolles.

D'après la connaissance qu'il a acquise lors des étapes précédentes de la planification de la mission, l'auditeur interne est alors prêt à :

- déterminer quels contrôles sont suffisamment importants pour nécessiter des tests ;
- définir une méthode de test pour ces contrôles ;
- documenter les jugements étayant le choix de cette méthode.

Chacune de ces activités est analysée plus en détail dans les sections suivantes.

Assurance raisonnable

Niveau d'assurance étayé par des procédures et des jugements d'audit généralement acceptés. Il peut concerner l'efficacité du contrôle interne, la maîtrise des risques, la réalisation des objectifs ou d'autres conclusions relatives à la mission.

Déterminer quels contrôles tester

Comme indiqué plus haut, les tests visent principalement à déterminer si les contrôles clés fonctionnent de manière suffisamment effective pour permettre une gestion suffisante des risques au niveau des processus. Bien que l'on puisse y parvenir en se contentant de vérifier tous les contrôles clés identifiés, l'auditeur interne doit aussi prendre en compte d'autres facteurs lorsqu'il détermine quels contrôles tester.

- Existe-t-il des contrôles de niveau général qui pourraient, par nature, apporter une assurance raisonnable quant à la gestion suffisante des risques concernés ? Ces contrôles peuvent être des rapprochements, du pilotage opérationnel ou de la supervision que des personnes effectuent indépendamment des propriétaires des contrôles détaillés (tels qu'un chef d'équipe ou un directeur, par exemple). Dans le cadre d'une évaluation descendante des risques fondée sur les contrôles, l'auditeur interne doit prêter attention à ces contrôles de niveau général, tout autant qu'à l'impact des contrôles à l'échelle de l'entité (voir plus haut dans ce chapitre).
- Existe-t-il d'autres contrôles compensatoires qui portent sur plusieurs risques ? Si tel est le cas, il peut être plus efficient de tester ces contrôles plutôt que chaque contrôle clé détaillé.
- La conception des contrôles évalués a-t-elle été jugée adéquate ? Si tel n'est pas le cas, il n'est peut-être pas nécessaire de tester ces contrôles, car, même s'ils fonctionnent efficacement, leur conception inadéquate peut les empêcher de maîtriser les risques.
  - Cependant, l'auditeur interne peut décider d'effectuer des tests pour déterminer l'ampleur des erreurs découlant d'une conception inadéquate des contrôles. Les types de tests destinés à quantifier les erreurs (extraction et analyse de données, par exemple) différeront probablement des tests directs visant à évaluer l'efficacité des contrôles.
  - Quand les contrôles clés se déroulent-ils et, d'après la période couverte par la mission, est-il possible d'en tester certains ?

Copyright © 2015 Eyrolles.

Il se peut, par exemple, qu'une partie de ces contrôles ne soit effectuée qu'en fin d'exercice. Si la mission est conduite en cours d'exercice, il n'est peut-être pas possible de tester certains de ces contrôles.

- Y a-t-il eu, durant la période couverte par la mission, des changements dans le processus qui auraient pour conséquence d'amoindrir l'efficacité des contrôles clés sur une période donnée ? Si tel est le cas, il faut impérativement s'intéresser à la façon dont ces changements pourraient influer sur les tests des contrôles clés.

Une fois que ces facteurs ont été pris en compte, l'auditeur interne est prêt à définir une méthode de test spécifique. Comme indiqué plus haut, celle-ci se concentre généralement sur l'évaluation de l'efficacité des contrôles conçus de manière adéquate, mais certains tests peuvent être nécessaires pour quantifier l'impact des contrôles qui ne sont pas conçus de manière adéquate.

Définir une méthode de test

Pour définir une méthode de test, il faut déterminer la nature, l'étendue et le calendrier des tests à effectuer. Ces derniers ont pour finalité première d'établir si les contrôles concernés fonctionnent comme prévu pour ramener les risques visés à un niveau acceptable. Les différents types de tests d'audit sont détaillés au chapitre 10, *Les preuves d'audit et les papiers de travail*. Voici toutefois un aperçu des décisions à prendre lorsque l'on définit une méthode de test.

- **Nature des tests.** Différents types de tests apportent des degrés d'assurance différents et demandent plus ou moins de temps.
- **Étendue des tests.** Les tests peuvent porter sur une partie ou sur la totalité de la population des contrôles, c'est-à-dire sur un échantillon de transactions ou sur 100 % des transactions. Bien sûr, plus l'échantillon est large, plus le degré d'assurance procuré par les tests sera élevé, mais plus ces derniers prendront du temps. Les techniques d'échantillonnage sont détaillées au chapitre 11, *L'échantillonnage en audit*.
- **Calendrier des tests.** Les tests peuvent être effectués à différentes fréquences (intervalles), en fonction de la période couverte par la mission, de la nature du contrôle et du type de test.

D'autres facteurs peuvent également influer sur la nature, l'étendue et le calendrier des tests. L'essentiel est que la méthode de test apporte des preuves suffisantes sur la gestion de l'ensemble des risques au niveau des processus.

Copyright © 2015 Eyrolles.

Documenter la méthode de test

On peut élargir la matrice de risques et de contrôles illustrée par l'encadré 13-10 en ajoutant une colonne qui présente la méthode de test appliquée à chaque risque. L'encadré 13-11 en donne un exemple (N.B. : la colonne Adéquation de la conception dans l'encadré 13-10 a été supprimée, de façon à montrer la relation étroite entre les colonnes Contrôle clé et Méthode de test).

Notons que certains des tests peuvent s'appliquer à plusieurs contrôles. Il s'agit alors de tests polyvalents.

ENCADRÉ 13-11

EXEMPLE DE MATRICE DE RISQUES ET DE CONTRÔLES AVEC MÉTHODES DE TEST

Risque au niveau du processus	Contrôle clé	Méthode de test
Risque A – Définition (objectifs au niveau du processus)	• Contrôle A • Contrôle B • Contrôle C	• Test A • Test B • Test C
Risque B – Définition (objectifs au niveau du processus)	• Contrôle A • Contrôle D • Contrôle E	• Test A • Test D • Test E

Exemple Books 2 Buy. L'encadré 13-12 présente une matrice de risques et de contrôles partiels pour la fonction décaissements.

Programme de travail

Document énumérant les procédures à mettre en œuvre, conçu pour réaliser le plan de mission.

ÉLABORER UN PROGRAMME DE TRAVAIL

L'étape suivante de la planification de la mission consiste à documenter tous les jugements et conclusions rendus au cours de la planification. Comme le montre l'étendue des activités traitées dans ce chapitre, de nombreuses tâches différentes mais importantes ont été exécutées à ce stade, et celles qu'il reste à effectuer sont également nombreuses (tests et reporting, notamment). Pour que tous les membres de l'équipe chargée de la mission comprennent ce qui a été fait et ce qui reste à faire, il convient d'élaborer un programme de travail. Celui-ci peut revêtir différentes formats, par exemple :

- un modèle standard ou une checklist que l'auditeur interne principal établit pour documenter l'achèvement des étapes de la planification. On recourt souvent à des modèles standard pour s'assurer que chaque mission couvre toutes les activités nécessaires ;
- une note de synthèse résumant les analyses menées au cours de cette phase. Lorsque les missions sont peu standard, cette approche est préférable, car elle sera plus flexible selon les thématiques ;

Copyright © 2015 Eyrolles.

EXEMPLE DE MATRICE DE RISQUES ET DE CONTRÔLES POUR LES DÉCAISSEMENTS

Risque au niveau du processus	Contrôle clé	Méthode de test
Risque relatif aux attentes L'absence de politiques, procédures et autres formes de communication de la direction générale bien conçues et bien articulées peut conduire des collaborateurs à exercer leurs responsabilités à l'encontre des attentes et des souhaits de la direction générale (objectifs d'exactitude, de rapidité, d'enregistrement, de conformité et d'autorisation).	• La politique de délégation de pouvoir définit des niveaux d'autorisation pour les décisions d'achat et de décaissement. • Le service CF a élaboré des procédures détaillées, qui couvrent toutes les tâches essentielles relatives aux décaissements.	• Examiner la politique de délégation de pouvoir et évaluer si elle est actualisée et appropriée étant donné les responsabilités actuelles des personnes concernées. • Sélectionner un échantillon de 80 décaissements (risque de 10 %, taux d'écarts acceptable de 5 % et taux d'écarts attendu de 1 %) et tester la conformité des autorisations à la politique établie. • Examiner les procédures et en discuter avec les collaborateurs du service CF, afin de déterminer si elles reflètent exactement les tâches requises et pourraient être suivies par d'autres intervenants.
Risque de double paiement L'incapacité à identifier des saisies multiples de factures peut entraîner des paiements en double aux fournisseurs. Ces paiements risquent de ne pas être décelés ou de se révéler difficiles à recouvrer (objectifs d'exactitude et d'enregistrement).	• Le système d'achats alerte le collaborateur du service CF si la référence du fournisseur, le numéro de la facture et le montant de la facture correspondent à une facture saisie antérieurement. • Le processus de décaissement marquera tout paiement de montant identique effectué au profit d'un même fournisseur, afin qu'il puisse être examiné avant décaissement.	• Tester la capacité du système à produire des factures en double en essayant de saisir des numéros de facture en double. Tester également ce qui se produit si un chiffre ou un symbole est ajouté à la fin d'un numéro de facture en double. • Étant donné que le système n'alerte l'utilisateur qu'en cas de possibilité de paiement en double, extraire 100 % des paiements relatifs à l'exercice précédent et vérifier si des paiements en double sont possibles. • Réaliser des tests pour s'assurer que le marquage des décaissements fonctionne comme prévu.
Risque de retard L'incapacité à traiter les paiements en temps opportun peut entraîner des amendes ou des pénalités (de retard) ou empêcher l'organisation de bénéficier de remises (objectifs de rapidité et de trésorerie).	• Le système impose de saisir une date de paiement lors de l'enregistrement des données relatives à la facture. • Un rapport d'édition est généré à chaque fois qu'une date de paiement est postérieure de 30 jours à la date de la facture. • L'écran de saisie des factures comporte un champ que l'on peut vérifier si la facture concernée remplit les conditions d'une remise pour paiement anticipé.	• Tester la fonctionnalité du système pour les trois contrôles clés. • À l'aide d'un logiciel d'analyse de données, calculer l'écart entre la date de paiement et la date de la facture pour 100 % des paiements effectués durant l'exercice précédent. Procéder au suivi de tout paiement en retard ou de toute occasion manquée de bénéficier d'une remise.
Risque associé à l'accès aux systèmes L'absence de pratiques efficaces visant la sécurité logique peut permettre à des personnes non autorisées d'accéder à des données importantes relatives aux décaissements, de les manipuler ou de les effacer (objectifs d'exactitude, d'enregistrement et de trésorerie).	• La sécurité logique est administrée par le SI de la même façon que pour toutes les autres applications. • Le manager du service CF doit examiner et confirmer deux fois par an les droits d'accès au système de décaissement.	• La sécurité logique du SI est testée dans le cadre d'une mission distincte par des spécialistes de l'audit des SI. Vérifier les résultats de cet audit pour établir l'absence de toute déficience de conception relative à la sécurité des décaissements. • Discuter avec le manager du service CF pour confirmer les droits d'accès. Examiner la documentation qui étaye cette procédure.

Copyright © 2015 Eyrolles.

- des colonnes supplémentaires sur la matrice de risques et de contrôles si l'auditeur interne souhaite que tous les éléments soient regroupés dans un seul document ;
- une combinaison des trois.

Le format varie d'une fonction d'audit interne à l'autre. L'essentiel est de disposer de moyens :

- permettant à tous les membres de l'équipe chargée de la mission de comprendre ce qui a été fait et ce qui reste à faire ;
- présentant les responsables de chaque activité entrant dans le cadre de la mission ;
- consignant par écrit les activités qui sont achevées ;
- facilitant la revue par un manager ou un directeur de mission, lequel assure la surveillance et donne l'orientation au cours de la planification de la mission.

Quel que soit son format, un programme de travail type porte sur les aspects suivants :

- les grandes tâches administratives, telles que la rédaction d'une note de planification, l'échéancier de déploiement des ressources, la définition des points d'étape, etc.
- la tenue d'une réunion de lancement avec les responsables du processus, afin de discuter des objectifs et du périmètre de la mission, des risques au niveau des processus, du calendrier de la mission, des informations qu'il est nécessaire d'obtenir des collaborateurs au niveau des processus, des rapports et autres prestations, et de toute attente du management vis-à-vis de la mission ;
- les activités de planification, énumérant chacune de celles traitées dans ce chapitre (par exemple comprendre le processus, évaluer les risques au niveau du processus et identifier les contrôles clés) ;
- les activités à réaliser lors du travail sur le terrain, énumérant les tests spécifiques à effectuer (ces tests peuvent être portés sur la matrice de risques et de contrôles présentée plus haut) ;
- les étapes de finalisation, par exemple la levée des points de revue, la tenue d'une réunion de clôture avec les responsables du processus et la finalisation des papiers de travail ;
- les activités de reporting, notamment la rédaction d'un projet de rapport de mission, la demande d'un retour d'information de la part des responsables du processus et la remise du rapport définitif de la mission (pour plus de détails, voir le chapitre 14, *La communication des résultats d'une mission d'assurance et les procédures de suivi*).

Copyright © 2015 Eyrolles.

L'élaboration d'un programme de travail est traitée à la fin du présent chapitre, mais se déroule en fait généralement tout au long du processus de planification de la mission. Comme indiqué, le format du programme de travail n'est pas ce qui importe : l'essentiel est de présenter les grandes phases, ainsi que les jugements et conclusions rendus au cours de ce processus, et d'aider à l'accomplissement du reste de la mission.

ALLOUER DES RESSOURCES À LA MISSION

La planification de la mission s'achève par la détermination des ressources nécessaires pour mener à bien les activités prévues. Il s'agit (1) d'estimer, ou de budgéter, ces ressources, (2) d'allouer les ressources humaines appropriées à la mission et (3) de programmer le déploiement de ces ressources de façon à ce que la mission soit achevée dans les délais.

Ressources affectées à la mission

– Auditeurs internes.
– Autres personnes (au sein/à l'extérieur de l'organisation).
– Déplacements.
– Technologie.
– Autres.

Budgétisation

La première tâche consiste à estimer les ressources nécessaires à la conduite de la mission. Il convient d'élaborer un budget prenant en compte le nombre d'heures requises pour mener à bien la mission et les autres coûts éventuels.

- **Nombre d'heures nécessaires pour mener à bien la mission.** Un auditeur interne expérimenté est en mesure de produire une estimation raisonnable du nombre d'heures nécessaires pour réaliser les phases de planification, d'exécution et de communication relatives à une mission. Cette estimation doit être réaliste, mais ne peut pas toujours être précise, car des événements inattendus sont susceptibles de retarder la mission (notamment si les collaborateurs clés au niveau du processus ne sont pas disponibles, si l'information demandée est obtenue après un long délai ou si des auditeurs internes sont malades). Il peut être utile de prévoir une marge de fluctuation (de ± 10 %, par exemple).
- **Autres coûts.** Outre le coût des ressources humaines, certaines missions peuvent nécessiter des dépenses supplémentaires. En voici des exemples courants :
  - frais de déplacement et frais connexes, lorsque la mission doit être menée, en totalité ou en partie, hors du site sur lequel les auditeurs internes sont basés ;
  - coût de la technologie, lorsque la réalisation de la mission impose d'accéder à une technologie unique ou non standard (licences pour des logiciels d'analyse de données et d'analyse de la sécurité réseau, par exemple) ;

Copyright © 2015 Eyrolles.

- coût des éventuelles fournitures non standard nécessaires (chaussures à embout en acier ou casques pour les observations du dénombrement des stocks, papier ou encre spécial[e] pour les documents à fournir qui comportent beaucoup d'illustrations ou des diagrammes et graphiques en couleur…).

Généralement, l'auditeur interne principal affecté à la mission a de l'expérience dans l'élaboration des budgets, et il devra rendre compte de la gestion de la mission au regard des limites budgétaires définies. Le responsable de l'audit interne se fie à l'efficacité de la budgétisation de la mission lorsqu'il détermine le budget global de son service. Pour de plus amples détails, voir le chapitre 9, *La gestion de l'audit interne*.

Allocation des ressources humaines

Externalisation (ou co-traitance)

Complément apporté à la fonction d'audit interne de l'organisation par le recours aux services de prestataires tiers afin de se doter d'une expertise dans un domaine précis et pour une mission spécifique ou de combler une lacune dans les ressources nécessaires pour mener à bien le plan d'audit interne.

Le budget de la mission ayant été fixé, il faut alors identifier et allouer les ressources permettant de mener à bien la mission. L'allocation des ressources humaines constitue la tâche la plus importante et la plus ardue. Il faut pour cela répondre aux questions suivantes.

- Quels types de compétences cette mission requiert-elle (par exemple, en termes de reporting financier ou de SI) ?
- Quelle est l'expérience nécessaire pour cette mission (connaissance du domaine, expérience antérieure acquise lors de missions analogues, etc.) ?
- Qui, au sein du service, dispose des qualifications et de l'expérience requises ?
- Faut-il des compétences spécialisées dont la fonction d'audit interne est dépourvue (dans le domaine des instruments financiers ou des risques environnementaux notamment) ? Si tel est le cas, où peut-on obtenir ces compétences, à un coût raisonnable ?
- Existe-t-il des aspects relatifs au développement professionnel qui sont susceptibles d'influer sur l'allocation des ressources pour cette mission ? Par exemple, certains auditeurs internes ont-ils besoin d'un type d'expérience particulière pour acquérir des connaissances et étoffer leurs compétences professionnelles ?
- Existe-t-il d'autres considérations spéciales, relatives au service concerné de l'organisation, qui sont susceptibles d'influer sur l'allocation des auditeurs internes pour la mission ?

Copyright © 2015 Eyrolles.

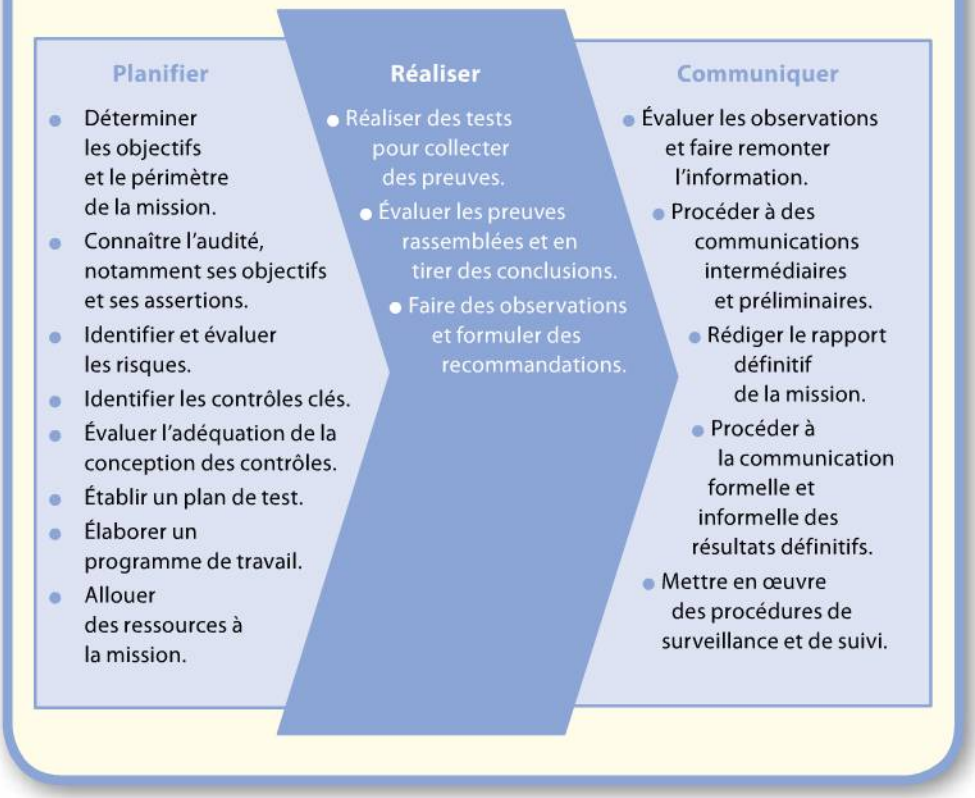
Planification

Après avoir déterminé quelles ressources humaines sont appropriées, il faut établir formellement un échéancier de déploiement. Ce peut être un processus très dynamique, lors duquel il faut notamment prendre en compte les aspects suivants.

- **Disponibilité des collaborateurs clés au niveau des processus.** Même s'il peut être pratique, pour l'audit interne, qu'une mission commence à une date donnée, ce calendrier ne conviendra pas forcément aux audités. C'est par exemple le cas sur certaines périodes du mois ou du trimestre (telle que la période durant laquelle le service comptable est occupé à la clôture des comptes). En outre, le calendrier de la mission peut devoir être modifié en raison d'absences (déplacement, congés, formation, etc.) ou lorsque les collaborateurs clés sont occupés à d'autres tâches.
- **Disponibilité des ressources de la mission.** Comme les collaborateurs clés au niveau des processus, il arrive que les auditeurs internes aient d'autres engagements (congés, formation, initiatives internes, etc.) susceptibles d'influer sur le calendrier d'une mission.

ENCADRÉ 13-13

LE DÉROULEMENT DE LA MISSION D'ASSURANCE



Copyright © 2015 Eyrolles.

- **Disponibilité des ressources extérieures.** Si des compétences spécialisées ou des personnes supplémentaires sont nécessaires pour une mission, leur disponibilité doit également entrer en ligne de compte. Les sociétés de services qui apportent ces ressources ont parfois un calendrier différent de celui de l'organisation (par exemple en ce qui concerne les jours de congé, les semaines de formation collective ou les initiatives internes).
- **Disponibilité des évaluateurs principaux.** Même si les ressources essentielles de la mission sont disponibles pour la réalisation des travaux sur le terrain, il faut que le responsable d'audit ou le directeur de la mission soit également disponible pour mettre en œuvre le niveau de revue requis, sans quoi l'achèvement de la mission peut être retardé.

Après l'allocation des ressources et l'élaboration de leur échéancier de déploiement, la mission peut commencer. L'encadré 13-13 met en lumière la phase fondamentale suivante de la mission d'assurance, à savoir l'exécution. Les activités essentielles qu'elle nécessite sont également répertoriées dans le même encadré.

RÉALISER DES TESTS POUR COLLECTER DES PREUVES

La mission d'assurance passe ici de la phase de planification à la phase d'exécution. Dès lors, il faut appliquer la méthode de test définie lors de la planification et présentée sur la matrice de risques et de contrôles (encadré 13-11), afin de déterminer si les contrôles fonctionnent comme prévu. La réalisation de chaque test permet de réunir des éléments permettant d'étayer les conclusions de l'auditeur interne quant au fonctionnement effectif des contrôles.

Les résultats des tests peuvent être portés sur la matrice de risques et de contrôles. On peut développer celle présentée à titre d'illustration dans l'encadré 13-11 en y ajoutant une colonne qui présente les résultats des tests. L'encadré 13-14 en donne un exemple. Remarque : dans ce dernier, la colonne de l'encadré 13-11 relative

Copyright © 2015 Eyrolles.

ENCADRÉ 13-14

EXEMPLE DE MATRICE DE RISQUES ET DE CONTRÔLES, AVEC RÉSULTATS DES TESTS

Risque au niveau du processus	Méthode de test	Résultats des tests
Risque A – Définition (objectifs au niveau du processus)	• Test A • Test B • Test C	• Résultat A • Résultat B • Résultat C
Risque B – Définition (objectifs au niveau du processus)	• Test A • Test D • Test E	• Résultat A • Résultat D • Résultat E

aux contrôles clés a disparu. Nous avons en effet simplifié cet exemple, car cette colonne n'est pas essentielle pour la réflexion à ce stade.

Exemple Books 2 Buy. L'encadré 13-15 présente une matrice de risques et de contrôles partielle pour la fonction décaissements. À la fin de chaque entrée présentant les résultats des tests on trouve un renvoi aux papiers de travail qui documentent les tests respectifs (X-#). Les encadrés 13-16 et 13-17 donnent des exemples de deux tests. Si une exception ou une déficience a été constatée au cours des tests, il existe également un renvoi au papier de travail qui documente ce constat (Z-#).

ENCADRÉ 13-15

EXEMPLE DE MATRICE DE RISQUES ET DE CONTRÔLES POUR LES DÉCAISSEMENTS

Risque au niveau du processus	Méthode de test	Résultats des tests
Risque relatif aux attentes L'absence de politiques, procédures et autres formes de communication de la direction générale bien conçues et bien articulées peut conduire des collaborateurs à exercer leurs responsabilités à l'encontre des attentes et des souhaits de la direction générale (objectifs d'exactitude, de rapidité, d'enregistrement, de conformité et d'autorisation).	• Examiner la politique de délégation de pouvoir et évaluer si elle est actualisée et appropriée étant donné les responsabilités actuelles des personnes concernées. • Sélectionner un échantillon de 80 décaissements (risque de 10 %, taux d'écarts acceptable de 5 % et taux d'écarts attendu de 1 %) et tester la conformité des autorisations à la politique établie. • Examiner les procédures et en discuter avec les collaborateurs du service CF, afin de déterminer si elles reflètent exactement les tâches requises et pourraient être suivies par d'autres intervenants.	• La politique de délégation de pouvoir dresse une liste de sept personnes qui ne font plus partie de l'organisation. De plus, neuf personnes qui ont pris leurs fonctions actuelles depuis peu ou qui sont arrivées récemment dans l'organisation devraient figurer sur la liste mais en sont absentes (Z-3). Toutes les autres responsabilités ont paru appropriées (papier de travail X-1). • Aucune observation ne s'est dégagée de ce test, toutes les autorisations étaient conformes à la politique de délégation de pouvoir, après prise en compte des changements à apporter à cette politique, qui sont décrits dans le papier de travail X-1 (papier de travail X-2). • D'après les discussions et observations, il semble que les procédures documentées restent appropriées, actualisées et bien comprises (papier de travail X-3).
Risque de double paiement L'incapacité à identifier des saisies multiples de factures peut entraîner des paiements en double aux fournisseurs. Ces paiements risquent de ne pas être décelés ou de se révéler difficiles à recouvrer (objectifs d'exactitude et d'enregistrement).	• Tester la capacité du système à produire des factures en double en essayant de saisir des numéros de facture en double. Tester également ce qui se produit si un chiffre ou un symbole est ajouté à la fin d'un numéro de facture en double. • Étant donné que le système n'alerte l'utilisateur qu'en cas de possibilité de paiement en double, extraire 100 % des paiements relatifs à l'exercice précédent et vérifier si des paiements en double sont possibles. • Réaliser des tests pour s'assurer que le marquage des décaissements fonctionne comme prévu.	• Le système a rejeté toutes les saisies de factures en double. En revanche, il a accepté les factures sur lesquelles un chiffre ou un symbole a été ajouté à la fin du numéro de facture, ce qui est susceptible d'entraîner un paiement en double (Z-4) (papier de travail X-4). • Quatorze (14) paiements potentiellement en double ont été identifiés, totalisant 357 782. Le management du service CF assure le suivi de tous ces éléments, qui apparaissent imputables à la déficience mentionnée dans le papier de travail X-4 (X-5). • Les transactions de test pour ce contrôle ont toutes fait l'objet d'un marquage lors du processus de décaissement. Les 14 opérations identifiées lors du test des paiements en double venaient de processus de décaissement différents et, par conséquent, n'ont pas fait l'objet d'un marquage dans le cadre de ce contrôle (papier de travail X-6).

Copyright © 2015 Eyrolles.

Risque au niveau du processus	Méthode de test	Résultats des tests
Risque de retard L'incapacité à traiter les paiements en temps opportun peut entraîner des amendes ou des pénalités (de retard) ou empêcher l'organisation de bénéficier de remises (objectifs de rapidité et de trésorerie).	• Tester la fonctionnalité du système pour les trois contrôles clés. • À l'aide d'un logiciel d'analyse de données, calculer l'écart entre la date de paiement et la date de la facture pour 100 % des paiements effectués durant l'exercice précédent. Procéder au suivi de tout paiement en retard ou de toute occasion manquée de bénéficier d'une remise.	• Le test de référence pour les trois contrôles a indiqué que ceux-ci fonctionnaient comme prévu (papiers de travail X-7, X-8 et X-9). • Il y a eu 172 paiements en retard (1,1 % du total des décaissements). Des pénalités de retard ont été appliquées pour 21 de ces paiements. La réaction du management du service CF a permis l'annulation de ces pénalités de retard pour 9 des paiements et les pénalités payées ont totalisé 24 489 (Z-5). Aucune occasion manquée de bénéficier d'une remise n'a été identifiée (papiers de travail X-10 et X-11).
Risque associé à l'accès aux systèmes L'absence de pratiques efficaces visant la sécurité logique peut permettre à des personnes non autorisées d'accéder à des données importantes relatives aux décaissements, de les manipuler ou de les effacer (objectifs d'exactitude, d'enregistrement et de trésorerie).	• La sécurité logique du SI est testée dans le cadre d'une mission distincte par des spécialistes de l'audit des SI. Vérifier les résultats de cet audit pour établir l'absence de toute déficience de conception relative à la sécurité des décaissements. • Discuter avec le manager du service CF pour confirmer les droits d'accès. Examiner la documentation qui étaye cette procédure.	• Aucune déficience de conception n'a été relevée lors des tests de la sécurité logique du SI (papier de travail X-12). • D'après la discussion et l'observation de la documentation appropriée, il apparaît que les droits d'accès sont revus de manière appropriée et en temps opportun (papier de travail X-13).

Les encadrés 13-16 et 13-17 donnent des exemples de quelques papiers de travail relatifs à ces tests.

Dans certaines circonstances, les résultats des tests peuvent indiquer une lacune ou un problème potentiel, mais ils peuvent également être non concluants. Dans ce cas, l'auditeur interne peut devoir réaliser des tests supplémentaires ou réviser l'approche de test pour pouvoir en tirer les conclusions nécessaires. Ces dernières font l'objet de la section qui suit.

ÉVALUER LES PREUVES RASSEMBLÉES ET EN TIRER DES CONCLUSIONS

Les tests d'audit permettent à l'auditeur interne de réunir les éléments nécessaires à l'évaluation de la conception et du fonctionnement effectif des contrôles clés, et d'en tirer des conclusions sur l'efficacité du processus ou du domaine examiné. Voici des questions auxquelles l'auditeur interne peut devoir répondre, en fonction de la charte d'audit interne, des objectifs de la mission, ainsi que des attentes de l'audité et d'autres parties prenantes à l'audit interne :

- Les contrôles clés sont-ils conçus de manière adéquate ?
- Les contrôles clés fonctionnent-ils de manière effective, c'est-à-dire comme on le prévoyait au moment de leur conception ?

Copyright © 2015 Eyrolles.

ENCADRÉ 13-16

EXEMPLE DE RISQUE RELATIF AUX ATTENTES, TEST N° 1

X-1
Élaboré par : Steve Braveheart
Revu par : David Richardson

Finalité du test : vérifier que la politique de délégation de pouvoir est complète, appropriée et actualisée pour définir qui détient le pouvoir d'autoriser les achats et décaissements.

Méthode de test : examiner la politique de délégation de pouvoir et évaluer si elle paraît actualisée et appropriée étant donné les responsabilités actuelles des personnes concernées.

Considérations relatives à l'échantillonnage : cette politique concerne 147 personnes. Étant donné la taille restreinte de cette population et la nature de l'assertion (selon laquelle un pouvoir est délégué à toutes les personnes habilitées, et à elles seulement, pour qu'elles autorisent achats et décaissements), un échantillon non statistique a été sélectionné. En commençant par la première figurant sur la liste, on a évalué, toutes les trois personnes, si la délégation de pouvoir qu'elles avaient reçue était appropriée.

Résultats du test : les résultats du test sont les suivants :

- l'échantillon initial ayant été complété, on a identifié trois personnes qui ne font plus partie de l'organisation ;
- en raison de cette observation, on a élargi le test pour y inclure les 147 personnes. Il a alors été constaté que sept ne faisaient plus partie de l'organisation, dont une depuis 15 mois ;
- constatant que la liste n'avait pas été actualisée en temps opportun, l'auditeur a également réalisé des tests portant sur les nouveaux collaborateurs et sur les promotions au cours des 18 mois précédents. Il a découvert que cinq des nouveaux collaborateurs et quatre des collaborateurs promus auraient dû figurer sur la liste, étant donné les responsabilités qui leur ont été assignées.

Conclusion : d'après les résultats des tests, le contrôle portant sur la politique de délégation de pouvoir **ne** fonctionne **pas** toujours de manière effective, car les listings n'ont pas été actualisés en temps opportun alors que la situation des collaborateurs avait changé (voir l'observation dans le papier de travail Z-3).

ENCADRÉ 13-17

EXEMPLE DE RISQUE DE DOUBLE PAIEMENT, TEST N° 2

X-5
Élaboré par : Jerry Coxswain
Revu par : David Richardson

Finalité du test : vérifier si des paiements potentiellement en double ont été effectués sur l'exercice précédent.

Méthode de test : étant donné que le système n'alerte l'utilisateur qu'en cas de possibilité de paiement en double, extraire 100 % des paiements relatifs à l'exercice précédent et vérifier si des paiements en double sont possibles.

Considérations relatives à l'échantillonnage : il est possible d'extraire la totalité des décaissements opérés au cours des 12 mois précédents, ce qui a été fait. À l'aide du logiciel d'audit généralisé pour lequel le service concerné détient une licence, nous avons sélectionné tous les paiements de même montant pour un fournisseur donné, indépendamment du numéro de facture ou de la date de règlement. Nous avons également examiné les paiements de même montant, indépendamment du fournisseur, pour déterminer si un vendeur avait reçu des paiements effectués sous différents noms.

Copyright © 2015 Eyrolles.

Résultats du test : après avoir analysé tous les décaissements correspondant à au moins un de nos critères, nous avons établi que les transactions suivantes constituaient des paiements en double potentiels :

Fournisseur	Numéro de facture	Date de paiement	Montant
ABC Office Supplies	8651032	21 février 20xx	2 316,50
ABC Office Supplies	8641032A	28 février 20xx	2 316,50
Alpha Printing and Binding	48637899	15 mars 20xx	125 414,22
Alpha Printing and Binding	48637899-1	15 mars 20xx	125 414,22
Alpha Printing and Binding	48637977	15 mai 20xx	86 213,47
Alpha Printing and Binding	48637977-1	31 mai 20xx	86 213,47
Alpha Printing and Binding	48638102	15 août 20xx	91 236,17
Alpha Printing and Binding	48638102*	31 août 20xx	91 236,17
Daily Shipping Services	12587	22 avril 20xx	487,95
Daily Shipping Services	12587X	22 avril 20xx	487,95
Dewey Cheatem Tax Services	489752	30 avril 20xx	19 495,00
Dewey Cheatem Tax Services	489753	30 avril 20xx	19 495,00
Dewey Cheatem Tax Services	489960	30 septembre 20xx	21 250,00
Dewey Cheatem Tax Services	489961	30 septembre 20xx	21 250,00
Newtown Catering	NC1568	14 février 20xx	685,73
Newtown Catering	NC1568A	28 février 20xx	685,73
Newtown Catering	NC1598	17 mars 20xx	443,65
Newtown Catering	NC1598A	31 mars 20xx	443,65
Newtown Catering	NC1677	4 juillet 20xx	772,43
Newtown Catering	NC1677A	31 juillet 20xx	772,43
Newtown Catering	NC1751	31 octobre 20xx	875,00
Newtown Catering	NC1751-1	30 novembre 20xx	875,00
Newtown Catering	NC1803	12 décembre 20xx	966,47
Newtown Catering	NC1804	31 décembre 20xx	966,47
Spellmen Training	667305832	18 juin 20xx	7 500,00
Spellmen Training	667305833	18 juin 20xx	7 500,00
Thompson Florists	1567	22 août 20xx	125,82
Thompson Florists	156X	31 août 20xx	125,82
Montant Total			**357 782,41**

Conclusion : il apparaît que des paiements en double sont effectués dans des cas où les factures sont présentées deux fois, soit avec des numéros légèrement différents soit avec les mêmes numéros, et la personne qui saisit la facture a ajouté un chiffre à la fin du numéro, afin d'empêcher que le système ne rejette la transaction. En conséquence, les contrôles **ne** fonctionnent **pas** toujours de manière effective (voir l'observation dans le papier de travail Z-4).

Copyright © 2015 Eyrolles.

- Les risques sous-jacents sont-ils ramenés à un niveau acceptable ?
- Globalement, la conception et le fonctionnement des contrôles clés contribuent-ils à la réalisation des objectifs pour le processus ou le domaine examiné ?

Pour répondre à ces questions, l'auditeur interne doit formuler des conclusions en s'appuyant sur les informations recueillies pendant la planification de l'audit et la réalisation des tests d'audit. Si les conclusions à rendre lui imposent, en général, de recourir largement à sa capacité de jugement, il existe par ailleurs un processus de pensée logique, qui découle des étapes décrites dans tout ce chapitre. Ces conclusions peuvent être portées sur la matrice de risques et de contrôles. Comme pour les activités précédentes, on peut partir de la matrice présentée à titre d'illustration dans l'encadré 13-14 et y ajouter une colonne pour les conclusions tirées des tests. L'encadré 13-18 en donne un exemple. Remarque : dans ce dernier, la colonne de l'encadré 13-14 relative à la méthode de test a disparu. Nous avons en effet voulu simplifier cet exemple, car cette colonne n'est pas essentielle pour la réflexion à ce stade. Cependant, lors de la conduite d'une mission d'assurance, toutes les colonnes sont nécessaires pour l'évaluation de l'adéquation de la conception et du fonctionnement effectif des contrôles clés.

ENCADRÉ 13-18

EXEMPLE DE MATRICE DE RISQUES ET DE CONTRÔLES, AVEC CONCLUSIONS TIRÉES DES TESTS

Risque au niveau du processus	Résultats des tests	Conclusions tirées des tests
Risque A – Définition (objectifs au niveau du processus)	• Résultat A • Résultat B • Résultat C	• Conclusion portant sur le risque A
Risque B – Définition (objectifs au niveau du processus)	• Résultat A • Résultat D • Résultat E	• Conclusion portant sur le risque B

Exemple Books 2 Buy. L'encadré 13-19 présente une matrice de risques et de contrôles partielle pour la fonction décaissements.

FAIRE DES OBSERVATIONS ET FORMULER DES RECOMMANDATIONS

Après avoir effectué les tests, collecté et évalué les éléments de preuve nécessaires, et tiré des conclusions, l'auditeur interne doit, pour finir, faire des observations et formuler des recommandations qui devront être communiquées à l'audité, ainsi qu'à d'autres parties prenantes à l'audit interne. Les principales composantes d'une

Copyright © 2015 Eyrolles.

ENCADRÉ 13-19

EXEMPLE DE MATRICE DE RISQUES ET DE CONTRÔLES POUR LES DÉCAISSEMENTS

Risque au niveau du processus	Résultats des tests	Conclusions tirées des tests
Risque relatif aux attentes L'absence de politiques, procédures et autres formes de communication de la direction générale bien conçues et bien articulées peut conduire des collaborateurs à exercer leurs responsabilités à l'encontre des attentes et des souhaits de la direction générale (objectifs d'exactitude, de rapidité, d'enregistrement, de conformité et d'autorisation).	• La politique de délégation de pouvoir dresse une liste de sept personnes qui ne font plus partie de l'organisation. De plus, neuf personnes qui ont pris leurs fonctions actuelles depuis peu ou qui sont arrivées récemment dans l'organisation devraient figurer sur la liste mais en sont absentes (Z-3). Toutes les autres responsabilités ont paru appropriées (papier de travail X-1). • Aucune observation ne s'est dégagée de ce test, toutes les autorisations étaient conformes à la politique de délégation de pouvoir, après prise en compte des changements à apporter à cette politique, qui sont décrits dans le papier de travail X-1 (papier de travail X-2). • D'après les discussions et observations, il semble que les procédures documentées restent appropriées, actualisées et bien comprises (papier de travail X-3).	D'après les résultats de l'échantillon sélectionné, nous pouvons conclure, avec un niveau de confiance de 90 %, que le taux d'écarts par rapport à la politique d'autorisation du management n'a pas dépassé 2,9 %, ce qui reste en deçà du taux d'écarts acceptable, situé à 5 %. Toutefois, les attentes relatives au pouvoir d'autorisation ne sont pas satisfaites, car la liste concernant la délégation de pouvoir n'est pas régulièrement actualisée pour tenir compte de l'évolution de la situation des collaborateurs (voir le papier de travail Z-3). En conséquence, ce risque n'est maîtrisé qu'en partie.
Risque de double paiement L'incapacité à identifier des saisies multiples de factures peut entraîner des paiements en double aux fournisseurs. Ces paiements risquent de ne pas être décelés ou de se révéler difficiles à recouvrer (objectifs d'exactitude et d'enregistrement).	• Le système a rejeté toutes les saisies de factures en double. En revanche, il a accepté les factures sur lesquelles un chiffre ou un symbole a été ajouté à la fin du numéro de facture, ce qui est susceptible d'entraîner un paiement en double (Z-4) (papier de travail X-4). • Quatorze (14) paiements potentiellement en double ont été identifiés, totalisant 357 782. Le management du service CF assure le suivi de tous ces éléments, qui apparaissent imputables à la déficience mentionnée dans le papier de travail X-4 (X-5). • Les transactions de test pour ce contrôle ont toutes fait l'objet d'un marquage lors du processus de décaissement. Les 14 opérations identifiées lors du test des paiements en double venaient de processus de décaissement différents et, par conséquent, n'ont pas fait l'objet d'un marquage dans le cadre de ce contrôle (papier de travail X-6).	Même si les contrôles systématiques paraissent fonctionner de manière effective, il est possible de les contourner en présentant et en saisissant un numéro de facture différent ou en ajoutant un chiffre à la fin du numéro de facture existant (voir le papier de travail Z-4). Il s'agit d'une déficience dans la conception des contrôles portant sur ce risque, ce qui, outre la déficience de conception mentionnée dans le papier de travail Z-2, indique que ce risque **n'**est **pas** maîtrisé de manière adéquate.

Copyright © 2015 Eyrolles.

Risque au niveau du processus	Résultats des tests	Conclusions tirées des tests
Risque de retard L'incapacité à traiter les paiements en temps opportun peut entraîner des amendes ou des pénalités (de retard) ou empêcher l'organisation de bénéficier de remises (objectifs de rapidité et de trésorerie).	• Le test de référence pour les trois contrôles a indiqué que ceux-ci fonctionnaient comme prévu (papiers de travail X-7, X-8 et X-9). • Il y a eu 172 paiements en retard (1,1 % du total des décaisasements). Des pénalités de retard ont été appliquées pour 21 de ces paiements. La réaction du management du service CF a permis l'annulation de ces pénalités de retard pour 9 des paiements et les pénalités payées ont totalisé 24 489 (Z-5). Aucune occasion manquée de bénéficier d'une remise n'a été identifiée (papiers de travail X-10 et X-11).	Tous les contrôles systématiques fonctionnent de manière effective. Cependant, des retards en amont dans le processus (par exemple, dans l'approbation et le traitement des factures par les acheteurs) entraînent un retard pour un nombre relativement restreint de paiements. Ces retards n'ont pas eu d'impact financier significatif (pénalités de retard). En conséquence, ce risque n'est maîtrisé qu'en partie.
Risque associé à l'accès aux systèmes – L'absence de pratiques efficaces visant la sécurité logique peut permettre à des personnes non autorisées d'accéder à des données importantes relatives aux décaissements, de les manipuler ou de les effacer (objectifs d'exactitude, d'enregistrement et de trésorerie).	• Aucune déficience de conception n'a été relevée lors des tests de la sécurité logique du SI (papier de travail X-12). • D'après la discussion et l'observation de la documentation appropriée, il apparaît que les droits d'accès sont revus de manière appropriée et en temps opportun (papier de travail X-13).	Les contrôles paraissent conçus de manière adéquate et fonctionnent de manière effective pour maîtriser ce risque.

observation bien rédigée sont analysées brièvement au chapitre 12, *Introduction au processus d'audit*. Elles sont détaillées au chapitre 14, *La communication des résultats d'une mission d'assurance et les procédures de suivi.*

Exemple Books 2 Buy. Cinq observations d'audit potentielles ont été identifiées. L'encadré 13-20 présente les principaux éléments de chacune.

Les exemples ci-dessus correspondent à la documentation que l'auditeur interne peut élaborer pendant les travaux sur place. Cependant, il peut avoir besoin d'informations supplémentaires avant d'intégrer ces observations dans une communication. Voir à ce propos le chapitre 14, qui analyse plus en détail le traitement et la communication des observations.

Copyright © 2015 Eyrolles.

ENCADRÉ 13-20

OBSERVATIONS D'AUDIT CONCERNANT LES DÉCAISSEMENTS DE BOOKS 2 BUY

Z-1

Fait : il n'y a pas de vérification auprès des utilisateurs pour déterminer si des produits ou des services ont été reçus mais n'ont pas encore été facturés.

Référentiel : tous les produits reçus dont la propriété a été transférée à l'organisation, ou les services délivrés, doivent être enregistrés dans les états financiers.

Cause : le management du service CF n'avait pas déjà considéré ou reconnu l'intérêt d'une telle vérification.

Conséquence : certains éléments de passif, et les actifs ou charges correspondants, risquent de ne pas être enregistrés lors de la clôture mensuelle, trimestrielle ou annuelle.

Z-2

Fait : le système alerte le collaborateur du service CF en cas de possibilité de facture en double, mais n'empêche pas ce collaborateur de continuer à traiter de telles factures.

Référentiel : la réception de biens et services ne doit être comptabilisée et traitée qu'une fois.

Cause : le système a été codé de façon à envoyer un rappel à l'utilisateur, et non à empêcher celui-ci de saisir une facture une nouvelle fois si les circonstances le justifient.

Conséquence : des éléments de passif, et les actifs ou charges correspondants, risquent d'être surévalués et des fonds indûment décaissés.

Z-3

Fait : la politique de délégation de pouvoir dresse une liste de sept personnes qui ne font plus partie de l'organisation. De plus, neuf personnes qui ont pris leurs fonctions actuelles depuis peu ou qui sont arrivées récemment dans l'organisation devraient figurer sur la liste mais en sont absentes.

Référentiel : le pouvoir de décaissement de fonds ne doit être délégué qu'aux personnes dont les responsabilités le justifient.

Cause : la politique de délégation de pouvoir est actualisée deux fois par an, et non à chaque fois qu'un changement intervient dans les effectifs ou dans les responsabilités des personnes autorisées.

Conséquence : certains décaissements risquent de ne pas être conformes aux orientations données par le management.

Z-4

Fait : le système a rejeté toutes les saisies de factures en double. En revanche, il a accepté les factures sur lesquelles un chiffre ou un symbole a été ajouté à la fin du numéro de facture, ce qui est susceptible d'entraîner un paiement en double.

Référentiel : la réception de biens et services ne doit être comptabilisée et traitée qu'une fois.

Cause : dans certains cas, il apparaît que les collaborateurs du service CF saisissent certaines factures une seconde fois, lorsqu'elles sont envoyées par le fournisseur. Ils ne s'aperçoivent pas que ces factures ont peut-être déjà été reçues et, étant donné la déficience dans la conception des contrôles décrite dans Z-3, ils ajoutent un chiffre à la fin des factures, de manière à en faciliter le traitement. Dans d'autres cas, le fournisseur a émis un duplicata de facture qui porte un numéro différent (généralement supérieur au précédent) et les collaborateurs du service CF ne se sont pas aperçus qu'il pouvait s'agir d'une facture en double.

Conséquence : les éléments de passif, et les actifs ou charges correspondants, ont été surévalués de 357 782,41 et le même montant a été indûment décaissé.

Z-5

Fait : il y a eu 172 paiements en retard (1,1 % du total des décaissements). Des pénalités de retard ont été appliquées pour 21 de ces paiements. La réaction du management du service CF a permis l'annulation de ces pénalités de retard pour 9 des paiements et les pénalités payées ont totalisé 24 489 (Z-5).

Référentiel : les paiements doivent être effectués en temps opportun, conformément aux attentes du management afin d'éviter les pénalités de retard.

Cause : pour diverses raisons, les factures n'ont pas été autorisées en temps opportun dans 19 des 21 cas. En conséquence, les paiements ont été effectués en retard par rapport aux délais de traitement des décaissements. Dans les deux autres cas, les retards ont résulté de la décision du management de ne pas payer jusqu'à ce qu'un différend avec le fournisseur ait pu être résolu.

Conséquence : l'organisation a dû payer au total 24 489 de pénalités de retard.

Copyright © 2015 Eyrolles.

OPPORTUNITÉS POUR UN POINT DE VUE DE L'AUDIT INTERNE

L'audit interne a la possibilité de créer de la valeur ajoutée en apportant son point de vue sur le déroulement de la mission d'assurance. L'encadré 13-21 présente 10 opportunités pour l'audit interne d'apporter son point de vue en réalisant des missions d'assurance.

APPORTER SON POINT DE VUE LORS DE LA RÉALISATION D'UNE MISSION D'AUDIT 10 OPPORTUNITÉS POUR L'AUDIT INTERNE

- Permettre une discussion autour des objectifs clés de l'audité pour garantir une compréhension commune de l'ensemble des collaborateurs dans ce domaine.
- Partager la documentation des processus (diagrammes de flux…) élaborée au cours de l'audit afin que l'audité puisse s'en servir comme support de formation.
- Partager les résultats de l'analyse des données, y compris les tableurs ou les outils élaborés qui pourront être réutilisés par l'audité.
- Donner des conseils sur le caractère exhaustif et suffisant des indicateurs clés de performance pour aider le management de l'audité à mieux piloter les performances.
- Partager des points de vue sur les risques de fraude au niveau des processus et donner des conseils sur les meilleurs moyens de prévenir, empêcher ou détecter les potentiels actes frauduleux.
- Évoquer les risques identifiés au niveau des processus pour s'assurer que l'audité en a tenu compte dans sa conception des contrôles et des procédures.
- Partager l'évaluation de ces risques réalisée par l'équipe d'audit interne, pour garantir l'alignement sur le niveau inhérent de chaque risque.
- Discuter avec le management de son seuil de tolérance au risque au niveau des processus et lui signaler, le cas échéant, les domaines où il accepte un risque trop élevé ou, au contraire, trop peu élevé.
- Partager l'évaluation de la conception des contrôles réalisée par l'équipe d'audit interne et parvenir à un accord sur le caractère acceptable de l'adéquation de la conception.
- Partager l'évaluation de l'exécution des contrôles réalisée par l'équipe d'audit interne et parvenir à un accord sur le caractère acceptable du fonctionnement effectif.

ENCADRÉ 13-21

Fonctionnement effectif

Caractéristique des activités de contrôle permettant d'affirmer que le management les a exécutées (opérées) de manière à donner l'assurance raisonnable que les risques sont gérés efficacement et que les buts et les objectifs de l'organisation seront atteints de manière efficiente et économique.

RÉSUMÉ

Le chapitre 12 évoquait une expression parfois utilisée en anglais, les « *six P* » : *Proper Prior Planning Prevents Poor Performance*. Cette expression signifie qu'il est primordial de bien planifier les missions pour en assurer le succès. Le temps préalable consacré à la phase de planification produira ultérieurement d'importants effets bénéfiques, ce qui contribue à une réalisation efficiente, efficace et complète de l'ensemble de l'audit.

Copyright © 2015 Eyrolles.

La première phase d'une mission d'assurance est la planification, qui se compose des grandes étapes suivantes.

- **Déterminer les objectifs et le périmètre de la mission.** Chaque mission d'assurance diffère légèrement des autres, en fonction de ce qui la justifie et des résultats finaux souhaités. Il faut tout d'abord définir les objectifs de la mission et délimiter le périmètre de celle-ci en termes de calendrier, zone géographique et procédures.
- **Connaître l'audité (notamment ses objectifs).** Pour mener sa mission avec efficacité, l'auditeur doit en premier lieu comprendre les objectifs de l'audité, les tâches effectuées dans le domaine examiné qui visent à atteindre ces objectifs, ainsi que les mécanismes de pilotage des performances et de mesure de la réussite.
- **Identifier et évaluer les risques.** Il faut identifier et évaluer les événements ou scénarios spécifiques qui pourraient empêcher la réalisation des objectifs de l'audité. Cette évaluation impose généralement d'estimer l'impact et la probabilité de concrétisation des scénarios de risque.
- **Identifier les contrôles clés.** Les contrôles clés sont les contrôles qui, individuellement ou conjointement avec d'autres, ramènent le risque de l'audité à un niveau acceptable. Il se peut que l'audité mette en œuvre de nombreux contrôles différents, mais les contrôles clés sont ceux qui font vraiment partie intégrante de la réalisation des objectifs.
- **Évaluer l'adéquation de la conception des contrôles.** La première évaluation fondamentale porte sur l'adéquation de la conception des contrôles. Elle impose à l'auditeur interne de déterminer si les contrôles, fonctionnant de manière effective, permettront de maîtriser les risques susceptibles d'empêcher la réalisation des objectifs.
- **Établir un plan des tests.** Le plan des tests définit la manière dont les contrôles clés seront testés, afin d'aider l'auditeur interne à en évaluer le fonctionnement effectif. Les tests doivent également être liés aux risques sous-jacents, afin que toute déficience éventuelle qu'ils décèleraient puisse être évaluée au regard de son impact sur la maîtrise des risques.
- **Élaborer un programme de travail.** Un programme de travail formel présente les principales activités du processus d'audit et tout jugement formulé concernant les objectifs et le périmètre de la mission.
- **Allouer des ressources à la mission.** En se fondant sur les activités à réaliser au cours d'une mission, l'auditeur doit identifier et désigner les collaborateurs qui correspondent au niveau d'expérience et de compétence approprié, afin que la mission puisse être menée rapidement et avec efficacité.

Copyright © 2015 Eyrolles.

La planification d'une mission ne se cantonne pas à la mise en œuvre des étapes décrites ci-dessus. Elle impose également de documenter efficacement les informations obtenues et les jugements formulés. La documentation produite durant la phase de planification peut revêtir différents formalismes, mais se compose habituellement des éléments suivants :

- un mémoire de planification ou une checklist relative à la planification, documentant la méthode d'audit et les jugements formulés ;
- des diagrammes de flux ou des notes narratives des principaux flux des processus ;
- une cartographie des risques, illustrant les jugements formulés concernant les risques au niveau des processus ;
- une matrice de risques et de contrôles, présentant les interactions entre les risques, les contrôles, la méthode de test, les résultats des tests et les conclusions tirées des tests.

La phase suivante d'une mission d'assurance consiste à effectuer les tests définis lors de la planification et à en évaluer les résultats. Plus précisément, l'auditeur interne doit passer par un certain nombre d'étapes.

- **Réaliser des tests pour collecter des preuves.** Il s'agit d'effectuer chacun des tests définis au cours de la phase de planification. L'auditeur interne doit réunir et documenter des preuves suffisantes et adéquates pour étayer ses conclusions sur le fonctionnement effectif des contrôles.
- **Évaluer les preuves rassemblées et en tirer des conclusions.** L'auditeur interne doit examiner l'évaluation initiale de la conception des contrôles, ainsi que les résultats des tests, et conclure si les risques sous-jacents sont ramenés à un niveau acceptable.
- **Faire des observations et formuler des recommandations.** Pour terminer, toute déficience des contrôles décelée au cours de la mission doit être documentée, de manière à faciliter la discussion avec le niveau de management approprié et, *in fine*, la communication des observations aux parties prenantes concernées.

L'élaboration d'une matrice de risques et de contrôles constitue un moyen efficace de documenter les nombreux jugements formulés et les résultats des tests réalisés pendant la mission d'assurance. L'encadré 13-22 présente un exemple de matrice complète.

Observation

Conclusion, déduction ou jugement découlant des résultats de tests effectués par l'auditeur interne. Également appelé constat ou constatation.

Copyright © 2015 Eyrolles.

ENCADRÉ 13-22

MATRICE DE RISQUES ET DE CONTRÔLES

Risque au niveau du processus	Contrôle clé	Adéquation de la conception	Méthode de test	Résultats des tests	Conclusions tirées des tests
Risque A – Définition (objectifs au niveau du processus)	• Contrôle A • Contrôle B • Contrôle C	Les contrôles clés mentionnés sont conçus de manière adéquate pour ramener ce risque à un niveau acceptable.	• Test A • Test B • Test C	• Résultat A • Résultat B • Résultat C	Conclusion portant sur le risque A
Risque B – Définition (objectifs au niveau du processus)	• Contrôle A • Contrôle D	Les contrôles clés mentionnés ne sont pas conçus de manière adéquate pour ramener ce risque à un niveau acceptable (décrire la faiblesse de conception).	• Test A • Test D • Test E	• Résultat A • Résultat D • Résultat E	Conclusion portant sur le risque B
Risque C – Définition (objectifs au niveau du processus)	• Contrôle C • Contrôle E • Contrôle F	Les contrôles clés mentionnés sont conçus de manière adéquate pour ramener ce risque à un niveau acceptable.	• Test F • Test G • Test H	• Résultat F • Résultat G • Résultat H	Conclusion portant sur le risque C

Copyright © 2015 Eyrolles.

Questions de révision

1. Quelles sont les quatre raisons pouvant motiver la réalisation d'une mission d'assurance ?

2. Pourquoi est-il important de définir les objectifs de la mission ?

3. Quels sont les cinq types d'énoncés du périmètre d'une mission ?

4. Quelles sont les cinq exceptions classiques que l'on peut identifier au cours d'une mission ?

5. Quel type d'objectif est le plus fréquent pour un processus, et pourquoi ?

6. De quels types d'informations les propriétaires de processus peuvent-ils disposer qui aideront l'auditeur interne à comprendre le processus ?

7. À quelle fin un auditeur interne pourrait-il vouloir effectuer des procédures analytiques au cours du processus de planification de la mission ?

8. À quelle fin un auditeur interne pourrait-il vouloir utiliser des outils informatiques d'aide à l'audit au cours du processus de planification de la mission ?

9. Pourquoi un auditeur interne doit-il comprendre comment les contrôles à l'échelle de l'entité peuvent influer sur les performances d'un processus avant d'auditer celui-ci ?

10. Quels sont les trois moyens les plus courants de documenter un flux de processus ?

11. Quelle est la différence entre un diagramme de flux détaillé et un diagramme de flux macro ?

12. Quels sont les six types d'information que devraient contenir les notes narratives ?

13. Pourquoi est-il important que les auditeurs internes repèrent et comprennent bien les indicateurs clés de performance d'un processus ?

14. Pourquoi la probabilité inhérente d'un risque pourrait-elle augmenter s'il existe un potentiel de fraude ?

15. Quelle est la différence entre un scénario de risque au niveau d'un processus et un risque au niveau d'un processus ?

16. Quelles sont les trois étapes généralement à suivre pour réaliser une évaluation des risques au niveau des processus ?

Copyright © 2015 Eyrolles.



Questions de révision

17. Quelles sont les trois grandes étapes qu'un auditeur interne doit suivre lorsqu'il cherche à comprendre les seuils de tolérance au risque du management ?

18. Parmi les neuf exemples de types de contrôles courants, lesquels interviennent généralement avant l'achèvement d'une transaction ?

19. Quelles sont les questions essentielles auxquelles il faut répondre lorsque l'on évalue l'adéquation de la conception des contrôles ?

20. Quels facteurs un auditeur interne devrait-il prendre en compte pour déterminer les contrôles à tester ?

21. Lorsque l'on met au point une méthode de test, quelles décisions faut-il prendre concernant les tests à effectuer ?

22. Quelles sont les principales activités d'un programme de travail type ?

23. Quelles informations le budget d'une mission d'audit interne devrait-il contenir ?

24. Quelles sont les questions à se poser lors de l'allocation des ressources humaines à une mission ?

25. Quels sont les quatre éléments à prendre en compte lorsque l'on programme une mission ?

26. Quelles sont les quatre questions auxquelles il faut répondre pour évaluer les preuves que les tests d'audit ont permis de recueillir ?

27. Quels sont les quatre éléments que doit contenir une observation d'audit bien rédigée ?

28. Quelles sont les six colonnes d'une matrice de risques et de contrôles complète ?

Copyright © 2015 Eyrolles.

Questions à choix multiples

Sélectionnez la meilleure réponse pour chacune des questions suivantes.

1. Lequel des objectifs suivants n'est pas susceptible de figurer parmi ceux d'une mission d'assurance ?
   a. Évaluer l'adéquation de la conception du processus de saisie des rémunérations.
   b. Garantir l'exactitude des soldes d'inventaire.
   c. Évaluer la conformité aux lois et règlements relatifs à l'hygiène et à la sécurité.
   d. Déterminer le fonctionnement effectif des contrôles portant sur les immobilisations corporelles.

2. Un objectif de processus est formulé comme suit : « Tous les contrats doivent bénéficier de l'aval d'un responsable de l'organisation avant d'être appliqués ». De quel type d'objectif constitue-t-il un exemple ?
   a. Objectif lié à la stratégie.
   b. Objectif lié aux opérations.
   c. Objectif lié au reporting.
   d. Objectif lié à la conformité.

3. Durant quelle(s) phase(s) d'une mission d'assurance peut-on appliquer des procédures analytiques ?
   a. La phase de planification.
   b. La phase d'exécution.
   c. La phase de communication.
   d. Les phases de planification et d'exécution.

4. Lequel des documents suivants élaborés par l'audité aidera probablement le plus l'auditeur interne à évaluer l'adéquation de la conception d'un processus ?
   a. Le manuel des règles et des procédures.
   b. Les organigrammes et les descriptifs de postes.
   c. Les diagrammes détaillés décrivant les flux du processus.
   d. Les notes narratives énumérant les activités relatives au processus.

5. Lequel des contrôles suivants ne constitue vraisemblablement pas un contrôle à l'échelle de l'entité ?
   a. Tous les collaborateurs doivent recevoir une formation continue afin que leur niveau de compétence soit préservé.
   b. Toutes les transactions de décaissement doivent être approuvées avant d'être effectuées.

Copyright © 2015 Eyrolles.

c. Tous les collaborateurs doivent se conformer au Code de déontologie/Charte de bonne conduite.
d. Une évaluation du risque est menée chaque année à l'échelle de l'organisation.

6. Lequel des éléments suivants n'est généralement pas une composante essentielle des diagrammes de flux ou des notes narratives ?
   a. Les objectifs globaux du processus.
   b. Les principales données d'entrée du processus.
   c. Les principales données de sortie du processus.
   d. Les risques principaux et contrôles clés.

7. Lequel des risques externes suivants est le moins susceptible d'influer sur l'exactitude du reporting financier ?
   a. Dans le pays où est sise l'organisation, l'organisme de normalisation publie une nouvelle norme de comptabilité financière.
   b. Une récente décision de justice accroît la probabilité d'une issue défavorable pour une affaire en cours.
   c. La révision des contrats-cadres sectoriels autorise désormais la compensation des comptes fournisseurs et clients.
   d. Les pressions exercées par la concurrence obligent l'organisation à trouver de nouveaux débouchés.

8. Parmi les catégories suivantes, quelles sont celles dont le seuil de tolérance au risque a le moins de pertinence lors d'une mission d'audit ?
   a. La direction générale.
   b. Les responsables du processus.
   c. L'audit interne.
   d. Les fournisseurs et clients.

9. Parmi les contrôles suivants, lequel est susceptible d'être le moins pertinent lors de l'évaluation de l'adéquation de la conception d'un processus d'encaissement ?
   a. Le calcul du montant des encaissements reçus.
   b. La justification du choix du compte bancaire qui recevra le dépôt.
   c. Le rapprochement du total des dépôts avec les montants crédités sur les soldes des comptes clients.
   d. La séparation entre l'établissement des bordereaux de dépôt et l'ajustement des soldes des comptes clients.

Copyright © 2015 Eyrolles.

Questions à choix multiples

10. Un auditeur interne établit que le processus n'est pas conçu de manière adéquate pour ramener les risques sous-jacents à un niveau acceptable. Que doit-il faire ensuite ?
    a. Rédiger le rapport d'audit, car il n'y a pas lieu de tester le fonctionnement effectif de contrôles qui ne sont pas conçus de manière adéquate.
    b. Tester les contrôles portant sur d'autres processus (adjacents), qui pourraient être compensatoires, afin de déterminer si les effets de l'inadéquation de la conception sont ramenés à un niveau acceptable.
    c. Tester quand même les contrôles clés existants, pour prouver que, malgré l'inadéquation de sa conception, le processus satisfait à ses objectifs.
    d. Différer la mission jusqu'à ce que l'inadéquation de la conception ait été corrigée.

11. Si un auditeur interne identifie une anomalie lors d'un test, laquelle des attitudes suivantes pourra être appropriée ?
    a. Tester des éléments supplémentaires afin de déterminer si l'anomalie est un cas isolé ou si elle est le signe d'une déficience du contrôle.
    b. Chercher à en comprendre les causes profondes, c'est-à-dire la raison pour laquelle cette anomalie s'est produite.
    c. Rédiger une observation destinée au rapport d'audit.
    d. Toutes les réponses ci-dessus.

12. Parmi les énoncés suivants, lequel est une conclusion appropriée que peut tirer l'auditeur interne lorsque les tests des contrôles lui permettent de dégager une observation ?
    a. Les objectifs au niveau du processus ne peuvent pas être réalisés.
    b. Il existe un risque de fraude dans le domaine audité.
    c. Certains risques ne sont pas maîtrisés efficacement.
    d. Globalement, le processus ne fonctionne pas de manière effective.

13. Une observation dégagée par l'auditeur interne doit :
    a. Être documentée dans les papiers de travail.
    b. Être discutée avec le comité d'audit.
    c. Être incluse dans le rapport d'audit final.
    d. Donner lieu à la planification d'un suivi.

Copyright © 2015 Eyrolles.

Thèmes de discussion

1. Pourquoi est-il si important de « commencer en gardant à l'esprit la fin » lorsque l'on planifie une mission d'assurance ?

2. Le COSO définit les objectifs stratégiques d'une organisation comme étant des objectifs de haut niveau correspondant à la mission de l'organisation et la soutenant. Étant donné cette définition, comment un processus administratif, orienté sur des activités spécifiques, peut-il tendre vers des objectifs stratégiques ?

3. Le management a tendance à se concentrer sur le risque résiduel au lieu du risque inhérent. D'après vous, pourquoi ? Pourquoi les auditeurs internes prennent-ils en compte à la fois le risque inhérent et le risque résiduel lorsqu'ils planifient une mission d'assurance ?

4. Si l'auditeur interne ne parvient pas à identifier la totalité des principaux risques au niveau des processus, quel peut en être l'impact sur l'ensemble de la mission d'assurance ? Si l'audit interne qualifie certains risques au niveau des processus d'essentiels alors qu'ils ne le sont pas, quel impact est-ce que cela pourrait avoir sur l'ensemble de la mission d'assurance ?

5. Outre l'incidence sur le reporting financier, quels types de répercussions doivent être pris en compte lors de l'évaluation de l'impact des risques ?

6. Anticipant une mission à venir, une équipe d'audit interne a récemment visité les bâtiments de réception, de stockage et de production de son organisation afin de mieux en comprendre les activités quotidiennes. Ce faisant, l'équipe a pris note de plusieurs éléments :
   - une grande quantité de matériaux était déposée dans un coin, près du quai de déchargement. Le manager de la réception a informé l'équipe d'audit que les camions de livraison étaient déjà partis. Ces matériaux n'avaient pas encore été comptés ni inspectés ;
   - une section de l'entrepôt contenait de grandes quantités d'articles munis de fiches de relevés d'inventaire venant de plusieurs comptes de stock physiques. Le manager du stock a affirmé à l'équipe d'audit que c'était le stock de pièces détachées de l'organisation, dont la loi prévoit qu'elles doivent rester à portée de main pendant une période donnée ;
   - des produits chimiques dangereux sont utilisés dans le processus de finissage. Les déchets chimiques sont stockés dans de grands contenants en plastique dans une zone de l'usine réservée à cet effet, avant d'être expédiés pour élimination.

Copyright © 2015 Eyrolles.

Pour chaque point relevé par l'équipe d'audit interne :

a. décrivez le(s) risque(s) opérationnel(s) potentiel(s) associé(s) ;

b. indiquez comment les connaissances qu'ont les auditeurs internes des risques identifiés sont susceptibles d'influer, par la suite, sur l'audit des acquisitions de matériel et des processus de production[2].

7. AVF Inc. fabrique plusieurs lignes de matériel de conditionnement. L'organisation estime que la fiabilité du produit et la qualité du service à la clientèle sont essentielles à sa réussite. Le service client est chargé de :

- fournir aux clients potentiels des informations sur les produits ;
- surveiller la disponibilité des pièces de rechange ;
- procurer aux clients des renseignements sur le fonctionnement et la maintenance du matériel ;
- concevoir et dispenser des cours de formation pour les clients ;
- répondre aux plaintes des clients et appeler le service des réparations ;
- gérer les réclamations au titre de la garantie ;
- maintenir de bonnes relations avec la clientèle.

Dernièrement, l'organisation a beaucoup investi pour mettre à jour le système informatique du service client. Cette mise à jour est supposée améliorer le fonctionnement effectif et la satisfaction de la clientèle. Ce nouveau système produit notamment des rapports de gestion permettant de suivre les performances dans les domaines mentionnés ci-dessus. Le comité d'audit demande à l'audit interne de vérifier le fonctionnement effectif et l'efficience du service client. Cette mission porte sur les aspects suivants :

- sécurité des actifs, y compris de l'information ;
- conformité aux lois en vigueur et aux politiques de l'organisation ;
- fiabilité des registres financiers ;
- efficacité dans l'accomplissement des responsabilités assignées ;
- évaluation du stock de pièces détachées.

a. Expliquez pourquoi chacun des cinq domaines spécifiés peut ou non être approprié pour cette mission d'assurance.

b. Identifiez trois autres aspects du service client qui peuvent requérir l'attention de l'auditeur interne.

c. Indiquez quelles tâches les auditeurs internes doivent effectuer en premier lieu pour évaluer le fonctionnement effectif et l'efficience du service client afin de vérifier s'il assume bien les responsabilités suivantes :

- concevoir et dispenser des cours de formation pour les clients ;
- répondre aux plaintes des clients et appeler le service réparations ;
- gérer les réclamations au titre de la garantie[3].

Copyright © 2015 Eyrolles.

8. Un auditeur de l'équipe d'audit interne constate les possibles écarts suivants par rapport aux contrôles imposés et les consigne dans ses papiers de travail.

Numéro de facture	Contrôle prescrit	Écart possible
248	Autorisations écrites émises par le service commercial.	Autorisation orale donnée par téléphone par le service commercial.
333	Vérification des quantités et prix sur les bons de commande.	Aucune preuve de vérification ; quantités et prix incorrects.
377	Vérification des quantités et prix sur les bons de commande.	Aucune preuve de vérification, mais les quantités et prix sont corrects.
617	Vérification des prix unitaires par le service facturation.	La vérification des prix est signalée sur la facture ; grâce à une reprise des calculs, vous pouvez certifier que les prix ne concordent pas avec la grille tarifaire en vigueur au moment de la vente.

Pour chaque élément énuméré ci-dessus, indiquez s'il existe ou non un écart par rapport à l'activité prescrite. Expliquez brièvement votre réponse[4].

9. Selon le cadre de référence relatif au management des risques de l'entreprise élaboré par le COSO, les objectifs stratégiques constituent l'une des quatre catégories d'objectifs. Si l'on suppose que certains objectifs stratégiques sont essentiels à la réussite d'une organisation, qu'est-ce que l'audit interne doit envisager lorsqu'il détermine s'il doit mener des missions relatives à ces objectifs ? Quels sont, selon vous, les objectifs de la mission d'assurance qui seraient appropriés et ceux qui ne le seraient pas ?

Copyright © 2015 Eyrolles.

ÉTUDE DE CAS

Vous êtes l'auditeur interne senior chargé de conduire une mission d'assurance portant sur le processus de la paie chez XYZ. Ce processus n'a pas été audité depuis trois ans et est inscrit dans le cycle d'audit normal. Depuis le dernier audit, il n'y a pas eu de changements majeurs dans le système, ni de réorganisation du service, ni de révision substantielle des procédures. Cependant, au cours de sa dernière mission d'assurance, l'audit interne a dégagé plusieurs observations, dont certaines peuvent être considérées comme significatives :

- les informations relatives aux collaborateurs qui ont quitté l'organisation n'ont pas été communiquées au service informatique, de sorte que les droits d'accès de ces anciens collaborateurs n'ont été résiliés que très longtemps après le départ de ces collaborateurs ;
- aucun relevé de temps validé n'a été présenté pour justifier les heures payées aux collaborateurs dont les heures supplémentaires sont rémunérées ;
- les retenues à la source ne correspondaient pas aux choix opérés par les collaborateurs ;
- il est possible que des collaborateurs « fantômes » aient été inclus dans la masse salariale sans que cela ait été décelé.

Le management de la paie a mis en œuvre des mesures pour réagir à toutes les observations significatives, et l'audit interne a appliqué des procédures de suivi pour confirmer l'application de ces mesures. C'est le premier audit depuis l'introduction de ce suivi.

Voici des informations pertinentes relatives à cette mission d'assurance portant sur la paie.

- XYZ emploie environ 4 400 personnes. Sur ce total, quelque 2 700 sont salariées et les autres sont rémunérées à l'heure.
- La rémunération est versée sur une base bihebdomadaire.
- Les collaborateurs rémunérés à l'heure sont payés au taux standard pour les 80 premières heures d'une période de rémunération bihebdomadaire, une fois et demie ce taux pour les 20 heures suivantes et le double pour toute heure dépassant les 100 heures effectuées sur la période de rémunération.
- L'organisation recourt à un logiciel de paie couramment utilisé et testé sur le marché pour traiter toutes les opérations relatives à la paie.
- Ce système de paie est doté d'une interface avec le système du grand livre général.
- XYZ a créé un compte bancaire de contrôle de la paie distinct pour le traitement des chèques de paie. Les montants sont déposés sur ce compte à partir du compte général de l'organisation, ce qui permet d'honorer *via* ce compte tout chèque présenté chaque jour.

Copyright © 2015 Eyrolles.

ÉTUDE DE CAS

- Un certain nombre d'éléments non liés à la paie sont retranchés du montant des chèques de paie, notamment :
  - les prêts aux collaborateurs, destinés à couvrir le coût de prestations supplémentaires ou à financer l'achat d'ordinateurs ;
  - les cotisations aux régimes de retraite à long terme ;
  - les dons à des organisations caritatives, telles que United Way ;
  - les contributions à des comités d'action politique (PAC).
- Les charges de personnel et les charges salariales connexes à payer sont considérées comme élevées pour l'organisation.

En vous appuyant sur les informations ci-dessus, mettez en œuvre les étapes suivantes pour conduire une mission d'assurance portant sur la paie.

A. Déterminez au moins quatre objectifs du service de la paie qui seraient pertinents pour cette mission.

B. Dressez une liste des scénarios de risque potentiel pour chaque objectif.

C. En vous fondant sur ces scénarios de risque, définissez et évaluez les risques principaux afférents à la paie.
   1. Pour cette évaluation, vous devrez formuler des hypothèses concernant l'impact et la probabilité d'occurrence. Documentez ces hypothèses.
   2. Formulez également des hypothèses sur les seuils de tolérance au risque des responsables du processus.

D. Documentez les flux potentiels du processus, sous la forme d'un diagramme de flux détaillé. Assurez-vous que celui-ci fait apparaître les risques principaux et les contrôles clés, et comporte au moins une inadéquation dans la conception.

E. Élaborez des indicateurs clés de performance potentiels pour le processus documenté en D.

F. Déterminez quels contrôles sont considérés comme clés. Dans le cadre de cette analyse, consignez par écrit vos hypothèses concernant l'efficacité des contrôles à l'échelle de l'entité, et la manière dont ces contrôles influencent, le cas échéant, ceux au niveau du processus de paie.

G. Mettez en relation les contrôles clés et les risques identifiés.

H. Établissez une matrice de risques et de contrôles pour traiter les informations appropriées recueillies depuis l'étape D jusqu'à l'étape G. Tirez-en une conclusion sur l'adéquation globale de la conception du processus de paie.

Copyright © 2015 Eyrolles.



I. Constituez un plan des tests pour rassembler des preuves sur le fonctionnement effectif des contrôles clés.

J. Définissez des résultats potentiels pour tous les tests. Veillez à identifier au moins deux observations portant sur le fonctionnement effectif de tous les contrôles clés.

K. Ajoutez les résultats des étapes I et J ci-dessus à la matrice de risques et de contrôles. Consignez par écrit vos conclusions quant à l'efficacité des contrôles.

L. Formulez des observations d'après les résultats de la mission qui énoncent, pour chaque observation, le fait, le référentiel, la cause et la conséquence.

Copyright © 2015 Eyrolles.


Copyright © 2015 Eyrolles.

CHAPITRE 14
LA COMMUNICATION DES RÉSULTATS D'UNE MISSION D'ASSURANCE ET LES PROCÉDURES DE SUIVI

Objectifs pédagogiques

- Comprendre pourquoi il est approprié et nécessaire de communiquer les résultats d'une mission d'assurance.
- Connaître les différentes formes de communication des résultats d'une mission d'assurance.
- Identifier les étapes permettant la communication efficace des résultats d'une mission d'assurance.
- Comprendre le processus de diffusion permettant de communiquer efficacement les résultats d'une mission d'assurance.
- Comprendre quels sont les éléments qui interviennent dans la surveillance et le suivi des résultats d'une mission d'assurance.

Le chapitre 12, *Introduction au processus d'audit*, donne une vue d'ensemble du déroulement des missions d'assurance, décomposé en trois phases fondamentales : planification, exécution et communication. Le chapitre 13, *Le déroulement de la mission d'assurance*, détaille les deux premières étapes (planification et exécution). L'encadré 14-2 reprend les composantes de chacune de ces trois phases. Dans ce chapitre, nous nous concentrerons sur l'étape relative à la communication.

Nous commencerons par souligner pourquoi il est approprié et nécessaire de communiquer les résultats d'une mission. Nous présenterons les différentes formes de communication employées pour diffuser les résultats d'une mission d'assurance et préciserons la finalité de chacune. Nous dégagerons également les différentes étapes qui permettent la création d'une communication adéquate pour la mission effectuée, ainsi que le processus de diffusion visant à communiquer efficacement les résultats des missions d'assurance. Enfin, nous identifierons les différentes étapes nécessaires à la surveillance et aux procédures de suivi des résultats de la mission qui ont été communiqués.

Parce que beaucoup de rapports de missions concernent l'adéquation de la conception et le fonctionnement effectif des contrôles, le référentiel du *Committee of Sponsoring Organizations of the Treadway Commission* (COSO), intitulé

Copyright © 2015 Eyrolles.

« Référentiel intégré de contrôle interne – Principes de mise en œuvre et de pilotage » (le *Référentiel*), servira de base à l'étude du processus de communication des résultats des missions, comme dans le chapitre 6, *Le contrôle interne*. Il importe cependant de noter que de nombreuses missions d'assurance sont effectuées dans le but d'obtenir une appréciation ou une évaluation des contrôles, ciblant des aspects plus restreints que l'appréciation globale des contrôles d'un processus opérationnel ou d'un domaine (exactitude de soldes de comptes, conformité à certaines réglementations ou règles et procédures opérationnelles, réalisation de certains objectifs de l'organisation en question…). Dans ce cas, les communications correspondantes se concentreront sur le retour d'informations indépendant, fourni au management, concernant l'évaluation de ces aspects. Le contenu de ces communications pourra quelque peu s'écarter des exemples présentés tout au long de ce chapitre, mais les concepts, méthodes et approches décrits n'en demeurent pas moins applicables.

ENCADRÉ 14-1

DISPOSITIONS DU CRIPP PERTINENTES RELATIVES AU CHAPITRE 14

Norme 2330 – Documentation des informations
Norme 2400 – Communication des résultats
Norme 2410 – Contenu de la communication
Norme 2420 – Qualité de la communication
Norme 2421 – Erreurs et omissions
Norme 2430 – Utilisation de la mention « conduit conformément aux *Normes internationales pour la pratique professionnelle de l'audit interne* »
Norme 2440 – Diffusion des résultats
Norme 2500 – Surveillance des actions de progrès
Norme 2600 – Communication relative à l'acceptation des risques

Modalité Pratique d'Application 2060-1 :	Rapports à la direction générale et au Conseil
Modalité Pratique d'Application 2320-2 :	Analyse causale
Modalité Pratique d'Application 2330-1 :	Documentation des informations
Modalité Pratique d'Application 2330.A1-1 :	Contrôle des dossiers d'audit
Modalité Pratique d'Application 2400-1 :	Aspects légaux de la communication des résultats
Modalité Pratique d'Application 2410-1 :	Contenu de la communication
Modalité Pratique d'Application 2420-1 :	Qualité de la communication
Modalité Pratique d'Application 2440-1 :	Diffusion des résultats de la mission
Modalité Pratique d'Application 2440-2 :	Communication d'informations sensibles dans ou en dehors de la ligne hiérarchique
Modalité Pratique d'Application 2440.A2-1 :	Diffusion des résultats d'audit en dehors de l'organisation
Modalité Pratique d'Application 2500-1 :	Surveillance des actions de progrès
Modalité Pratique d'Application 2500.A1-1 :	Processus de suivi de la mission

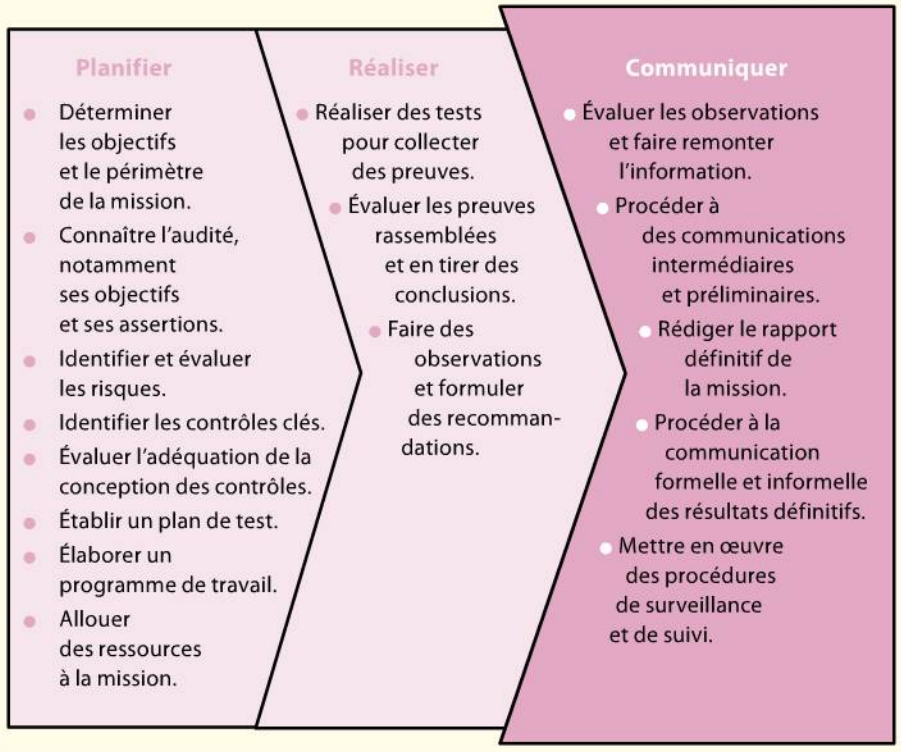
Copyright © 2015 Eyrolles.

L'OBLIGATION DE COMMUNICATION DES RÉSULTATS D'UNE MISSION

Comme détaillé dans le chapitre 9, *La gestion de l'audit interne*, le responsable de l'audit interne doit « rendre compte périodiquement à la direction générale et au Conseil des missions, des pouvoirs et des responsabilités de l'audit interne, ainsi que du degré de réalisation du plan d'audit. Il doit plus particulièrement rendre compte de l'exposition aux risques significatifs (y compris des risques de fraude) et des contrôles correspondants ; des sujets relatifs au gouvernement d'entreprise ; et de tout autre problème répondant à un besoin ou à une demande de la direction générale ou du Conseil » (Norme 2060, Rapports à la direction générale et au Conseil). Le responsable de l'audit interne démontre que le service s'est acquitté de ses responsabilités professionnelles en communiquant notamment périodiquement les résultats des missions d'assurance à la direction générale et au comité d'audit à l'occasion des réunions programmées régulièrement tout au long de l'année.

LE DÉROULEMENT DE LA MISSION D'ASSURANCE

ENCADRÉ 14-2



Les missions d'assurance doivent notamment donner le résultat de l'évaluation indépendante effectuée par l'audit interne sur l'efficacité de la stratégie de maîtrise des risques qui pèsent sur l'organisation. Considérées ensemble, ces différentes évaluations contribuent

Copyright © 2015 Eyrolles.

à corroborer et à étayer les critères de qualité retenus par la direction générale, à savoir que le système de contrôle interne de l'organisation est conçu de manière adéquate et fonctionne de manière effective. Ceci illustre en quoi la fonction d'audit interne constitue un niveau d'assurance dans le modèle des trois lignes de maîtrise présenté dans le chapitre 9.

La communication fait partie intégrante de toute mission d'assurance et se déroule tout au long de la mission. Les résultats sont communiqués de diverses manières : notes de service, résumés, discussions, versions préliminaires des papiers de travail. Au moment où la mission s'achève, les résultats finaux sont communiqués aux parties concernées. Cette communication finale sur les résultats de la mission est souvent appelée « rapport d'audit » ; c'est le moyen formel, pour l'audit interne, de communiquer les résultats de la mission au management, ainsi qu'à toute autre partie concernée qui a besoin de ces résultats.

Comme expliqué dans le chapitre 13, *Le déroulement de la mission d'assurance*, toute mission d'assurance est conçue pour atteindre des objectifs d'audit spécifiques. Ceux-ci sont directement liés à l'évaluation annuelle des risques et au plan d'audit interne. Le présent chapitre est axé sur la communication des résultats des missions d'assurance et sur les procédures de suivi découlant des observations qui ont été dégagées lors d'une mission d'assurance.

Le chapitre 13 présente également les étapes permettant de conduire une mission d'assurance. Au cours de la mission, l'audit interne teste des contrôles pour s'assurer qu'ils sont conçus de manière adéquate et fonctionnent de manière effective afin de répondre à des assertions spécifiques relatives aux contrôles (les objectifs). L'encadré 14-3 décrit quelques-unes de ces assertions fondamentales relatives aux contrôles, ainsi que les assertions plus traditionnelles relatives aux états financiers. Une observation est formulée si, au cours du test, l'audit interne conclut que certains des contrôles identifiés dans le cadre de la mission ne sont pas conçus de manière adéquate ou ne fonctionnent pas de manière effective. Il arrive bien entendu qu'une mission ne produise aucune observation. Cependant, dès qu'une observation est identifiée, l'audit interne doit procéder en plusieurs étapes afin de déterminer les répercussions éventuelles que cette observation peut avoir sur son évaluation de l'adéquation de la conception et du fonctionnement effectif du contrôle. En outre, l'audit interne doit prendre en compte l'incidence des observations relevées sur l'obligation de communication, conformément aux *Normes internationales pour la pratique professionnelle de l'audit interne* (*Normes*), comme nous le décrirons plus loin dans ce chapitre. Même si aucune observation n'est identifiée au cours de la mission, une communication formelle reste nécessaire pour en faire état et indiquer que l'on considère que l'audit interne s'est pleinement acquitté de ses obligations professionnelles conformément aux *Normes*.

Copyright © 2015 Eyrolles.

ENCADRÉ 14-3

CRITÈRES POUR L'APPRÉCIATION DES ASSERTIONS DU MANAGEMENT

Critères pour l'appréciation des assertions du management relatives aux contrôles	
Habilitation	La transaction a-t-elle été autorisée par une personne habilitée ?
Validité	La transaction ou l'événement sous-jacent ont-ils effectivement eu lieu ?
Exactitude	Les conditions, les montants, etc. sont-ils corrects ?
Rapidité	Est-ce que tout a été comptabilisé dans la période adéquate ?
Confidentialité	Les informations sont-elles restées confidentielles ?
Intégrité	L'information est-elle exempte de toute corruption ou altération ?
Disponibilité	L'information a-t-elle été stockée et est-elle facile à retrouver ?
Critères pour l'appréciation des assertions du management relatives aux états financiers	
Existence ou occurrence	Tout ce qui figure ici est-il supposé s'y trouver ?
Exhaustivité	Tout ce qui est censé y être s'y trouve-t-il effectivement ?
Droits et obligations	Tous les éléments sont-ils réels, autorisés et approuvés ?
Évaluation ou affectation	Sont-ils correctement calculés et comptabilisés ?
Présentation et communication	Sont-ils correctement classifiés ?

L'audit interne parvient à déterminer l'obligation de communication indiquée par les observations identifiées en suivant une série d'étapes qui lui permettent d'évaluer les facteurs influençant chaque observation en termes d'impact, de probabilité d'occurrence, de classification et de répercussions sur la maîtrise des risques. L'audit interne doit également déterminer l'origine de l'observation, à savoir si le contrôle en question est conçu de manière inadéquate ou ne fonctionne pas de manière effective. Une fois ces facteurs identifiés pour chaque observation relevée durant la mission, l'audit interne doit s'appuyer sur son jugement professionnel pour déterminer l'impact global de toutes les observations prises dans leur ensemble. Ainsi, une mission peut aboutir à trois observations dont aucune, individuellement, ne constitue une observation « significative ». Cependant, l'audit interne peut déterminer que les trois, prises ensemble, constituent une observation « significative ». Si l'évaluation des observations s'applique à tous les contrôles (qu'ils portent sur les opérations, sur la conformité ou sur le reporting, comme indiqué au chapitre 6, *Le contrôle interne*), l'évaluation du contrôle interne relatif au reporting financier et des contrôles et procédures liés à la communication externe nécessite, quant à elle,

Copyright © 2015 Eyrolles.

que les obligations de communication spécifiques imposées par la réglementation des pays dans lesquels opère l'organisation soient prises en compte. Par conséquent, lorsqu'une observation ayant trait à un contrôle relatif au reporting financier doit être communiquée, l'audit interne a moins de latitude pour décider comment et à qui communiquer ces informations.

L'encadré 14-4 illustre ce processus complexe et montre les diverses combinaisons de jugements que l'audit interne peut rencontrer lorsqu'il détermine le mode adéquat de remontée de l'information et la forme de la communication des résultats de la mission d'assurance. Cette communication finale revêt une importance particulière parce qu'elle donne l'appréciation indépendante de l'audit interne concernant l'adéquation de la conception et le fonctionnement effectif des contrôles couverts par le périmètre de la mission d'assurance en question, ainsi qu'une évaluation indépendante de l'opinion du management sur les contrôles couverts par la mission d'assurance. Prises collectivement, les communications finales de toutes les missions, incluses dans le plan d'audit interne annuel, permettent à l'audit interne de corroborer les critères de qualité retenus par le management sur le système de contrôle interne de l'organisation.

Même si, pour déterminer comment et à qui communiquer des observations, l'audit interne doit s'appuyer sur des jugements tout au long du processus, l'encadré 14-4 montre que ce processus peut être scindé en plusieurs étapes. Il faut tout d'abord déterminer si des observations ont été relevées durant l'exécution de la mission d'assurance et, *in fine*, comment et à qui communiquer ces observations.

Observation

Conclusion, déduction ou jugement découlant des résultats de tests effectués par l'auditeur interne dans le cadre d'une mission d'assurance ou de conseil. Également appelé constat ou constatation.

PROCESSUS D'ÉVALUATION DES OBSERVATIONS ET DE REMONTÉE DE L'INFORMATION

Comme indiqué plus haut, une observation est généralement identifiée sur la base de preuves qu'un contrôle ne fonctionne pas de manière effective. Cependant, lorsque l'on évalue un contrôle au regard des assertions fondamentales relatives aux contrôles, telles que celles listées dans l'encadré 14-3, un défaut dans sa conception peut également donner lieu à une observation. Indépendamment de la manière dont une observation est identifiée, les auditeurs internes doivent apprécier chacune des observations à partir d'un processus d'évaluation et de remontée de l'information, tel que celui décrit dans l'encadré 14-4, et déterminer quelles répercussions ces observations auront sur les communications afférentes au domaine (processus) examiné. Ils peuvent le déterminer en suivant une série d'étapes permettant d'évaluer les facteurs influençant l'observation en termes d'impact, de probabilité d'occurrence, de classification et de répercussions sur la maîtrise des risques. Les

Copyright © 2015 Eyrolles.

auditeurs internes doivent également définir l'origine de l'observation, à savoir si le contrôle en question est conçu de manière inadéquate ou ne fonctionne pas de manière effective. Comme indiqué à l'encadré 14-4, chaque fois qu'une décision est prise à une étape du processus, elle se répercute sur l'étape suivante.

Les catégories d'objectifs fixés par le COSO

Une fois une ou plusieurs observations identifiées, il convient de déterminer quelle catégorie d'objectifs, répertoriés par le COSO, est le plus directement affectée par le contrôle compromis, sans oublier qu'une observation peut avoir une incidence sur plusieurs catégories. Les contrôles permettent de maîtriser les risques qui menacent la réalisation des objectifs, selon trois catégories définies par le COSO :

- Objectifs liés aux opérations. Ils concernent l'efficacité et l'efficience des opérations. Il s'agit notamment des objectifs de performance opérationnelle et financière, ainsi que la sauvegarde des actifs.
- Objectifs liés au reporting. Ils concernent le reporting interne et externe, financier et extrafinancier. Ils peuvent englober la fiabilité, les délais, la transparence ou d'autres aspects demandés par les régulateurs, les organismes de normalisation ou les instructions internes.
- Objectifs liés à la conformité. Ils concernent le respect des lois et règlements applicables.[1]

Classification

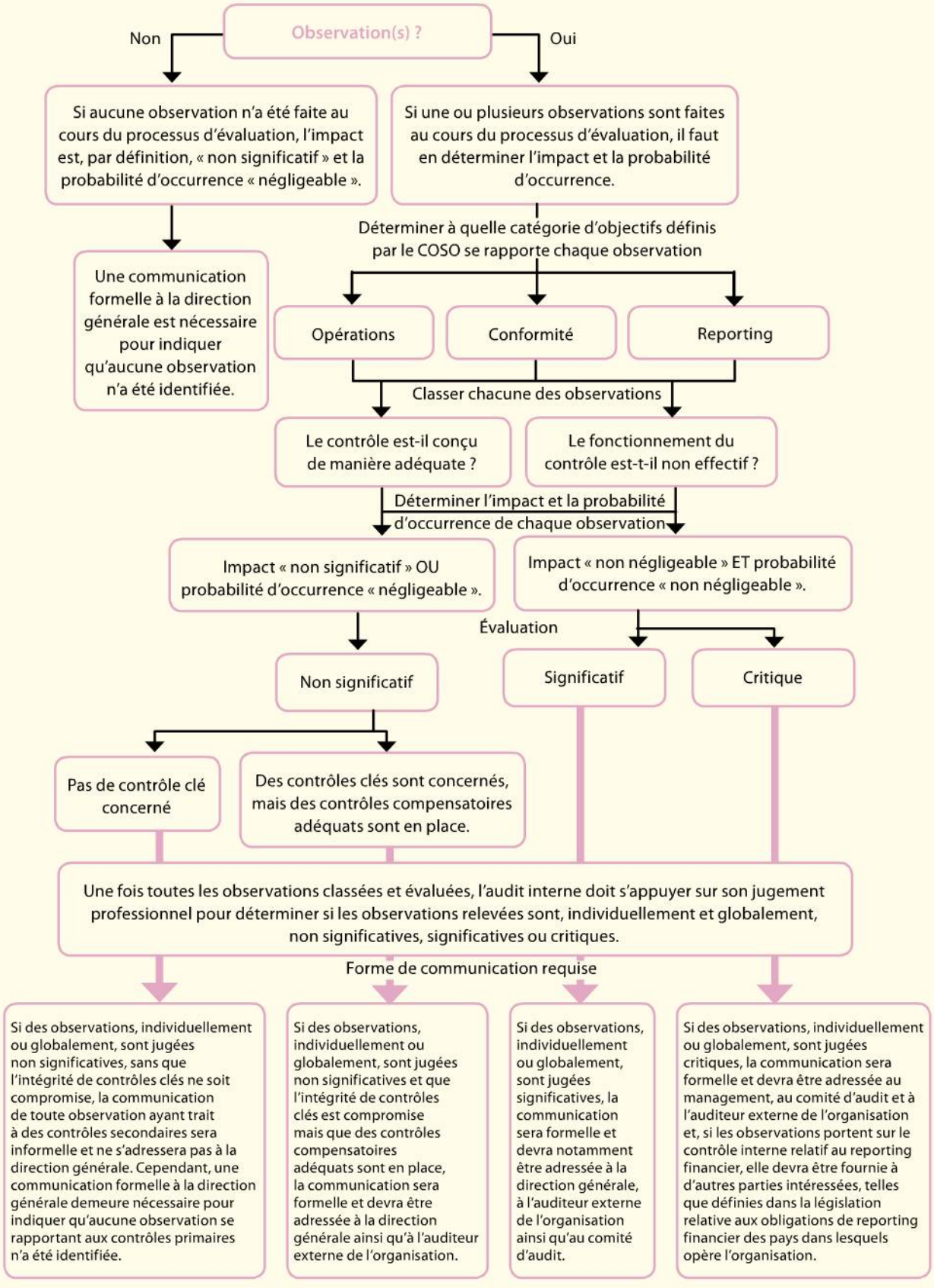
Une fois qu'il a été déterminé à quelle catégorie correspond l'observation, il s'agit de la classer en fonction du fait que sa défaillance provienne d'une conception inadéquate ou d'un fonctionnement non effectif du contrôle.

Impact et probabilité d'occurrence des observations

L'étape suivante consiste à déterminer l'impact et la probabilité d'occurrence de l'observation en question. Il faut alors formuler un jugement sur la gravité de l'observation : représente-t-elle une faille non significative, significative ou critique dans la capacité du contrôle à maîtriser un risque ou un groupe de risques spécifique ? Comme toutes les autres étapes, celle-ci doit être effectuée pour chacune des observations relevées durant la mission. Cependant, une fois qu'on est arrivé à cette étape pour chacune des observations, tout le processus sera effectué à nouveau pour les

Copyright © 2015 Eyrolles.

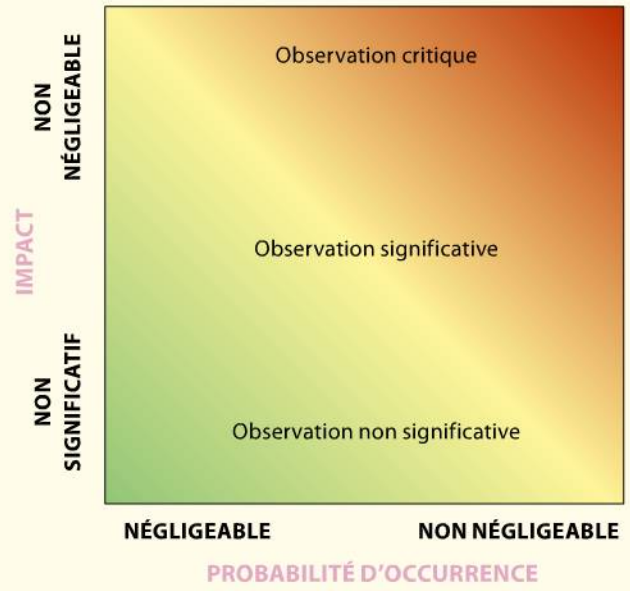
PROCESSUS D'ÉVALUATION DES OBSERVATIONS ET DE REMONTÉE DE L'INFORMATION



Copyright © 2015 Eyrolles.

ENCADRÉ 14-5

SCHÉMA D'ÉVALUATION DES OBSERVATIONS



observations prises toutes ensemble. Pour une représentation des relations et interdépendances entre impact et probabilité d'occurrence, voir l'encadré 14-5.

Il existe trois niveaux d'importance : non significatif, significatif et critique. Bien que les termes « significatif » et « critique » viennent de la réglementation sur le reporting financier instaurée dans de nombreux pays et soient particulièrement pertinents lorsque le contrôle interne porte sur le reporting financier ou lorsqu'il s'agit de contrôles et procédures liés à la communication externe, ils sont également utilisés ici pour les contrôles relatifs aux opérations, à la conformité et au reporting extrafinancier. Nous allons définir chacun de ces trois termes, mais il faut bien garder à l'esprit qu'il s'agit avant tout de concepts. En pratique, les fonctions d'audit interne s'appuient, à juste titre, sur les paramètres de tolérance au risque, en place dans l'organisation, qui sont définis et révisés par la fonction de gestion des risques. Il arrive parfois que ces paramètres tiennent compte de l'importance relative prévue de l'auditeur externe, ce qui simplifie le processus d'appréciation des observations et permet que les termes et définitions pertinents soient appliqués de façon uniforme à tous les contrôles relatifs aux opérations, à la conformité et au reporting extrafinancier, en plus de ceux relatifs au reporting financier et des contrôles et procédures liés à la communication externe. L'encadré 14-6 donne un exemple d'indicateurs financiers de hiérarchisation des risques, tandis que l'encadré 14-7 illustre les critères d'appréciation des observations, avec notamment un exemple de calcul d'anomalie tolérable (acceptable) et d'importance relative prévue de l'auditeur externe.

Copyright © 2015 Eyrolles.

ENCADRÉ 14-6

INDICATEURS DE HIÉRARCHISATION DES RISQUES

Impact (sévérité)				
Indicateur	**Cotation**	**Description**	**Fourchette (base de résultat avant impôt)**	**Bénéfice par action**
Impact	1	**Perte faible**	< X millions	< X,XXX
	2	**Perte moyenne** (non significatif)	≥ X millions < XX millions	< X,XXX
	3	**Perte importante** (significatif)	≥ XX millions < XXX millions	≥ X,XXX < X,XXX
	4	**Impact majeur sur l'exploitation** (critique)	≥ XXX millions < X XXX millions	≥ X,XXX < X,XXX
	5	**Impact nécessitant une action du Conseil**	≥ X XXX millions < XX XXX millions	≥ X,XXX < X,XXX
	6	**Mise en péril potentielle**	≥ XX XXX millions	≥ X,XXX

Probabilité d'occurrence = Fréquence + Alerte			
Indicateur	**Cotation**	**Description**	**Fourchette**
Fréquence	1	Survient extrêmement rarement	Au plus une fois tous les 5 ans
	2	Survient rarement	Une fois tous les 1-4 ans
	3	Survient périodiquement	1 à 11 fois par an
	4	Survient souvent	12 fois ou plus par an
Indicateur	**Cotation**	**Description**	**Exemple**
Alerte	1	Alerte depuis des mois ou des années	Changement dans la législation ou la réglementation
	2	Alerte depuis des heures ou des jours	Tempête ou inondation
	3	Pas d'alerte	Incendie ou piratage informatique

Observation non significative

Indique qu'un contrôle présente une probabilité « négligeable » d'échouer ou que l'impact de cet échec serait négligeable.

Observation non significative

Une ou plusieurs observations sont jugées non significatives si le contrôle en question présente une probabilité « négligeable » d'échouer[2] ou si l'impact de cet échec est « non significatif » (négligeable). Si la ou les observations sont jugées non significatives, l'audit interne doit approfondir son évaluation pour déterminer si des contrôles clés sont en jeu. Ce point est crucial, car il détermine comment et à qui les observations doivent être rapportées. Si la ou les observations sont non significatives et qu'aucun contrôle clé n'est concerné, la communication sera généralement informelle et n'aura pas besoin d'être adressée au management en dehors du

Copyright © 2015 Eyrolles.

(ou des) domaine(s) soumis à l'audit. Néanmoins, une communication formelle à la direction générale reste nécessaire pour indiquer qu'aucune observation touchant des contrôles clés n'a été détectée. Rappelons que le chapitre 6, *Le contrôle interne*, définit les contrôles clés (primaires ou essentiels) comme ceux conçus pour maîtriser des risques significatifs associés aux objectifs critiques d'une organisation. Si des contrôles clés sont touchés et qu'il existe des contrôles compensatoires adéquats pour réduire l'effet négatif des contrôles clés compromis, l'observation restera considérée comme non significative. Cependant, il faudra qu'une communication formelle remonte jusqu'au management extérieur au domaine audité, qui est chargé de la surveillance de ce domaine, et si nécessaire, à l'auditeur externe de l'organisation.

Observation significative

Observation significative

Indique qu'un contrôle présente une probabilité « non négligeable » d'échouer et que l'impact de cet échec ne serait pas négligeable.

Comme évoqué plus haut, le terme *déficience significative* est issu de la réglementation sur le reporting financier qui existe dans de nombreux pays et renvoie spécifiquement à des observations liées au contrôle interne relatif au reporting financier ainsi qu'aux contrôles et procédures liés à la communication externe. Cependant, certaines organisations choisissent, pour des raisons de conformité, d'appliquer les mêmes critères de définition aux observations portant sur les opérations, la conformité et le reporting extrafinanciers. C'est dans ce sens que nous utilisons l'expression *observation significative*. Une ou plusieurs observations sont jugées significatives si le contrôle en question présente une probabilité « non négligeable » d'échouer, et si l'impact de cet échec est « non négligeable » (c'est-à-dire qu'il est significatif). Dans ce cas, la communication doit être formelle et être notamment adressée à la direction générale, à l'auditeur externe de l'organisation et au comité d'audit.

Observation critique

Observation critique

Indique qu'un contrôle présente une probabilité « non négligeable » d'échouer et que l'impact de cet échec dépasserait le seuil d'importance relative.

Comme le terme *déficience significative*, le terme *faiblesse importante* est issu de la réglementation sur le reporting financier et s'applique spécifiquement à des observations liées au contrôle interne relatif au reporting financier ainsi qu'aux contrôles et procédures liés à la communication externe. Là encore, certaines organisations appliquent les critères de définition d'une faiblesse importante aux observations portant sur la conformité, les opérations et le reporting extrafinanciers. C'est dans ce sens que nous utilisons l'expression *observation critique*. Une ou plusieurs observations sont jugées critiques si le contrôle en question présente une probabilité « non négligeable » d'échouer, et si l'impact de cet échec est non seulement « non négligeable », mais également supérieur au seuil d'importance relative des états financiers (ou tout autre

Copyright © 2015 Eyrolles.

seuil d'importance relative établi). Pour un exemple de critères d'évaluation des observations, se reporter à l'encadré 14-7. Si la ou les observations sont jugées critiques, la communication doit être formelle et être notamment adressée à la direction générale, à l'auditeur externe de l'organisation et au comité d'audit. De surcroît, si elle concerne un contrôle interne relatif au reporting financier et des contrôles et procédures liés à la communication externe, la loi Sarbanes-Oxley de 2002 aux États-Unis, la loi sur la Sécurité financière (LSF) en France et la réglementation sur le reporting financier dans d'autres pays imposent aux managements des sociétés concernées de nuancer leur opinion par une réserve concernant le contrôle interne relatif au reporting financier (et les contrôles et procédures liés à la communication externe), ainsi que d'établir un plan d'actions correctives visant à corriger la faiblesse identifiée dans les contrôles en question. Le management doit continuer à formuler des réserves sur le contrôle interne relatif au reporting financier (et sur les contrôles et procédures liés à la communication externe) jusqu'à ce que non seulement il ait été remédié à la faiblesse importante (l'observation en question) mais également qu'il en soit assuré, en testant à nouveau le contrôle, test qui doit aboutir à la conclusion que le contrôle en question est conçu de manière adéquate et fonctionne de manière effective. Si le management détermine qu'il est nécessaire d'exprimer des réserves sur le contrôle interne relatif au reporting financier (et sur les contrôles et procédures liés à la communication externe), ce fait doit être porté à la connaissance des parties prenantes, conformément à la législation du pays dans lequel opère l'organisation.

Éléments d'une observation

- Référentiels.
- Faits.
- Causes.
- Conséquences.

La documentation des conclusions dégagées, découlant de l'exécution du processus d'évaluation des observations et de remontée de l'information, est essentielle pour justifier que l'audit interne a correctement établi comment et à qui communiquer les observations issues de la mission d'assurance. Comme indiqué précédemment, le processus consiste tout d'abord à déterminer si des observations ont été relevées durant l'exécution de la mission d'assurance et, *in fine*, à déterminer comment et à qui communiquer ces observations. De nombreuses fonctions d'audit interne utilisent des modèles de papiers de travail ou des checklists pour les aider à documenter ces résultats. L'encadré 14-8 en constitue un exemple. En outre, ce modèle aide à satisfaire aux obligations de documentation telles que précisées dans les *Normes* et traitées dans le chapitre 13, *Le déroulement de la mission d'assurance*. Plus précisément, les *Normes* indiquent que « les auditeurs internes doivent documenter les informations pertinentes pour étayer les conclusions et les résultats de la mission » (Norme 2330, Documentation des informations). La MPA 2330-1, Documentation des informations, précise : « les auditeurs internes préparent les papiers de travail qui servent à documenter les informations obtenues, les analyses faites, et qui confortent les conclusions et les résultats de la mission. »

Copyright © 2015 Eyrolles.

Le chapitre 13 décrit les diverses étapes associées à l'exécution d'une mission d'assurance, en prenant pour exemple une organisation fictive **Books 2 Buy**. Les encadrés 14-9 et 14-10 présentent les modèles d'évaluation des observations complétés avec les informations obtenues durant le déroulement des missions d'assurance menées chez **Books 2 Buy** au chapitre 13. L'encadré 14-9 documente une observation concernant la délégation de pouvoir, dont on a déterminé qu'elle est non significative et qu'aucun contrôle clé n'est affecté. Par conséquent, elle sera communiquée de manière informelle au management du service des décaissements uniquement. L'encadré 14-10 documente une observation concernant d'éventuels paiements en double. Même si l'on a déterminé que cette observation est non significative, des contrôles clés étant concernés, il est possible de communiquer cette observation de manière formelle (dans tous les cas de documents) à la direction générale et au comité d'audit (ainsi qu'à l'auditeur externe, le cas échéant), en plus du management du service des décaissements.

ENCADRÉ 14-7

CRITÈRES D'ÉVALUATION DES OBSERVATIONS IMPACT (SÉVÉRITÉ)

Exemples d'importance relative prévue et d'anomalie tolérable (acceptable)	
Description	**Fourchette**
Importance relative prévue	5 % du résultat avant impôt
Anomalie tolérable	50 % de l'importance relative prévue
Critères d'évaluation des observations	
Classification des observations	**Fourchette**
Non significatif	< 20 % de l'importance relative prévue
Significatif	20-50 % de l'importance relative prévue
Critique	> 50 % de l'importance relative prévue

Observations et recommandations de mission

Toutes les observations sont rédigées pour inclure des informations spécifiques qui doivent être communiquées quelle que soit la forme de la communication prescrite à l'issue du processus d'évaluation des observations et de remontée de l'information décrit ci-dessus. Les référentiels, les faits, les causes et les conséquences doivent tous être inclus pour chaque observation communiquée. Comme nous l'avons indiqué plus haut, les observations d'audit sont des éléments qui ont attiré l'attention de l'audit interne et qui peuvent influer sur les critères de qualité retenus par le management quant à l'adéquation de la conception et/ou le fonctionnement effectif des contrôles. Les observations de la mission doivent être traitées

Copyright © 2015 Eyrolles.

MODÈLE D'ANALYSE DES OBSERVATIONS

Description des observations d'audit de la mission d'assurance
Mission exécutée : la date

1.	**Synthèse des observations :**	
2.	**Faits** – Preuves factuelles et description des activités de contrôle existantes (ce qui existe réellement). Ce que l'on a découvert grâce aux tests.	
3.	**Référentiels** – Normes, mesures, exigences, règles ou procédures, utilisées pour réaliser l'évaluation (ce qui devrait être).	
4.	**Cause** – Ce qui a permis ou engendré l'existence des faits (la raison de cette différence).	
5.	**Conséquences** – Le risque ou le danger encouru du fait que les situations diffèrent du référentiel (conséquences passées et futures éventuelles). Considère à la fois l'incidence (financière, sur la réputation, en termes de sécurité, etc.) et la probabilité d'occurrence.	
6.	**Contrôles compensatoires** – Autres contrôles en place permettant d'atténuer le problème observé, y compris les activités de surveillance.	
7.	**Conclusions** – Analyse détaillée, évaluation et justification de la classification à laquelle aboutit l'évaluation et les conclusions finales.	
8.	**Recommandations détaillées** – Ce que l'audit interne recommande. Ces recommandations doivent concorder avec la solution du management telle qu'examinée durant le processus de communication préliminaire.	
9.	**Solution du management** – Ce que le management entreprendra pour remédier à la situation existante ou pour empêcher que le problème ne se présente à nouveau.	
10.	**Évaluation des observations :** • Catégories d'objectifs définis par le COSO • Classification • Appréciation **Évaluation effectuée par :** • l'audit interne • le management d'une unité opérationnelle • un auditeur externe	Reporting ____ Critique (faiblesse) ____ Opérations ____ Significatif (déficience) ____ Conformité ____ Non significatif ____ Conception inadéquate ____ Contrôle clé (primaire) ____ Fonctionnement non effectif ____ Contrôle secondaire ____ Nom Date
11.	**Référence du papier de travail**	

ENCADRÉ 14-8

conformément aux indications du processus d'évaluation et de remontée de l'information. Lorsqu'une communication formelle est indiquée, en plus des éléments répertoriés ci-dessus (référentiels, faits, causes et conséquences), l'audit interne formule des recommandations afin de donner à l'audité des orientations sur la manière appropriée de remédier à la déficience constatée et d'améliorer la conception ou le fonctionnement des contrôles.

Copyright © 2015 Eyrolles.

MODÈLE D'ANALYSE DES OBSERVATIONS : OBSOLESCENCE DE LA DÉLÉGATION DU POUVOIR D'EFFECTUER DES DÉCAISSEMENTS

ENCADRÉ 14-9

Procédure de décaissement Books 2 Buy Holding Corporation.
Mission exécutée : le 10 février 20XX

1.	**Synthèse des observations :**	Obsolescence de la délégation du pouvoir d'effectuer des décaissements.
2.	**Faits** – Preuves factuelles et description des activités de contrôle existantes (ce qui existe réellement). Ce que l'on a découvert grâce aux tests.	Dans la délégation du pouvoir d'effectuer des décaissements, sept des personnes répertoriées ne font plus partie de l'organisation. De plus, on a identifié neuf personnes qui occupent depuis peu leur fonction ou qui viennent de rejoindre l'organisation et qui devraient disposer du pouvoir d'effectuer des décaissements, mais qui ne figurent pas sur la liste.
3.	**Référentiels** – Normes, mesures, exigences, règles ou procédures, utilisées pour réaliser l'évaluation (ce qui devrait être).	Le pouvoir d'effectuer des décaissements ne devrait être délégué qu'aux personnes dont les responsabilités justifient qu'elles disposent de ce pouvoir.
4.	**Cause** – Ce qui a permis ou engendré l'existence des faits (la raison de cette différence).	Le règlement sur la délégation du pouvoir d'effectuer des décaissements est mis à jour semestriellement mais il n'y a pas de mise à jour lorsque les collaborateurs ou les responsabilités des personnes habilitées changent.
5.	**Conséquences** – Le risque ou le danger encouru du fait que les situations diffèrent du référentiel (conséquences passées et futures éventuelles). Considère à la fois l'incidence (financière, sur la réputation, en termes de sécurité, etc.) et la probabilité d'occurrence.	Il est possible que des décaissements effectués ne soient pas en conformité avec les lignes directrices de la direction générale ou du Conseil.
6.	**Contrôles compensatoires** – Autres contrôles en place permettant d'atténuer le problème observé, y compris les activités de surveillance.	Une fois que les collaborateurs quittent l'organisation, tous les droits d'accès au système sont supprimés. En conséquence, même si les sept personnes qui ne font plus partie de l'organisation conservent, en théorie, le pouvoir de signature, elles ne pourraient pas se connecter pour valider des transactions. Une analyse des prévisions budgétaires par rapport aux dépenses réelles est réalisée chaque mois par tous les responsables de service et les propriétaires de centre de coûts.
7.	**Conclusions** – Analyse détaillée, évaluation et justification de la classification à laquelle aboutit l'évaluation et les conclusions finales.	Étant donné les activités de contrôle compensatoires, le risque d'un décaissement indûment autorisé est minime. Si le management peut faire des efforts pour mettre à jour le règlement plus fréquemment, il s'appuie sur d'autres contrôles clés pour maîtriser le risque et accepte le niveau de risque actuel. *Cette observation d'audit ne sera donc pas incluse dans le rapport final.*
8.	**Recommandations détaillées** – Ce que l'audit interne recommande. Ces recommandations doivent concorder avec la solution du management telle qu'examinée durant le processus de communication préliminaire.	Le management doit mettre en place des procédures permettant de mettre à jour la liste de personnes habilitées et les limites de décaissement autorisé correspondantes.
9.	**Solution du management** – Ce que le management entreprendra pour remédier à la situation existante ou pour empêcher que le problème ne se présente à nouveau.	Le management estime que le risque soulevé par cette observation est minime et, par conséquent, accepte de supporter la faiblesse identifiée entre deux mises à jour du règlement. **Responsabilité :** sans objet (N/A) **Date cible :** sans objet (N/A)
10.	**Évaluation des observations :** • Catégories d'objectifs définis par le COSO • Classification • Appréciation **Évaluation effectuée par :** • l'audit interne • le management d'une unité opérationnelle • un auditeur externe	Reporting X — Critique (faiblesse) ____ Opérations X — Significatif (déficience) ____ Conformité ____ — Non significatif X Conception inadéquate X — Contrôle clé (primaire) ____ Fonctionnement non effectif ____ — Contrôle secondaire X Nom — Date Robert Dupont — jj/mm/aa
11.	**Référence du papier de travail**	Z-3, X-1

Copyright © 2015 Eyrolles.

ENCADRÉ 14-10

MODÈLE D'ANALYSE DES OBSERVATIONS : POSSIBILITÉ DE PAIEMENTS EN DOUBLE

Procédure de décaissement Books 2 Buy Holding Corporation.
Mission exécutée : le 10 février 20XX

1.	**Synthèse des observations :**	Possibilité de paiements en double
2.	**Faits** – Preuves factuelles et description des activités de contrôle existantes (ce qui existe réellement). Ce que l'on a découvert grâce aux tests.	Le système a rejeté toutes les saisies de factures en double. En revanche, il a accepté des factures pour lesquelles un chiffre ou un symbole était ajouté à la fin du numéro de facture, si bien qu'un paiement en double n'est pas exclu.
3.	**Référentiels** – Normes, mesures, exigences, règles ou procédures, utilisées pour réaliser l'évaluation (ce qui devrait être).	La réception de biens et services ne doit être comptabilisée et traitée qu'une fois.
4.	**Cause** – Ce qui a permis ou engendré l'existence des faits (la raison de cette différence).	Dans certains cas, les collaborateurs du service de la comptabilité fournisseurs (CF) peuvent saisir des factures une seconde fois lorsqu'une facture en double est envoyée par le fournisseur. Ils peuvent ne pas se rendre compte que ces factures ont déjà été reçues auparavant et, étant donné la faiblesse dans la conception du contrôle décrite au paragraphe 2 ci-dessous, ils peuvent ajouter un caractère à la fin pour en faciliter le traitement. Dans d'autres cas, le fournisseur émet un duplicata de facture qui porte un numéro différent (généralement supérieur au précédent) et les collaborateurs du service CF ne s'aperçoivent pas qu'il peut s'agir d'une facture en double.
5.	**Conséquences** – Le risque ou le danger encouru du fait que les situations diffèrent du référentiel (conséquences passées et futures éventuelles). Considère à la fois l'incidence (financière, sur la réputation, en termes de sécurité, etc.) et la probabilité d'occurrence.	Les dettes et les actifs ou charges correspondants ont été surestimés de 357 782,41 et ce même montant a été décaissé indûment.
6.	**Contrôles compensatoires** – Autres contrôles en place permettant d'atténuer le problème observé, y compris les activités de surveillance.	Une analyse des prévisions budgétaires par rapport aux dépenses réelles est réalisée chaque mois par tous les responsables de service et les propriétaires de centre de coûts.
7.	**Conclusions** – Analyse détaillée, évaluation et justification de la classification à laquelle aboutit l'évaluation et des conclusions finales.	Si les contrôles compensatoires peuvent permettre de détecter des paiements en double de gros montant, les paiements en double n'en doivent pas moins être recouvrés auprès du fournisseur. En outre, de petits montants sans conséquence risquent de ne pas être détectés (comme l'a prouvé le test d'audit). Le management est d'accord avec l'observation et propose un plan pour remédier à cette faiblesse. *En conséquence, cette observation d'audit figurera dans le rapport définitif.*
8.	**Recommandations détaillées** – Ce que l'audit interne recommande. Ces recommandations doivent concorder avec la solution du management telle qu'examinée durant le processus de communication préliminaire.	On recommande que le service CF crée un programme d'interrogation des données qui reprenne les tests effectués par l'audit interne et qu'il l'effectue avant de traiter chaque lot. Les résultats de cette requête doivent ensuite être examinés par le superviseur CF et si un quelconque paiement est identifié comme potentiellement redondant, cette transaction doit être sortie du lot et examinée de près avant d'être réglée.
9.	**Solution du management** – Ce que le management entreprendra pour remédier à la situation existante ou pour empêcher que le problème ne se présente à nouveau.	Un programme d'interrogation des données fonctionnant de la même manière que le test de l'audit interne sera élaboré. Il sera appliqué avant qu'un lot ne soit traité, puis examinée par le superviseur CF. Si un paiement redondant potentiel est identifié, la transaction sera sortie du lot et examinée de près avant d'être réglée. **Responsabilité :** Superviseur CF **Date cible :** jj/mm/aa
10.	**Évaluation des observations :** • Catégories d'objectifs définis par le COSO • Classification • Appréciation **Évaluation effectuée par :** • l'audit interne • le management d'une unité opérationnelle • un auditeur externe	Reporting X — Critique (faiblesse) ____ Opérations ____ — Significatif (déficience) ____ Conformité ____ — Non significatif X Conception inadéquate X — Contrôle clé (primaire) X Fonctionnement non effectif _____ — Contrôle secondaire ____ Nom — Date Robert Dupont — jj/mm/aa
11.	**Référence du papier de travail**	Z-4, X-5

Copyright © 2015 Eyrolles.

La MPA 2410-1, Contenu de la communication, donne de plus amples détails sur les éléments que doit contenir chaque observation de mission lorsqu'elle est communiquée : « les observations et recommandations sont le résultat d'un processus de comparaison d'un référentiel (la situation normale) et d'un fait (la situation actuelle). Qu'il y ait ou non constat d'un écart, l'auditeur interne dispose d'éléments sur lesquels fonder son rapport. Les observations et recommandations sont fondées sur les caractéristiques suivantes :

- des référentiels : les normes, mesures ou exigences requises, utilisés pour évaluer ou vérifier (la situation normale) ;
- des faits : les preuves factuelles identifiées par l'auditeur interne au cours de son examen (la situation actuelle) ;
- des causes : la raison de la différence entre les situations attendues et existantes ;
- des conséquences : le risque ou le danger encouru par l'organisation ou d'autres, du fait que les situations diffèrent du référentiel (l'impact de la différence). Pour déterminer l'importance du risque ou de l'enjeu, les auditeurs internes prennent en considération les conséquences de leurs observations et recommandations sur le fonctionnement et les états financiers de l'organisation ;
- les observations et recommandations peuvent inclure les réalisations [de l'entité auditée], des questions connexes et des informations destinées à étayer les conclusions ».

Les référentiels, faits, causes et conséquences sont décrits de manière plus détaillée ci-dessous.

Référentiels
Ce qui devrait être.

Faits
La situation actuelle (ce qui est).

Causes
Raison de la différence entre ce qui devrait être et ce qui est.

Conséquences
L'impact de la différence entre ce qui devrait être et ce qui est.

Les référentiels

Les référentiels énoncent ce qui devrait être. Cette composante d'une observation identifie ce qui doit être réalisé. Ces référentiels peuvent être déjà énoncés dans une règle, une procédure, une loi, un règlement, etc., ou bien être déterminés par l'auditeur interne en fonction de normes raisonnables pour la réalisation des objectifs de l'organisation.

Les faits

Les faits décrivent les contrôles tels qu'ils sont et tels qu'ils fonctionnent au moment de l'audit ou de l'évaluation. Ils énoncent ce que l'on a découvert grâce aux tests. Ils forment le cœur des observations de la mission et doivent être étayés par des preuves et des informations appropriées (pertinentes et fiables).

Copyright © 2015 Eyrolles.

Les causes

Les causes expliquent ce qui a permis aux faits d'exister. Elles décrivent les éléments des processus du management qui soit n'existaient pas soit ont échoué, permettant ainsi aux faits de se produire. C'est une composante essentielle, car si elles ne sont pas connues, les recommandations ou les actions correctives ne sont pas possibles, et le problème peut réapparaître.

Les conséquences

Les conséquences sont les effets (à la fois passés et potentiels à venir) qui pourraient découler de l'observation. Elles décrivent ce qui s'est produit ou pourrait se produire parce que les faits ne correspondent pas aux référentiels (à savoir des répercussions défavorables). Cette composante est nécessaire pour convaincre le management qu'une action corrective s'impose. Dès que possible, elle doit être quantifiée par l'indication de la valeur monétaire associée au risque, du nombre d'occurrences, etc.

Recommandation

Actions correctives proposées pour remédier à la situation.

Recommandation détaillée

La recommandation donne des indications sur la manière de remédier à la situation. Elle décrit la conduite que le management doit adopter pour régler le problème et en éliminer les conséquences néfastes ou défavorables. La mesure recommandée doit traiter les causes du problème et proposer des mesures pour en éviter la récurrence.

Selon la MPA 2410-1, Contenu de la communication, « l'auditeur interne peut communiquer des recommandations sur les améliorations et faire état des fonctionnements satisfaisants et des mesures correctives. Les recommandations sont fondées sur les observations et conclusions de l'auditeur interne. Elles appellent des actions destinées à corriger les situations existantes ou à améliorer le fonctionnement et peuvent suggérer des approches visant à corriger ou à améliorer le fonctionnement, approches que le management peut utiliser comme guide pour l'atteinte des résultats fixés. Les recommandations peuvent être de nature générale ou spécifique. »

PROCÉDER À DES COMMUNICATIONS INTERMÉDIAIRES ET PRÉLIMINAIRES

Comme indiqué précédemment, la communication fait partie intégrante de toute mission d'assurance et intervient tout au long de la mission, à mesure que celle-ci progresse. Durant l'exécution d'une

Copyright © 2015 Eyrolles.

mission d'assurance, l'audit interne communique régulièrement avec les acteurs principaux du domaine audité. L'essentiel de cette communication s'effectue par courriel, lors de réunions en face à face ou de conférences téléphoniques. Elle a pour objet de discuter des observations au fur et à mesure qu'elles sont établies. Cette manière de procéder permet de s'assurer que les faits sont exacts tout en ouvrant le dialogue sur les meilleures actions correctives pour les observations identifiées. Lorsqu'une observation appelle une attention immédiate, la communication intermédiaire permet de la porter rapidement à l'attention des personnes concernées, ce qui accroît la probabilité que le problème soit vite résolu. L'audit interne utilise les informations réunies lors des communications intermédiaires pour finaliser les observations qui se retrouveront, à terme, dans la communication finale, et pour formaliser le plan d'action proposé par le management, qui sera également inclus dans la communication finale.

Dans l'objectif de respecter les impératifs de la communication finale, le processus d'évaluation des observations et de remontée de l'information fait passer les observations de la mission par un processus méthodique. Cependant, l'audit interne doit confirmer les faits et conclusions préliminaires avec les représentants du management du domaine audité avant de diffuser ses papiers finaux. Il peut le faire de plusieurs manières, mais la méthode la plus courante consiste à organiser une réunion formelle avec le management, que l'on appelle généralement réunion de clôture ou réunion de fin de mission, à l'issue de laquelle une communication finale est élaborée, quelle qu'en soit la forme. Dans le cadre de ce processus, l'audit interne rencontre les représentants du management du domaine audité afin de s'assurer qu'ils sont d'accord avec les observations et conclusions préliminaires discutées tout au long de la mission. Cette méthode permet à toutes les parties d'examiner ce que contiendra la communication formelle des résultats de la mission et donne l'opportunité de lever toute ambiguïté éventuelle. En outre, elle permet non seulement au management du domaine qui a fait l'objet de la mission d'assurance d'émettre son opinion et de présenter les actions relatives aux éléments qui seront intégrés à la communication finale, mais également de donner un retour d'information sur la qualité de la mission d'assurance menée par l'équipe d'audit. Le plan d'action du management destiné à remédier aux déficiences de contrôle identifiées au cours de la mission est généralement appelé commentaires ou réponses du management. Ces actions correctives sont formulées à partir des éléments fournis par l'audit interne, mais leur mise en œuvre relève, *in fine*, de la responsabilité du management. De nombreuses fonctions d'audit interne incluent les réponses du management dans la communication finale des résultats de la mission.

La MPA 2410-1, Contenu de la communication, donne des orientations relatives à l'intégration de la réponse du management dans la communication des résultats de la mission : « dans le cadre des

Copyright © 2015 Eyrolles.

discussions entre l'auditeur interne et l'audité, l'auditeur interne obtient l'accord de l'audité sur les résultats de l'audit et sur tout plan d'action nécessaire à l'amélioration des activités. Si l'auditeur interne et l'audité ne s'entendent pas sur les résultats de l'audit, le rapport d'audit mentionne les deux positions ainsi que les raisons du désaccord. Les commentaires écrits de l'audité peuvent être inclus en annexe au rapport, dans le corps du rapport ou dans une lettre introductive ».

De plus, la MPA 2410-1 affirme que « des rapports intermédiaires sont utilisés pour communiquer des informations nécessitant une attention immédiate, pour signaler un changement dans le champ de la mission ou pour informer le management de l'avancement des travaux lorsque la mission est de longue durée. L'emploi de rapports intermédiaires ne réduit ni n'élimine la nécessité d'un rapport définitif ».

Au moment où la mission s'achève, les résultats finaux doivent être communiqués aux parties compétentes concernées. La communication finale des résultats de la mission peut revêtir différentes formes, que nous détaillerons plus loin dans ce chapitre, et constitue le moyen formel pour l'audit interne de s'acquitter de son obligation de communication professionnelle, conformément aux *Normes*, ce que nous verrons aussi ultérieurement dans ce chapitre.

Communication finale

Moyen par lequel l'audit interne informe les parties intéressées des résultats de la mission.

RÉDIGER LE RAPPORT DÉFINITIF DE LA MISSION

L'élaboration d'un rapport définitif à la suite d'une mission d'assurance est importante pour plusieurs raisons. Comme indiqué dans le chapitre 1, *Introduction à l'audit interne*, et dans le chapitre 2, *Le Cadre de référence international des pratiques professionnelles : des lignes directrices incontournables pour l'audit interne*, la grande différence entre une mission d'assurance et une mission de conseil réside dans le fait que, dans la première, trois parties sont concernées :

- la personne ou le groupe directement impliqué dans le processus, le système ou autre, appelé l'audité ;
- la personne ou le groupe qui réalise l'évaluation indépendante, à savoir l'audit interne ;
- la personne ou le groupe qui utilise l'évaluation indépendante : l'utilisateur.

Une mission de conseil fait, elle, généralement intervenir deux parties :

- la personne ou le groupe qui formule le conseil, c'est-à-dire l'audit interne ;
- la personne ou le groupe qui demande et reçoit le conseil : le client.

Copyright © 2015 Eyrolles.

Étant donné que les résultats présentés dans le rapport définitif d'une mission d'assurance seront utilisés par quelqu'un d'autre que l'audité (par exemple, le comité d'audit), il est impératif que la communication soit concise, complète et précise. De plus, le rapport final apporte la preuve que l'audit interne a réalisé une évaluation indépendante du système de contrôle interne de l'organisation ou du domaine concerné et permet la conservation permanente des travaux relatifs à la mission d'assurance ainsi que des résultats.

Le rapport définitif d'une mission d'assurance permet à l'audit interne de s'acquitter des obligations suivantes :

- communiquer en temps opportun des informations pertinentes au management concernant les déficiences des activités de contrôle (conception inadéquate ou fonctionnement non effectif), les points forts des activités de contrôle, les possibilités d'optimiser l'utilisation des ressources ou la réduction des coûts, ainsi que les domaines dans lesquels on peut accroître la productivité ou l'efficience ;
- documenter le périmètre de la mission, ses conclusions, les observations et les plans d'actions du management ;
- établir des archives permanentes des travaux effectués pendant une mission et des résultats de cette mission.

Comme tous les rapports de mission, le rapport définitif doit être professionnel, précis, complet et diffusé en temps opportun. La réalisation de tous ces objectifs représente souvent un compromis. En effet, un rapport de mission de qualité doit donner l'assurance que suffisamment de temps a été consacré à l'exécution d'un travail précis et détaillé et qu'il est diffusé en temps opportun, afin de répondre au besoin du management de disposer d'informations à jour. Le temps nécessaire à la diffusion d'un rapport de mission varie en fonction du temps consacré à la réalisation de la mission, du nombre et de la complexité des observations contenues dans le rapport. Cependant, la pratique veut que le management reçoive le rapport définitif de la mission dans les dix jours ouvrés après achèvement de la communication préliminaire (réunion de clôture ou de fin de mission).

Pour être bien conçue, la communication finale doit comporter les éléments suivants :

- **l'exposé de l'objet et du périmètre de la mission :** les objectifs et le périmètre de la mission. Selon la MPA 2410-1, « l'exposé du périmètre de la mission précise les activités auditées et peut comporter des informations complémentaires telles que la période couverte et les activités connexes non examinées afin de délimiter l'intervention. Il peut préciser la nature et l'étendue des travaux réalisés » ;

Copyright © 2015 Eyrolles.

- **la période couverte par la mission :** la période des opérations couverte par le périmètre de la mission, généralement à partir d'une certaine date ou pour une certaine période ;
- **les observations telles que définies par le processus d'évaluation et de remontée de l'information (encadré 14-4) et les recommandations :** les détails concernant la communication des observations et recommandations seront abordés plus loin dans ce chapitre ;

Périmètre (ou champ)

Ce qui est ou non inclus dans une mission.

- **les conclusions de la mission et la notation éventuelle :** l'évaluation, par l'audit interne, de l'adéquation de la conception et du fonctionnement effectif des contrôles sur lesquels porte l'audit. Une notation peut être attribuée en plus par l'audit interne au domaine audité si un système de notation est utilisé. Les notes sont abordées en détail plus loin. La MPA 2410-1, Contenu de la communication, donne les informations suivantes concernant les conclusions : « les conclusions et les opinions sont les évaluations de l'auditeur interne sur les conséquences des observations et recommandations sur les activités auditées. Habituellement, elles situent les observations et recommandations dans la perspective de leurs implications globales. Les conclusions de la mission sont clairement exposées dans le rapport d'audit. Elles peuvent exposer, entre autres, dans quelle mesure les objectifs opérationnels et les programmes sont conformes à ceux de l'organisation, si les buts et objectifs de l'organisation sont atteints, et si l'activité examinée fonctionne comme prévu. L'opinion peut consister en une évaluation globale des contrôles ou être limitée à des contrôles spécifiques ou certains aspects de la mission » ;
- **le plan d'action du management pour remédier aux observations exposées (le cas échéant) :** la synthèse de la réponse du management aux observations d'audit contenues dans la communication finale. Le plan de mesures correctives convenu, assorti d'un échéancier de réalisation qui servira de base aux travaux de suivi de l'audit interne, devra également être inclus. Le plan d'action doit comporter le nom de la (ou des) personne(s) qui doit (doivent) rendre des comptes et/ou est (sont) en charge de sa réalisation.

Conclusion

Évaluation, par l'audit interne, de l'adéquation de la conception et du fonctionnement effectif des contrôles sur lesquels porte l'audit.

De plus, la MPA 2410-1, Contenu de la communication, précise : « les rapports définitifs d'audit peuvent comporter des informations sur le contexte et des synthèses. Les informations sur le contexte peuvent présenter les entités et activités examinées et fournir des explications. Le statut des observations, conclusions et recommandations des rapports précédents peut aussi être repris ; on peut aussi indiquer si cet audit est une mission inscrite au plan d'audit [...] ou répondant à une demande particulière. » Et d'ajouter : « L'auditeur interne peut communiquer sur les réalisations de l'audité, qu'il s'agisse d'améliorations apportées depuis le dernier audit, ou de la mise en place d'activités bien maîtrisées. Cette

Copyright © 2015 Eyrolles.

information peut être nécessaire pour représenter fidèlement les conditions actuelles d'exercice, offrir une perspective et assurer un équilibre dans le rapport d'audit. »

Systèmes de notation

Système de notation

Attribution d'une évaluation numérique ou descriptive aux résultats de la mission dans le but de les comparer ou d'en établir la tendance par rapport aux autres résultats de mission.

Il n'existe pas une manière unique d'exprimer les conclusions d'une mission (observations, recommandations et conséquences de ces observations et recommandations sur l'évaluation que fait le management des activités examinées). Cela va du recensement et de la hiérarchisation des observations découlant de la mission d'assurance à l'expression d'une conclusion générale sur l'efficacité et l'efficience des activités de contrôle examinées. Comme souligné dans le chapitre 12, *Introduction au processus d'audit*, l'évaluation des contrôles par l'audit interne, qui est incluse dans le rapport définitif de la mission, peut être énoncée de manière positive ou négative. Si l'audit interne choisit d'affirmer que le système de contrôle interne est conçu de manière adéquate et fonctionne de manière effective, il donne une assurance de forme positive. Si, en revanche, il choisit de communiquer que rien ne peut le porter à penser que le système de contrôle interne n'est pas conçu de manière adéquate et ne fonctionne pas de manière effective, il donne une assurance de forme négative. Les deux manières d'exprimer l'assurance sont acceptables et conformes aux *Normes*. Cependant, de nombreux responsables de l'audit interne considèrent que l'assurance de forme positive constitue une bonne pratique. Les orientations (*Guidance*) données par l'IIA vont dans ce sens : « L'assurance positive (ou assurance raisonnable) confère le niveau d'assurance le plus élevé, c'est une des opinions d'audit la plus solide »[3]. Lorsque l'audit interne fournit une assurance de forme négative (assurance modérée), il n'assume « aucune responsabilité quant au caractère suffisant du périmètre et des procédures d'audit pour détecter tous les problèmes ou points douteux »[4].

Assurance positive

Note ou conclusion de l'auditeur interne qui procure des assurances spécifiques à propos d'une mission.

De nombreuses fonctions d'audit interne et comités d'audit ont opté pour un système formel de notation qu'ils associent à leurs conclusions. Ce système permet au management et au comité d'audit de comparer les résultats des missions d'assurance entre les différents domaines fonctionnels d'une organisation. Il procure également un outil permettant, pour un dossier donné, de déterminer la tendance des résultats de l'audit dans le temps. Il existe de nombreux systèmes de notation, depuis les systèmes numériques (par exemple de 1 à 5) à des systèmes de nature plus descriptive (qui peuvent, par exemple, classer les résultats selon qu'ils sont satisfaisants ou non). Si une fonction d'audit interne choisit d'utiliser un système de notation, il doit y avoir concordance entre la note affectée et la conclusion de l'audit interne relative aux critères de qualité retenus par le management, à savoir que le système de contrôle interne sur lequel a porté la mission d'assurance est conçu de manière

Copyright © 2015 Eyrolles.

Assurance négative (ou limitée)

Note ou conclusion indiquant que rien de négatif n'a retenu l'attention de l'auditeur interne.

adéquate et fonctionne de manière effective. Lorsque la conclusion et/ou la notation de l'audit interne ne concorde pas avec les critères de qualité initialement retenus par le management, ce dernier devra revenir sur ces critères afin qu'ils correspondent à la conclusion de l'audit interne et notamment à la notation. Par exemple, une notation faible indique que l'audit interne a découvert qu'un (ou plusieurs) risque(s) n'avai(en)t pas été ramené(s) à un niveau tolérable. Dans ce cas, le management doit réévaluer son évaluation de l'adéquation de la conception et du fonctionnement effectif

ENCADRÉ 14-11

EXEMPLE DE COMMUNICATION FINALE FORMELLE (RAPPORT D'AUDIT)

À l'attention de : Chef comptable, Books 2 Buy Holding Corp.
De la part de : Directeur de mission/superviseur, Books 2 Buy Holding Corp.
OBJET : Books 2 Buy Holding Corp., Rapport d'audit sur les décaissements
NOTE SATISFAISANTE
DATE : 27 avril 20XX

L'audit interne de Books 2 Buy a réalisé une revue de contrôle interne du service des décaissements le 24 mars 20XX. Le périmètre de la revue, effectuée à compter du 10 février 20XX, consistait à évaluer l'adéquation de la conception et le fonctionnement effectif du système de contrôle interne au sein du processus de décaissements. La revue comportait des procédures de vérification visant à s'assurer du caractère adéquat des autorisations, de la validité, de la précision, de la rapidité d'exécution, de l'exhaustivité, de l'existence, du classement, de la confidentialité, de l'intégrité et de la disponibilité des livres, registres et autres documents pertinents concernant les décaissements effectués pendant l'exercice clos le 31 décembre 20XX.

Le périmètre de l'examen incluait, de manière non exhaustive, la documentation, l'évaluation et le test des éléments suivants :

- procédures de réception et de validation des demandes de décaissement ;
- procédures d'approbation et de traitement des décaissements (virements ou chèques) ;
- procédures de validation des décaissements pour diffusion ;
- procédures de comptabilisation et d'établissement de la balance ;
- procédures de rapprochement des différents journaux par rapport aux comptes collectifs du grand livre pour les décaissements.

Conclusion
Selon notre opinion, le processus de décaissement est satisfaisant et le système de contrôle interne est acceptable, d'où une note d'audit SATISFAISANTE. Cette note indique que les contrôles internes sont globalement suffisants pour protéger les actifs et minimiser l'exposition à des pertes. Elle signale également que peu de déficiences ont été repérées et que le management fait preuve d'un niveau d'attention approprié. L'annexe A présente la définition des notes attribuées à l'environnement de contrôle interne.

Plan d'action du management
Le management a élaboré un plan d'action satisfaisant pour remédier aux observations énumérées dans ce rapport. Le rapport ci-joint donne une explication détaillée de nos observations et recommandations, ainsi que la réponse du management.

Copies à :

Président du Conseil	Président du comité d'audit	Directeur juridique
Directeur général	Auditeur externe	Directeur administratif
Directeur financier	Contrôleur de gestion	Responsable de la conformité

Copyright © 2015 Eyrolles.

ENCADRÉ 14-11
Suite

EXEMPLE DE COMMUNICATION FINALE FORMELLE, *SUITE*

Page 2

- **Améliorer les procédures d'examen et d'autorisation des décaissements.**

Les tests que nous avons effectués sur le système de décaissements ont confirmé que ce système rejetait, de manière appropriée, toutes les saisies de factures en double sur la base du numéro de facture. Cependant, le système ne compare pas les autres informations sur les factures pour rechercher d'éventuels doublons. Nos tests ont indiqué que le système acceptait les factures lorsqu'un chiffre ou un symbole est ajouté à la fin du numéro de facture, ce qui créé la possibilité que des paiements soient effectués en double. Or, la réception des marchandises ou des services ne doit être comptabilisée et traitée qu'une seule fois.

En conséquence, nous avons étendu nos tests de manière à inclure toutes les factures traitées pour règlement entre le 1er janvier 20XX et le 31 décembre 20XX à la recherche d'éventuels paiements en double. À l'aide d'un logiciel d'audit généralisé, nous avons sélectionné tous les décaissements de même montant pour un fournisseur donné, indépendamment du numéro de facture ou de la date de règlement. Notre recherche a mis en évidence plusieurs cas (14 factures pour un montant total de 357 782) dans lesquels les collaborateurs du service CF ont pu saisir certaines factures une deuxième fois lorsque le fournisseur a émis un duplicata de facture. Une enquête auprès de ces collaborateurs a indiqué qu'ils ne savaient pas qu'il était possible que ces factures aient déjà été reçues et qu'ils avaient ajouté un caractère à la fin pour en faciliter le traitement. Dans d'autres cas, le fournisseur a émis un duplicata de facture qui porte un numéro différent (généralement supérieur au précédent) et les collaborateurs du service CF ne se sont pas aperçus qu'il pouvait s'agir d'une facture en double. En conséquence, les créances et les actifs ou charges correspondants ont été surestimés de 357 782 et ce même montant a été décaissé indûment. Une analyse des prévisions budgétaires par rapport aux dépenses réelles est réalisée chaque mois par tous les responsables de service et les propriétaires de centre de coûts, mais cette analyse n'est pas conçue pour déceler des erreurs de ce type.

Nous recommandons que soit développé un programme d'interrogation des données qui compare le nom du fournisseur, le montant de la facture, la date de celle-ci et toute autre caractéristique importante pour le service de la comptabilité fournisseurs aux caractéristiques des factures traitées précédemment ; ceci avant qu'il soit procédé aux décaissements pour chaque lot. Les résultats de cette interrogation doivent être analysés par le superviseur du service afin de déceler d'éventuels doublons. Toutes les transactions suspectes doivent être sorties du lot et examinées avec attention avant d'être réglées.

Réponse du management :

Un programme d'interrogation des données sera développé. Il comparera les caractéristiques « principales » de la facture (montant, description du fournisseur, numéro de facture et date) aux factures déjà traitées et signalera qu'une facture peut être un doublon si l'une des caractéristiques est identique. Ce programme sera lancé avant qu'un lot (*batch*) soit traité et examiné par le superviseur du service. Si des doublons potentiels sont identifiés, ces transactions seront sorties du lot et examinées avec attention avant d'être réglées.

Devoir de rendre compte : Chef comptable

Responsabilité : Superviseur du service de la comptabilité fournisseurs

Date de mise en œuvre : 30 juin 20XX

Copyright © 2015 Eyrolles.

des contrôles existants. Elle doit également chercher à comprendre pourquoi sa propre auto-évaluation n'a pas identifié les déficiences. Quelle que soit la manière dont l'audit interne décide de présenter ses conclusions, l'objectif ultime est de procurer à l'audité et aux autres destinataires de la communication des informations

suffisantes pour comprendre les conséquences des observations de l'audit interne et la manière dont les recommandations peuvent remédier aux causes profondes de ces observations.

Certaines fonctions d'audit interne choisissent délibérément de ne pas noter les rapports d'audit, parce qu'elles pensent que, si elles diffusent une communication assortie d'une notation montrant que le domaine ou le processus audité est loin d'être satisfaisant, cela aura pour résultat des rapports antagonistes, opposés entre l'audit interne et le reste de l'organisation. Moody's Investors Service n'est toutefois pas de cet avis et avance que la notation des rapports d'audit constitue une bonne pratique : « [...] les professionnels de l'audit doivent adopter un système de classement ou de notation simple et logique de leurs rapports, afin d'aider les utilisateurs à distinguer les rapports qui posent problème des autres rapports d'audit. Le comité d'audit doit être capable de distinguer les différents types de rapports produits par l'équipe d'audit :

- les rapports qui présentent le dispositif concernant un niveau de criticité élevé et qui recommandent des mesures correctives significatives ;
- les rapports qui énoncent des déficiences à corriger, mais qui n'indiquent pas de manquement significatif ;
- les rapports qui font le diagnostic d'un dispositif de contrôle pertinent, même si des possibilités d'amélioration sont mentionnées. »[5]

ENCADRÉ 14-11
Suite

EXEMPLE DE COMMUNICATION FINALE FORMELLE, *SUITE*

Annexe A
Les rapports d'audit de Books 2 Buy portent un jugement global sur l'environnement de contrôle sur la base des objectifs, du périmètre et des conclusions des travaux détaillés effectués. L'environnement de contrôle peut être qualifié de :

- **Satisfaisant**
Dans l'ensemble, les contrôles sont conçus de manière adéquate et fonctionnent de manière effective pour ramener le risque sous-jacent à un niveau acceptable. Ce jugement indique qu'il y a relativement peu de déficiences (mineures) et que le management y porte un niveau d'attention approprié.

- **Doit s'améliorer**
Dans l'ensemble, les contrôles doivent être améliorés en permanence pour ramener le risque sous-jacent à un niveau acceptable. Ce jugement indique que le nombre et la nature des déficiences nécessitent que le management y accorde rapidement de l'attention afin de ramener l'exposition à un niveau plus acceptable.

- **Insuffisant**
Dans l'ensemble, les contrôles ne sont pas conçus de manière adéquate et/ou ne fonctionnent pas de manière effective pour ramener le risque sous-jacent à un niveau acceptable. Ce jugement indique que le nombre et la nature des déficiences sont d'une importance critique et nécessitent que le management y accorde beaucoup d'attention. Des actions correctives immédiates sont essentielles pour éviter que la dégradation ne se poursuive.

Copyright © 2015 Eyrolles.

Certaines fonctions d'audit interne attribuent non seulement une note globale aux rapports d'audit, mais également une note spécifique à chaque problématique abordée dans ces rapports. Cette méthode permet de différencier les problématiques, de telle sorte qu'un niveau approprié d'attention et de priorité leur soit accordé.

DIFFUSION DES COMMUNICATIONS FINALES FORMELLES ET INFORMELLES

Une fois toutes les observations identifiées et évaluées, tant individuellement que globalement, conformément au processus d'évaluation des observations et de remontée de l'information, elles doivent être communiquées conformément aux résultats de ce processus. La MPA 2410-1, Contenu de la communication, réitère l'importance de cette communication en affirmant que « les observations sont des exposés pertinents des faits. L'auditeur interne communique les observations nécessaires pour soutenir ses conclusions et recommandations, et éviter les malentendus. L'auditeur interne peut communiquer de manière informelle les informations ou observations moins importantes. »

Avant que les communications puissent être diffusées, elles doivent être revues et approuvées par le responsable de l'audit interne ou son délégué. Puis, « le responsable de l'audit interne adresse le rapport définitif au management de l'activité auditée et aux membres de l'organisation qui peuvent s'assurer que les résultats de l'audit recevront l'attention nécessaire et qui peuvent entreprendre les actions correctives qui s'imposent ou s'assurer que de telles mesures seront prises. Lorsque cela est approprié, le responsable de l'audit interne peut adresser une note de synthèse aux membres de l'organisation occupant un poste plus élevé dans la hiérarchie. Lorsque cela est prévu dans la charte d'audit interne ou par une règle interne, le responsable de l'audit interne communique également les résultats de la mission aux personnes intéressées ou concernées, telles que les auditeurs externes et le Conseil » (MPA 2440-1, Diffusion des résultats de la mission).

De plus, la MPA 2410-1, Contenu de la communication, affirme qu'« il peut ne pas être opportun de communiquer certaines informations à tous les destinataires du rapport, notamment lorsqu'il s'agit de renseignements couverts par le secret professionnel, protégés ou relatifs à des actes irréguliers ou illégaux. Ces informations sont alors incluses [par le responsable de l'audit interne] dans un rapport distinct [et,] si les faits rapportés impliquent la direction générale, le rapport est adressé au Conseil ».

La communication des résultats de la mission d'assurance peut être formelle ou informelle en fonction du résultat tel que déterminé par le processus d'évaluation des observations et de remontée

Copyright © 2015 Eyrolles.

de l'information. Cependant, pour chaque mission d'assurance, il y aura toujours une communication finale formelle, même s'il n'y a pas d'observations à communiquer au management.

Communication formelle

Généralement, les destinataires d'un rapport formel d'une mission d'assurance sont la direction générale, le comité d'audit, l'auditeur externe de l'organisation et/ou le management de l'audité. Il convient de réaliser une communication formelle lorsque les contrôles évalués dans le cadre d'une mission d'assurance sont :

- compromis de manière non significative bien que des contrôles clés soient concernés ;
- compromis de manière significative ;
- compromis de manière critique.

Traditionnellement, les rapports formels se présentent sous forme papier (rapports écrits) ou bien, s'ils sont diffusés par voie électronique, sous forme d'un document Word. À mesure que la technologie progresse, l'audit interne évolue vers d'autres formats, comme les présentations PowerPoint. Le format utilisé pour le rapport importe peu (dans la mesure où il reste adapté à l'information présentée ainsi qu'à ses destinataires). En revanche, la communication doit impérativement comporter toutes les composantes d'une communication formelle.

Comme déjà indiqué plus haut dans ce chapitre, les communications formelles constituent le dossier d'archive final et permanent des résultats d'une mission d'assurance. En tant que telles, elles doivent renfermer les informations nécessaires pour refléter précisément les travaux effectués et les conclusions tirées. Il ne faut pas oublier, comme souligné précédemment, que toutes les communications formelles doivent comporter :

- l'objet et le périmètre de la mission ;
- le calendrier d'exécution de l'audit ;
- les observations et recommandations (résultats) de l'audit, le cas échéant ;
- la conclusion (opinion et/ou note) de l'audit interne ;
- la réaction du management (plan d'action) face aux recommandations.

Copyright © 2015 Eyrolles.

Les informations ci-dessus doivent être organisées clairement et incluses dans le rapport dans un langage concis et précis qui ne laisse pas de place à l'ambiguïté. L'encadré 14-11 présente un exemple de communication finale formelle.

Communication informelle

Lorsqu'à l'issue de l'application du processus d'évaluation et de remontée de l'information, les observations sont qualifiées de non significatives, l'audit interne peut choisir de communiquer ces observations de manière informelle, au management du domaine audité, *via* une note de service, un courriel, une réunion en face à face ou une conférence téléphonique. Peu importe la forme ou le support retenu(s), les communications informelles portant sur des missions d'assurance, dont les observations sont non significatives, sont tout de même considérées comme des communications finales et contribuent à ce que l'audit interne remplisse ses obligations de reporting conformément aux *Normes*. Les communications informelles finales sont exclusivement destinées au management du domaine audité. La communication informelle est considérée comme appropriée si et seulement si, pendant le processus d'évaluation des observations et de remontée de l'information, toutes les observations ont été jugées non significatives, ne compromettant aucun contrôle clé. La communication informelle couvre les observations non significatives liées aux contrôles secondaires susceptibles d'être compromis et, là encore, elle sera uniquement diffusée au management du domaine qui a fait l'objet de la mission. L'encadré 14-12 présente un exemple de communication finale informelle. Même lorsqu'une communication informelle est indiquée, ceci afin de s'acquitter pleinement des obligations énoncées dans les *Normes* concernant la communication des résultats d'une mission d'assurance, il reste nécessaire de faire savoir à la direction générale, au comité d'audit et à l'auditeur externe qu'aucune observation ne porte sur des contrôles clés.

Communication informelle

Communication couvrant les observations non significatives liées aux contrôles secondaires susceptibles d'être compromis.

Autres obligations à respecter dans un rapport de mission d'assurance

Les *Normes* donnent des orientations sur la qualité des rapports de missions d'assurance et spécifient ce qu'il faut faire en cas d'erreur ou d'omission. Voici les normes et les Modalités Pratiques d'Application pertinentes en la matière.

Copyright © 2015 Eyrolles.

ENCADRÉ 14-12

EXEMPLE DE COMMUNICATION FINALE INFORMELLE (NOTE DE DISCUSSION AVEC LE MANAGEMENT)

À l'attention de : Chef comptable, Books 2 Buy Holding Corporation
De la part de : Directeur de mission/superviseur, Books 2 Buy Holding Corporation
OBJET : Conclusions de la discussion avec le management – Processus de décaissements
DATE : 27 avril 20XX

L'audit interne a effectué une revue du processus de décaissement afin d'évaluer l'adéquation de la conception et le fonctionnement effectif du système de contrôle interne pour les décaissements. Pendant l'examen, l'observation suivante a été portée à notre attention. Elle affecte l'efficience opérationnelle de votre service. Selon notre opinion, cette observation ne constitue pas une déficience de contrôle devant être signalée et, en conséquence, elle n'est pas incluse dans le rapport d'audit formel.

Nous recommandons au management d'évaluer l'impact de l'observation sur l'efficience opérationnelle et le rapport coût/avantage qui émane de la mise en œuvre d'une éventuelle action corrective.

Renforcer le processus de mise à jour du règlement relatif à la délégation du pouvoir d'effectuer des décaissements.

Il ressort de notre examen du règlement, relatif à la délégation du pouvoir d'effectuer des décaissements, que sept personnes sont dotées de ce pouvoir alors qu'elles ne font plus partie de la société et que neuf personnes dont la fonction est associée à ce pouvoir ne figurent pas dans le règlement parmi les personnes disposant de ce pouvoir. Le pouvoir de décider du décaissement de fonds doit être limité à des personnes actuellement employées par la société, habilitées à effectuer des décaissements conformément au règlement édicté par la société et dont les responsabilités liées au poste qu'elles occupent justifient qu'elles disposent de ce pouvoir. Si ces cadrages ne sont pas mis en place, des décaissements risquent d'être effectués par des personnes non habilitées.

En poursuivant l'enquête, nous avons constaté que la procédure relative à la délégation du pouvoir d'effectuer des décaissements est mise à jour seulement deux fois par an. Actuellement, aucune mise à jour n'est effectuée lorsque les collaborateurs ou les responsabilités des personnes habilitées changent. Concernant les personnes qui font usage du pouvoir d'effectuer des décaissements, mais qui ne sont pas listées dans le règlement de l'organisation, toutes étaient dûment habilitées à effectuer des décaissements et devaient le faire afin de s'acquitter des responsabilités associées à leur fonction. De plus, nos tests ont montré que les droits d'accès au système de décaissements sont supprimés dès qu'un collaborateur quitte l'organisation. Par conséquent, même si des personnes qui ont quitté l'organisation restent des signataires habilités selon le règlement de l'organisation, elles ne peuvent pas accéder au système pour approuver des décaissements. Dans les sept cas notés durant notre examen, l'accès au système avait été désactivé lorsque les collaborateurs ont quitté l'organisation. Enfin, nous avons constaté qu'une analyse des prévisions budgétaires par rapport aux dépenses réelles était réalisée chaque mois par tous les responsables de service et les propriétaires de centres de coûts. Tout décaissement d'importance non autorisé sera ainsi identifié et fera immédiatement l'objet d'une enquête.

Nous recommandons au management d'envisager de renforcer les procédures de mise à jour du règlement relatif à la délégation du pouvoir d'effectuer des décaissements. Les personnes auxquelles ce pouvoir a été conféré doivent être incluses dans le règlement par le biais d'une annexe énumérant les personnes habilitées à effecteur des décaissements. Cette annexe pourrait être actualisée dans le cadre du processus d'intégration des nouveaux collaborateurs et de radiation des anciens, à l'instar de l'ajout ou de la suppression des droits d'accès au système, ce qui permettrait une actualisation du règlement au fur et à mesure que des changements surviennent.

Réponse du management :

Le management pense que le risque de décaissements non autorisés est minime et, par conséquent, accepte de conserver le niveau de risque identifié entre deux mises à jour du règlement de l'organisation. Cependant, le management perçoit l'intérêt qu'il y a à distinguer la liste des personnes habilitées du règlement lui-même, et à inclure l'actualisation de cette liste aux procédures liées à l'arrivée et au départ de collaborateurs. Le management va évaluer le rapport coût/avantage que présentent les changements proposés pour le processus d'actualisation et de conservation du règlement de délégation du pouvoir d'effectuer des décaissements.

Devoir de rendre compte : Directeur financier

Responsabilité : Chef comptable

Date de mise en œuvre : Sans objet

Copyright © 2015 Eyrolles.

Qualité de la communication

La Norme 2420, Qualité de la communication, précise : « la communication doit être exacte, objective, claire, concise, constructive, complète et émise en temps utile ». L'interprétation de la Norme 2420 définit ces termes :

- une communication **exacte** ne contient pas d'erreur ou de déformation, et est fidèle aux faits sous-jacents ;
- une communication **objective** est juste, impartiale, non biaisée et résulte d'une évaluation équitable et mesurée de tous les faits et circonstances pertinents ;
- une communication **claire** est facilement compréhensible et logique. Elle évite l'utilisation d'un langage excessivement technique et fournit toute l'information significative et pertinente ;
- une communication **concise** va droit à l'essentiel et évite tout détail superflu, tout développement non nécessaire, toute redondance ou verbiage ;
- une communication **constructive** aide l'audité et l'organisation, et conduit à des améliorations lorsqu'elles sont nécessaires ;
- une communication **complète** n'omet rien qui soit essentiel aux destinataires cibles. Elle intègre toute l'information significative et pertinente, ainsi que les observations permettant d'étayer les recommandations et conclusions ;
- une communication **émise en temps utile** est opportune et à propos, elle permet au management de prendre les actions correctives appropriées en fonction du caractère significatif de la problématique.

Définition des notations

Il est important de veiller à ce que les destinataires d'un rapport d'audit comprennent la signification des notations utilisées par l'audit interne.

La MPA 2420-1, Qualité de la communication, donne des orientations supplémentaires concernant les mesures que les auditeurs internes doivent prendre pour faire en sorte que la communication respecte les critères de la Norme 2420. En particulier, les auditeurs internes doivent :

- collecter, évaluer et synthétiser les données et les preuves avec soin et précision ;
- développer et énoncer les constats, conclusions et recommandations sans préjugé, parti pris, intérêt personnel ni influence inappropriée ;
- améliorer la clarté en évitant l'utilisation d'un langage excessivement technique et en fournissant toute l'information significative et pertinente dans ce contexte ;
- préparer des communications dont chaque élément est porteur de sens tout en étant concises ;

Critères de qualité d'une communication :

– exactitude ;
– objectivité ;
– clarté ;
– concision ;
– constructivité ;
– complétude ;
– émission en temps utile.

Copyright © 2015 Eyrolles.

- adopter un contenu et un ton utiles, positifs et bienveillants qui convergent avec les objectifs de l'organisation ;
- s'assurer que la communication est cohérente avec le style et la culture de l'organisation ;
- prévoir le délai de présentation des résultats de la mission afin d'éviter des contretemps excessifs.

Erreur

Inexactitude ou omission non intentionnelle, de la part de l'audit interne, concernant des informations importantes dans le rapport de la mission.

Erreurs et omissions

Même si l'on accorde beaucoup d'attention à ce qu'un rapport de mission soit exact et complet, il arrive qu'il comporte une erreur ou omette un élément. Les *Normes* mentionnent ce cas dans la MPA 2421, Erreurs et omissions : « si une communication finale contient une erreur ou une omission significative, le responsable de l'audit interne doit faire parvenir les informations corrigées à tous les destinataires de la version initiale ». Une erreur se définit comme une inexactitude ou omission non intentionnelle concernant des informations importantes dans le rapport de la mission.

SURVEILLANCE ET SUIVI

Les responsabilités de l'audit interne ne prennent pas fin avec la diffusion des résultats de la mission. Rappelons que, pendant la mission, lorsque les observations ont été faites, le management du domaine qui faisait l'objet de la mission d'assurance s'est engagé soit à entreprendre des actions correctives, soit à ne rien faire. Le processus collaboratif en place pendant la mission est la garantie que l'audit interne était d'accord avec le plan d'action proposé et documenté dans le rapport définitif. En conséquence, des procédures de surveillance et de suivi sont élaborées afin que les observations soient prises en compte et les problèmes résolus conformément à la réponse du management incluse dans le rapport définitif de la mission. D'après les *Normes*, « le responsable de l'audit interne doit mettre en place un processus de suivi permettant de surveiller et de garantir que des mesures ont été effectivement mises en œuvre par le management ou que la direction générale a accepté de prendre le risque de ne rien faire » (Norme 2500.A1). En d'autres termes, le management doit choisir soit de mettre en place les changements pour remédier à l'observation, soit d'accepter le risque associé à la décision de ne rien faire. Si des changements sont introduits, l'audit interne doit avoir mis en place un processus de surveillance et de suivi des actions décidées afin de s'assurer que le management fait bien ce qu'il avait l'intention de faire.

Le calendrier de suivi des observations dépend de l'importance (non significative, significative ou critique) de l'observation, telle qu'elle a été déterminée au cours du processus d'évaluation des

Copyright © 2015 Eyrolles.

observations et de remontée de l'information décrit dans l'encadré 14-4. En règle générale, plus l'observation est critique, plus l'audit interne effectue un suivi rapide et régulier. Le suivi d'une observation consiste à la fois à confirmer au client que les actions correctives ont été mises en œuvre, et à exécuter à nouveau les procédures de test appropriées afin de s'assurer que le risque applicable est maîtrisé. Selon les règles de l'audit interne, le calendrier de ces tests dépendra de divers facteurs tels que la maturité, l'importance et le type de l'observation. Une observation n'est pas réputée résolue tant que les tests exécutés à nouveau par l'audit interne n'ont pas confirmé que le contrôle défaillant ou manquant est conçu de manière adéquate et fonctionne de manière effective, et que le risque associé est maîtrisé au vu des paramètres de tolérance au risque établis au sein de l'organisation. Afin de garantir un niveau d'attention approprié et un traitement en temps opportun, des observations non résolues sont régulièrement signalées au management du domaine qui a fait l'objet de la mission d'assurance. En outre, si une observation non résolue est non significative mais porte sur des contrôles clés, significative ou critique, elle doit également être signalée à la direction générale. Si une observation non résolue qui a trait au contrôle interne relatif au reporting financier est significative ou critique, elle doit être signalée au comité d'audit et à l'auditeur externe. En règle générale, ce reporting est réalisé au moins une fois par trimestre.

Si le management a choisi d'accepter le risque, les *Normes* indiquent que le responsable de l'audit interne doit émettre un jugement quant à la prudence de cette décision. De plus, « lorsque le responsable de l'audit interne conclut que le management a accepté un niveau de risque qui pourrait s'avérer inacceptable pour l'organisation, il doit examiner la question avec la direction générale. Si le responsable de l'audit interne estime que le problème n'a pas été résolu, il doit soumettre la question au Conseil » (Norme 2600, Communication relative à l'acceptation des risques).

L'interprétation de cette norme précise que cette obligation incombe au responsable de l'audit interne, quelle que soit la situation : « l'identification du niveau de risque accepté par le management peut résulter d'une mission d'assurance, d'une mission de conseil, du suivi des plans d'actions du management à la suite de missions d'audit interne antérieures, ou d'autres moyens. » La norme conclut en outre que « la réponse au risque ne relève pas du responsable d'audit interne ».

Si, en revanche, le management accepte la responsabilité de mettre en œuvre des changements pour remédier aux observations, l'audit interne doit suivre les progrès du management. Les procédures de suivi régulières doivent veiller à ce que les améliorations soient apportées dans les délais indiqués dans le rapport définitif de la mission. En fin de compte, il revient au responsable de l'audit

Copyright © 2015 Eyrolles.

interne de « mettre en place et tenir à jour un système permettant de surveiller la suite donnée aux résultats communiqués au management » (Norme 2500, Surveillance des actions de progrès). Ce système doit être décrit dans le manuel d'audit interne. Au minimum, des actions de suivi doivent être documentées et inscrites dans les papiers de travail de l'audit interne de la mission d'assurance suivante portant sur le domaine qui a été l'objet du premier audit. De plus, lorsque les observations ont été jugées significatives ou critiques, une mission de suivi est généralement prévue avec pour objectif d'évaluer et de tester si les contrôles portant sur le domaine en question ont été améliorés et les risques ramenés à un niveau acceptable. Cette mission doit être planifiée, exécutée et faire l'objet d'une communication de manière analogue à toute autre mission d'assurance.

En 2009, le COSO a publié le document *Guidance on Monitoring Internal Control Systems*. Il s'agit d'orientations sur la surveillance des systèmes de contrôle interne, détaillées dans le chapitre 6, *Le contrôle interne*. Si ces orientations se concentrent sur les activités du management au sein d'une organisation, certains aspects sont également pertinents pour l'audit interne.

Par exemple, lorsqu'il examine de façon ciblée les améliorations apportées aux contrôles, l'audit interne a la responsabilité d'en communiquer le résultat aux personnes déjà destinataires du rapport relatif à la première mission d'assurance. De plus, lorsque les contrôles, qui ont été jugés compromis de manière significative ou critique dans le premier rapport, ont trait à la communication des informations financières, la réglementation sur le reporting financier des pays dans lesquels opère l'organisation doit être suivie. En outre, la correction de la déficience significative ou de la faiblesse importante, ainsi que le résultat de l'examen ciblé, doivent être notifiés à la direction générale, au comité d'audit et à l'auditeur externe. Dans le cas d'une faiblesse importante, la correction et les améliorations correspondantes apportées aux contrôles doivent également être communiquées aux tiers conformément à la législation du pays dans lequel opère l'organisation.

AUTRES TYPES DE MISSIONS

Ce chapitre traite uniquement de la communication des résultats d'une mission d'assurance. Pour les missions de conseil, y compris les enquêtes, projets, efforts de *due diligence*, etc., les critères de communication sont différents. Pour plus d'informations sur les critères pertinents pour les rapports relatifs à une mission de conseil, veuillez vous reporter au chapitre 12, *Introduction au processus d'audit*, et au chapitre 15, *La mission de conseil*.

Copyright © 2015 Eyrolles.

RÉSUMÉ

La communication fait partie intégrante de toute mission d'assurance et se déroule tout au long des communications intermédiaires et finales. En raison de leur immédiateté, les communications intermédiaires ont tendance à revêtir la forme d'entretiens en face à face, de conférences téléphoniques et de courriels, tandis que les communications finales ont tendance à être documentées de manière plus formelle par des rapports ou des notes de service.

Une communication finale diffuse les résultats d'une mission d'assurance et doit présenter :

- l'objet et le périmètre de la mission ;
- la période couverte par la mission ;
- les observations à l'issue du processus d'évaluation et de remontée de l'information, et les recommandations ;
- les conclusions de la mission et la note (le cas échéant) ;
- le plan d'action du management pour remédier aux observations rapportées.

Chaque observation rapportée doit comporter les éléments suivants : référentiels, faits, causes et conséquences. Il doit être préconisé de remédier à chaque observation. L'importance de ces observations, tant individuellement que globalement, ainsi que le fait que les contrôles clés soient compromis ou non, dictera le caractère formel ou informel de la communication ou l'adéquation des deux types de communication. Une communication formelle est généralement adressée à la direction générale, au comité d'audit, à l'auditeur externe de l'organisation et/ou au management de l'audité. Il convient de réaliser une communication formelle lorsque l'évaluation des contrôles conclut qu'ils sont compromis de manière :

- non significative bien que des contrôles clés soient concernés ;
- significative ;
- critique.

Une communication informelle est généralement adressée uniquement au management du domaine audité et n'est pertinente que si les observations rapportées sont non significatives et qu'aucun contrôle clé n'est compromis.

Toute communication, qu'elle soit formelle ou informelle, intermédiaire ou finale, doit être « exacte, objective, claire, concise, constructive, complète et émise en temps utile », conformément à la Norme 2420, Qualité de la communication. De plus, si elle est significative, toute erreur ou omission identifiée dans une

Copyright © 2015 Eyrolles.

communication finale doit être corrigée et communiquée « à tous les destinataires de la version initiale » (Norme 2421, Erreurs et omissions).

Le rôle de l'audit interne ne s'achève pas avec la diffusion des communications finales. Il faut effectuer un suivi et une surveillance, afin de vérifier que le management a mis en œuvre le plan d'action dont il a été convenu en vue de remédier à toutes les observations présentes dans la communication finale. Pour cela, il faut notamment vérifier auprès du management que les actions de progrès sont réalisées dans les délais convenus, ce qui peut déboucher sur une mission de suivi qui permettra d'évaluer si les contrôles ont été suffisamment renforcés pour être à même de ramener les risques à un niveau acceptable.

Si le management de l'audité choisit de ne rien faire pour remédier aux observations communiquées, le responsable de l'audit interne doit évaluer la situation. Si le niveau de risque est supérieur à la tolérance au risque, la direction générale doit en être informée et, au besoin, le Conseil.

Copyright © 2015 Eyrolles.

Questions de révision

1. En quoi les missions d'assurance de l'audit interne sont-elles liées aux critères de qualité retenus par la direction générale concernant le système de contrôle interne de l'organisation ?

2. À quel moment et de quelle manière la communication des résultats d'une mission d'assurance intervient-elle ?

3. Comment les observations d'une mission d'assurance sont-elles identifiées ?

4. Quelles sont les étapes que suit un auditeur interne pour évaluer les observations identifiées pendant une mission d'assurance ?

5. Qu'est-ce qui distingue une observation significative d'une observation non significative ? Qu'est-ce qui distingue une observation critique d'une déficience significative ?

6. Quelles informations devraient être contenues dans une description des observations d'une mission d'assurance ? Indice : voir l'encadré 14-8.

7. Pourquoi la communication intermédiaire et la communication préliminaire sont-elles importantes dans une mission d'assurance ?

8. Quel est l'objectif d'une réunion de clôture ?

9. Quelles sont les informations qui doivent être présentes dans la communication finale des résultats d'une mission d'assurance bien conçue ?

10. Quelle est la différence entre une assurance positive et une assurance négative dans un rapport d'audit ?

11. Quelle différence y a-t-il entre une communication finale formelle et une communication finale informelle, et quand doit-on utiliser l'une plutôt que l'autre ?

12. Quelles devraient être les caractéristiques qualitatives de la communication des résultats d'une mission d'assurance ? Quelles mesures les auditeurs internes devraient-ils prendre pour s'assurer que la communication est de qualité ?

13. Une fois le rapport définitif diffusé, que doit faire l'audit interne concernant les observations de la mission d'assurance ?

Copyright © 2015 Eyrolles.

Questions à choix multiples

Sélectionnez la meilleure réponse pour chacune des questions suivantes.

1. Il convient d'inclure des recommandations dans les communications finales de l'audit afin de :
   a. Proposer au management diverses options pour remédier aux observations d'audit.
   b. S'assurer que les problèmes seront résolus de la manière indiquée par l'auditeur.
   c. Minimiser le temps requis pour corriger les observations d'audit.
   d. Garantir que les observations d'audit seront traitées, quel qu'en soit le coût.

2. Les observations d'audit interne dont il est fait état découlent d'un processus comparant « ce qui devrait être » à « ce qui est ». Lorsque, pour une mission d'audit interne, on définit « ce qui devrait être », quel serait, parmi les critères suivants, le moins approprié pour évaluer les systèmes de contrôle actuels ?
   a. Les meilleures pratiques du secteur.
   b. Les règles et procédures de contrôle prescrites par la direction générale.
   c. Une norme d'efficacité des contrôles déterminée par l'audit interne.
   d. Les systèmes de contrôle documentés comme étant en place lors du dernier audit.

3. Selon le Cadre de référence international des pratiques professionnelles de l'audit interne (CRIPP), quels sont les éléments qui devraient, *a minima*, être inclus dans les rapports définitifs ?
   I. Des informations de base.
   II. L'objectif de la mission.
   III. Le périmètre de la mission.
   IV. Les résultats de la mission.
   V. Des résumés.
   a. I, II et III.
   b. I, III et V.
   c. II, III et IV.
   d. II, IV et V.

4. Parmi les objectifs suivants, lequel ne doit pas être considéré comme un objectif principal d'une réunion de fin de clôture ?
   a. Résoudre des conflits.
   b. Identifier des points dont devront se préoccuper les futures missions d'audit.
   c. Discuter des observations et recommandations de la mission.
   d. Identifier les commentaires et plans d'action du management à la suite des observations et recommandations formulées dans le cadre de la mission.

Copyright © 2015 Eyrolles.

Questions à choix multiples

5. Au cours de l'examen de transactions d'achat, un auditeur interne constate que certaines procédures appliquées sont en contradiction avec les procédures énoncées par l'organisation. Cependant, les tests d'audit ont fait apparaître que les procédures employées permettent une efficience accrue et une réduction du temps de traitement, sans baisse visible du niveau de contrôle. L'auditeur interne doit :
   a. Mentionner le non-respect des procédures prescrites comme une déficience opérationnelle.
   b. Élaborer un diagramme de flux présentant les nouvelles procédures et l'inclure dans le rapport adressé au management.
   c. Faire état du changement de procédure et suggérer qu'il soit documenté.
   d. Suspendre la mission jusqu'à ce que le client ait documenté les nouvelles procédures.

6. Une communication formelle dans le cadre d'une mission doit :
   a. Donner à l'audité la possibilité de réagir.
   b. Documenter les actions correctives attendues de la direction générale.
   c. Offrir à un auditeur externe un moyen formel d'évaluer la fiabilité potentielle d'une fonction d'audit interne.
   d. Communiquer les observations significatives.

7. Parmi les éléments suivants, quels sont ceux que le responsable de l'audit interne doit prendre en compte lorsqu'il détermine l'étendue du suivi nécessaire ?
   I. Le caractère significatif de l'observation rapportée.
   II. Le comportement qu'il a pu observer par le passé de la part du manager chargé d'effectuer l'action corrective.
   III. Les efforts nécessaires pour mener l'action corrective ainsi que son coût.
   IV. L'expérience des auditeurs internes.
   a. I et III.
   b. I, II et III.
   c. II, III et IV.
   d. I, II, III et IV.

Copyright © 2015 Eyrolles.

8. L'extrait d'une observation d'audit interne indique que les avances de déplacement dépassent le montant maximal prévu. La politique de l'organisation accorde aux collaborateurs habilités des avances pour leurs déplacements. Ces avances ne peuvent excéder 45 jours de dépenses prévues. Les procédures de l'organisation n'exigent pas de justification pour les avances de gros montants. Les collaborateurs peuvent accumuler, et accumulent, d'importantes avances dont ils n'ont pas besoin. Dans cette observation, à quel élément d'un constat d'audit les « conséquences » renvoient-elles ?
   a. Les avances ne doivent pas dépasser 45 jours de dépenses prévues.
   b. Les avances de déplacement dépassent le montant maximal prévu.
   c. Les collaborateurs accumulent d'importantes avances dont ils n'ont pas besoin.
   d. Des collaborateurs non habilités reçoivent des avances de déplacement.

9. Les rapports d'audit interne peuvent être structurés de manière à inciter le management à corriger les déficiences. Parmi les techniques de rédaction de rapport suivantes, laquelle sera vraisemblablement la plus efficace ?
   a. Énoncer, dans des termes précis, les insuffisances au niveau des procédures et les pratiques répréhensibles qui en résultent.
   b. Recommander des changements et énoncer les sanctions qui s'ensuivront si les recommandations ne sont pas mises en œuvre.
   c. Dresser la liste des déficiences constatées, afin de constituer une checklist facile à suivre.
   d. Suggérer des améliorations pratiques pour remédier aux observations identifiées.

10. La publication d'un rapport intermédiaire pendant une mission d'audit interne a pour objectif principal :
   a. De donner au management de l'audité la possibilité d'agir immédiatement au vu de certaines observations.
   b. De préparer le terrain pour le rapport final.
   c. D'informer rapidement le management de l'audité et les superviseurs des procédures d'audit mises en œuvre à ce jour.
   d. De décrire le périmètre de l'audit.

Copyright © 2015 Eyrolles.

Thèmes de discussion

1. Le processus d'évaluation des observations et de remontée de l'information pendant une mission d'assurance peut être relativement complexe. Il nécessite plusieurs étapes et du jugement.
   a. Quels sont les jugements auxquels doit procéder une équipe d'audit interne pendant le processus d'évaluation des observations et de remontée de l'information ?
   b. Quels sont les trois degrés d'importance d'une observations, décrits dans ce chapitre ? Décrivez brièvement chacun.
   c. Pourquoi est-il important de documenter soigneusement les conclusions auxquelles on est parvenu, à la suite d'un processus d'évaluation des observations et de remontée de l'information ?

2. Toutes les observations identifiées par une équipe d'audit interne pendant une mission d'assurance appellent-elles une action de la part du management ? Expliquez votre réponse. Quelles sont les conséquences pour l'audit interne si le management ne répond pas de façon adéquate à une observation nécessitant une action corrective ?

3. La situation

   L'organisation ABC est un important grossiste en luminaires et ventilateurs de plafond. L'organisation a ouvert un grand magasin dans une zone métropolitaine en pleine expansion vers le début de l'exercice budgétaire de l'organisation.

   Les faits suivants ont été relevés par l'auditeur externe des états financiers de l'organisation durant les contrôles postérieurs à la clôture.

   - Le manager du nouveau magasin avait comptabilisé une importante régularisation de clôture (un débit dans les ventes et un crédit dans les comptes clients). L'explication de l'écriture au journal indiquait que cette dernière a été effectuée afin d'ajuster les créances clients du grand livre général par rapport au grand livre auxiliaire des comptes clients.
   - Le ratio de marge brute de clôture du nouveau magasin est ressorti nettement en dessous de celui des autres magasins.
   - Le manager du magasin volait les acomptes des clients. C'est pourquoi le grand livre général ne correspondait pas au grand livre auxiliaire. Le manager a effectué cette importante régularisation de clôture afin de couvrir le vol, ce qui explique que le ratio de marge brute du magasin soit inférieur à la moyenne des autres magasins.
   - La régularisation de clôture était importante pour le magasin, mais pas pour l'organisation dans sa globalité.

Copyright © 2015 Eyrolles.

Travail à effectuer au moyen du processus d'évaluation des observations et de remontée de l'information (encadré 14-4). Évaluez les faits présentés et déterminez les éléments suivants :

a. Quelle(s) observation(s) est (sont) requis(es) ?
b. Quelles catégories d'objectifs définis par le COSO sont affectées ?
c. Indiquez si l'observation ou les observations découlent d'une conception inadéquate, d'un fonctionnement non effectif ou des deux.
d. Déterminez l'impact et la probabilité d'occurrence de la ou des observations.
e. Précisez si la ou les observations sont non significatives, significatives ou critiques.
f. D'après vos réponses, comment et à qui devez-vous communiquer cette ou ces observations ?

4. Certains auditeurs internes pensent que leur profession devrait exiger des fonctions d'audit interne qu'elles adoptent un système de cotation simple mais cohérent pour leurs rapports de mission, ceci dans l'objectif de mieux communiquer les conclusions générales exprimées dans ces rapports. Ils proposent qu'une note globale soit incluse dans le rapport d'audit pour chaque unité opérationnelle (*business unit*) ou fonction auditée. L'objectif de cette notation est d'indiquer l'adéquation de la conception et le fonctionnement effectif du contrôle interne. Exemple de système de notation proposé :

A	Les contrôles sont conçus de manière adéquate et fonctionnent de manière effective afin de donner l'assurance raisonnable que les risques sont maintenus à un niveau acceptable.
B	Certaines possibilités d'amélioration ont été identifiées ; mais dans l'ensemble, les contrôles sont conçus de manière adéquate et fonctionnent de manière effective afin de donner l'assurance raisonnable que les risques sont maintenus à un niveau acceptable.
C	D'importantes possibilités d'amélioration ont été identifiées. De nombreuses faiblesses de contrôle ont été observées et, dans certains domaines, les contrôles ne peuvent pas donner l'assurance raisonnable que les risques sont maintenus à un niveau acceptable.
F	Insatisfaisant. Les contrôles sont conçus de manière inadéquate et/ou ne fonctionnent pas de manière effective. Par conséquent, ils ne donnent pas l'assurance raisonnable que les risques sont maintenus à un niveau acceptable.

Présentez des arguments pour et contre l'utilisation d'un système de notation. Pensez-vous que l'utilisation d'un tel système soit appropriée ? Argumentez votre réponse.

Copyright © 2015 Eyrolles.

Thèmes de discussion

5. Le président du comité d'audit a demandé au responsable de l'audit interne de réfléchir à la possibilité de présenter une opinion globale annuelle sur l'état du système de contrôle interne de l'organisation. Le responsable de l'audit interne a effectué quelques recherches préliminaires et proposé le modèle d'opinion suivant :

À l'attention de : Président du comité d'audit
De la part de : Directeur de l'audit interne
Sujet : Opinion de l'audit interne sur le système de contrôle interne pour la période se terminant le 31 décembre 20XX.

Nous avons achevé le plan d'audit interne annuel de la société. Ce plan était conçu de manière à nous permettre d'évaluer l'adéquation du système de contrôle interne de l'organisation en ce qui concerne les risques opérationnels, les risques liés au reporting financier et les risques de non-conformité.

Le plan a été élaboré en tenant compte des résultats de l'évaluation des risques effectuée dans le cadre du processus de gestion des risques de l'organisation et des évaluations des risques effectuées par l'audit interne et par les auditeurs externes de l'organisation. Notre travail a été réalisé conformément aux *Normes internationales pour la pratique professionnelle de l'audit interne*.

Les critères utilisés pour évaluer le système de contrôle interne de l'organisation sont repris dans le référentiel de contrôle interne de l'organisation, qui s'appuie sur le référentiel COSO. Les critères ont fait l'objet de discussions et d'un accord avec le management de chaque domaine avant que les différentes missions prévues dans le plan d'audit interne annuel ne soient menées.

Notre opinion globale est la suivante : au 31 décembre 20XX, les contrôles internes relatifs aux opérations, au reporting financier et à la conformité sont conçus de manière adéquate et fonctionnent de manière effective. Nous avons mené suffisamment de procédures d'audit appropriées et collecté des preuves suffisantes pour étayer cette conclusion. Les preuves collectées satisfont aux normes professionnelles de l'audit interne et suffisent à donner une assurance raisonnable.

Le responsable de l'audit interne vous a demandé d'effectuer des recherches supplémentaires sur le caractère approprié du fait que l'audit interne donne une telle opinion et de dresser une liste préliminaire des questions que le service doit prendre en compte s'il veut formuler une telle opinion. Il vous propose de commencer par examiner le guide pratique de l'IIA intitulé « Formuler et exprimer une opinion d'audit interne » (*Practice Guide : Formulating and Expressing Internal Audit Opinions*).

a. L'opinion envisagée par le responsable de l'audit interne à l'attention du comité d'audit relève-t-elle de l'assurance positive ou négative ? Expliquez votre réponse.
b. Qu'implique cette opinion à propos du périmètre du travail d'audit interne effectué ?
c. Dans le rapport que vous adressez au responsable de l'audit interne, quels sont les facteurs que vous recommanderiez à l'audit interne de prendre en compte avant de formuler une opinion globale sur le système de contrôle interne de l'organisation ?

Copyright © 2015 Eyrolles.

ÉTUDES DE CAS

CAS N° 1

Examinez les observations suivantes, qui sont extraites d'une mission d'assurance, et notez les informations spécifiques qui représentent les recommandations et chacun des attributs d'observation suivants : référentiel, faits, causes et conséquences.

Observation d'audit et recommandation

Les associés de l'organisation X doivent respecter le Code de conduite et de déontologie formel de l'organisation (le Code). Pour s'assurer que tous les collaborateurs sont sensibilisés à ce Code et aux obligations qui en découlent, l'organisation X demande à tous les associés d'accuser réception du Code. Le 1er juillet, un courriel général a été envoyé à tous les associés, les informant de leur obligation de lire le Code et d'en accuser réception. Les associés ont reçu pour instruction de compléter et renvoyer les accusés de réception avant le 1er décembre. Notre test d'audit indique les éléments suivants concernant le processus d'accusé de réception :

- au 1er mars, moins de 50 % des associés avaient complété et retourné l'accusé de réception ;
- à ce jour, ni les ressources humaines (RH) ni la direction générale n'ont effectué de procédure de suivi ;
- il n'existe aucune politique formelle quant aux mesures à prendre lorsque des associés ne renvoient pas l'accusé de réception ;
- aucune mesure n'a été prise à l'encontre des associés qui, à ce jour, n'ont pas rempli l'accusé de réception du Code.

Améliorer le processus d'accusé de réception aidera l'organisation X à faire la preuve de sa conformité avec la réglementation externe requérant un Code de déontologie. Cela permettra également de s'assurer que tous les associés sont conscients de leurs responsabilités et obligations vis-à-vis de l'organisation, aux termes du Code.

Nous recommandons au management de renforcer le processus de suivi des accusés de réception afin de s'assurer que tous les associés confirment qu'ils ont reçu le Code, le comprennent et s'y conforment. Des règles et des procédures doivent être établies et appliquées pour que des mesures appropriées puissent être prises lorsque des associés ne réagissent pas. Il convient de prendre des mesures disciplinaires si les associés refusent de compléter et de renvoyer l'accusé de réception, comme le requiert le règlement.

Réponse du management

Les associés qui n'auront pas accusé réception du Code le 24 mars recevront un rappel la semaine du 3 avril soulignant le caractère impératif de l'accusé de réception du Code. Une liste de tous les associés qui continuent de ne pas se conformer à cette exigence sera fournie à l'agent de liaison des RH compétent, pour examen et suivi la semaine du 17 avril. Le service des RH se rapprochera des

Copyright © 2015 Eyrolles.

responsables des services dans lesquels se trouvent les associés retardataires afin d'obtenir les accusés de réception manquants. Un rapport final sera produit dans la semaine du 24 avril afin de déterminer quels associés n'ont toujours pas accusé réception du Code. Ceux qui n'auront alors pas accusé réception recevront un avertissement oral et un avertissement écrit si la situation perdure jusqu'au 30 avril.

Devoir de rendre compte : Jane Doe

Responsabilité : John Smith

Date de mise en œuvre : 24 mars

Est-ce que cette observation, telle que présentée, répond correctement à tous les attributs d'observation suggérés ? Dans la négative, veuillez expliquer pourquoi.

CAS N° 2

Considérez les faits suivants.

Au cours de son évaluation du service fournisseur, l'audit interne fait les observations suivantes :

- séparation inadéquate des tâches concernant certains contrôles d'accès au système d'information. Exposition à des pertes potentielles de 45 millions ;
- plusieurs transactions n'ont pas été correctement comptabilisées dans les grands livres auxiliaires. Ces transactions n'étaient pas importantes, ni individuellement ni globalement. Exposition à des pertes potentielles de 60 millions ;
- absence de rapprochement, en temps opportun, des comptes concernés par les transactions mal comptabilisées. Exposition à des pertes potentielles de 25 millions.

Compte tenu du contexte dans lequel ces observations interviennent, le management et l'audit interne sont d'accord sur les pertes potentielles que représentent individuellement ces transactions.

L'organisation dispose d'un service de gestion des risques qui détermine, en accord avec l'auditeur externe, qu'une perte inférieure à 20 millions représente un impact négligeable, et un montant supérieur à 80 millions un impact significatif.

À partir de ces faits :

- déterminez à quelle catégorie d'objectifs définis par le COSO se rapporte chacune de ces observations ;
- indiquez si la déficience relève de l'adéquation de la conception ou du fonctionnement effectif ;
- déterminez l'impact et la probabilité d'occurrence de chaque observation ;
- évaluez si chaque observation est non significative, significative ou critique.

Après quoi, présentez les grandes lignes des mesures que l'audit interne doit prendre ensuite et les suites à donner à la conclusion générale, notamment en termes de communication (modalités, destinataires).

Copyright © 2015 Eyrolles.



Copyright © 2015 Eyrolles.



CHAPITRE 15
LA MISSION DE CONSEIL

Objectifs pédagogiques

- Différencier clairement les missions d'assurance et de conseil.
- Comprendre que les missions peuvent être des missions mixtes qui comportent à la fois des éléments d'assurance et de conseil.
- Analyser les différents types d'activités de conseil réalisées par les auditeurs internes.
- Comprendre comment les fonctions d'audit interne sélectionnent les missions de conseil à réaliser.
- Comprendre le processus de réalisation d'une mission de conseil destinée à formuler un avis.
- Décrire les avantages qu'une organisation peut retirer des activités de conseil réalisées par l'audit interne.
- Montrer en quoi l'audit interne peut apporter son point de vue aux parties prenantes en réalisant des missions de conseil.
- Souligner l'importance de la formulation des attentes du client à l'égard des activités de conseil.
- Examiner quelles *Normes* se rapportent aux missions de conseil.
- Comprendre la nécessité, pour l'audit interne, de délimiter les activités de conseil.

Comme indiqué précédemment dans ce manuel, la profession d'audit interne connaît une transformation : en raison de sa connotation, le terme « consulting » est de moins en moins utilisé pour qualifier la profession, dans la mesure où il désigne des prestations exécutées par des sources extérieures à l'organisation. Le terme « advisory », qui désigne des prestations exécutées par des professionnels au sein de l'organisation, est désormais privilégié. Du fait du contexte dans lequel s'inscrit cette transformation, les auteurs de ce manuel ont choisi de conserver la terminologie actuelle dans ce chapitre, afin de garantir une cohérence avec la définition de l'audit interne et les Normes internationales pour la pratique professionnelle de l'audit interne *(les* Normes*)*.

Depuis quelques années, l'accent est mis sur les tests des contrôles, qui permettent de veiller à ce que les contrôles fonctionnent de manière efficace et efficiente. Néanmoins, de récentes réflexions ont mis en évidence que le meilleur

Copyright © 2015 Eyrolles.

ENCADRÉ 15-1

DISPOSITIONS DU CRIPP PERTINENTES RELATIVES AU CHAPITRE 15

Norme 1000.C1 – Mission, pouvoirs et responsabilités
Norme 1130.C1 – Atteinte à l'indépendance ou à l'objectivité
Norme 1130.C2 – Atteinte à l'indépendance ou à l'objectivité
Norme 1210.C1 – Compétence
Norme 1220.C1 – Conscience professionnelle
Norme 2010.C1 – Planification
Norme 2120.C1 – Management des risques
Norme 2120.C2 – Management des risques
Norme 2120.C3 – Management des risques
Norme 2130.C1 – Contrôle
Norme 2201.C1 – Considérations relatives à la planification
Norme 2210.C1 – Objectifs de la mission
Norme 2220.C1 – Champ de la mission
Norme 2240.C1 – Programme de travail de la mission
Norme 2330.C1 – Documentation des informations
Norme 2410.C1 – Contenu de la communication
Norme 2440.C1 – Diffusion des résultats
Norme 2440.C2 – Diffusion des résultats
Norme 2500.C1 – Surveillance des actions de progrès

Modalité Pratique d'Application 1000-1 : Charte d'audit interne
Modalité Pratique d'Application 1110-1 : Indépendance dans l'organisation
Modalité Pratique d'Application 1120-1 : Objectivité individuelle
Modalité Pratique d'Application 1130-1 : Atteintes à l'indépendance ou à l'objectivité
Modalité Pratique d'Application 1200-1 : Compétence et conscience professionnelle
Modalité Pratique d'Application 1210-1 : Compétence
Modalité Pratique d'Application 1220-1 : Conscience professionnelle
Modalité Pratique d'Application 2020-1 : Communication et approbation
Modalité Pratique d'Application 2030-1 : Gestion des ressources
Modalité Pratique d'Application 2040-1 : Règles et procédures
Modalité Pratique d'Application 2060-1 : Rapports à la direction générale et au Conseil
Modalité Pratique d'Application 2120-1 : Évaluer la pertinence des processus de management des risques
Modalité Pratique d'Application 2130-1 : Évaluer la pertinence des processus de contrôle
Modalité Pratique d'Application 2200-1 : Planification de la mission
Modalité Pratique d'Application 2210-1 : Objectifs de la mission
Modalité Pratique d'Application 2230-1 : Ressources affectées à la mission
Modalité Pratique d'Application 2240-1 : Programme de travail de la mission
Modalité Pratique d'Application 2330-1 : Documentation des informations
Modalité Pratique d'Application 2340-1 : Supervision de la mission
Modalité Pratique d'Application 2410-1 : Contenu de la communication
Modalité Pratique d'Application 2440-1 : Diffusion des résultats de la mission
Modalité Pratique d'Application 2500-1 : Surveillance des actions de progrès

moyen pour l'audit interne d'apporter de la valeur ajoutée réside dans les activités de conseil. Si la plupart des fonctions d'audit interne souhaitent consacrer une part importante de leur budget

Copyright © 2015 Eyrolles.

annuel à des missions de conseil, la majorité des organisations requièrent un minimum de missions d'assurance. Pour s'adapter à un environnement dynamique en mutation, les fonctions d'audit interne doivent réaliser des activités de conseil prospectives, dans le but d'apporter des enseignements et de faciliter des processus solides de gouvernance, de gestion des risques et de contrôle, plutôt que d'auditer des contrôles qui évolueront avec les nouveaux systèmes et processus ou lors de la restructuration de l'organisation.

Les missions de conseil sont les plus susceptibles d'apporter une valeur ajoutée à long terme au système de contrôle interne de l'organisation. Elles n'ont pas pour finalité d'évaluer les événements passés mais tendent plutôt à être prospectives. À l'heure où de nouveaux processus, règles et procédures sont élaborés, il est préférable d'y intégrer des contrôles dès le départ et de veiller à ce que des pistes d'amélioration soient prises en compte de manière proactive. Par son implication dans les grandes initiatives de changement de l'organisation, la fonction d'audit interne peut donner un éclairage prospectif sur la manière dont les choses devraient fonctionner avec des contrôles optimisés, plutôt que de réaliser uniquement des activités d'assurance liées à des contrôles qui évolueront au fil du temps.

De nombreux auditeurs internes qui réalisent des missions de conseil savent combien il est important pour l'organisation d'obtenir un point de vue dès le début d'un projet. Par exemple, en réalisant des travaux de *due diligence* au cours de l'acquisition d'une société, la fonction d'audit interne apporte un point de vue précieux. Grâce à cette méthode, les insuffisances des contrôles de l'organisation cible peuvent être prises en compte dès le début du processus de négociation. La fonction d'audit interne occupe une position unique, qui lui permet d'examiner l'organisation en profondeur et d'apporter un point de vue sur l'ensemble du système de contrôle interne, ainsi que d'autres éléments, comme le référentiel sur lequel s'appuie l'organisation pour évaluer le système. Par exemple, une équipe d'auditeurs internes peut être constituée pour examiner le contrôle interne et les contrôles d'une organisation susceptible d'être rachetée en Chine. Cet audit de *due diligence* (ou « contrôle diligent ») vise à déterminer ce qu'il sera nécessaire de faire pour appliquer à la nouvelle entité le même niveau de maîtrise que celui en place dans l'organisation actuelle.

Dans de nombreuses organisations, la fonction d'audit interne participe au dispositif d'alerte interne. Il s'agit pour celle-ci d'une autre opportunité de réaliser des activités de conseil. Dans le cadre de ce dispositif, un cas de fraude potentiel au sein du service de la comptabilité fournisseurs peut par exemple être signalé. La fonction d'audit interne peut alors déployer des ressources pour enquêter. Dans cet exemple, la fonction d'audit interne a découvert que des factures avaient été réglées auprès de fournisseurs fictifs pendant

Copyright © 2015 Eyrolles.

plusieurs mois. Le fraudeur était le manager du service de la comptabilité fournisseurs, qui contrôlait l'enregistrement des fournisseurs ainsi qu'un certain nombre de centres de coûts qu'il pouvait facturer. À l'issue de son enquête, la fonction d'audit interne a formulé des recommandations qui ont conduit à une modification des procédures relatives à l'enregistrement et à la validation des fournisseurs, ainsi qu'à la mise en place d'une surveillance du processus d'enregistrement de nouveaux comptes. Le service de la comptabilité fournisseurs de cette organisation affichait un taux de risque faible, si bien que la fonction d'audit interne ne l'avait pas audité depuis plusieurs années. Une fois son enquête terminée, l'audit interne a modifié cette évaluation. Il réalise désormais des missions d'assurance plus régulières pour les processus liés à la comptabilité fournisseurs.

Du fait de leur caractère imprévisible, les missions de conseil comportent une dimension particulièrement stimulante pour les auditeurs internes qui en effectuent régulièrement. Un auditeur interne peut être à n'importe quel moment amené à réaliser des activités de conseil, telles que des enquêtes sur une fraude, des missions faisant intervenir un groupe de travail spécial, des études sur des fusions et acquisitions, des *due diligence*, des examens portant sur des tiers fournisseurs ou prestataires de services, des demandes spéciales de la direction générale ou des demandes visant à définir les causes de problèmes de performance opérationnelle. Ces missions peuvent amener à suspendre les activités d'assurance quotidiennes, et les ressources disponibles affectées sur les missions de conseil. Nombre de ces missions imposent d'apporter une réponse très rapide au management et peuvent être assorties de délais plus tendus que les missions d'assurance déjà programmées.

Norme 2010.C1

Lorsqu'on lui propose une mission de conseil, le responsable de l'audit interne, avant de l'accepter, devrait considérer dans quelle mesure elle est susceptible de créer de la valeur ajoutée, d'améliorer le management des risques et le fonctionnement de l'organisation. Les missions de conseil qui ont été acceptées doivent être intégrées dans le plan d'audit.

L'ensemble des projets examinés apporte un éclairage significatif à l'organisation. Des ressources sont nécessaires pour les mettre en œuvre. Comme le précise la Norme 2010.C1, ces projets créent de la valeur ajoutée en améliorant le management des risques et le fonctionnement de l'organisation. Pour que la fonction d'audit interne soit en mesure de réaliser ces missions de conseil, le plan annuel devrait prévoir le calendrier et les ressources nécessaires. À cet égard, plusieurs facteurs devraient être pris en compte, comme le degré d'évolution de l'organisation, la mise en œuvre de systèmes majeurs ou encore les problématiques significatives liées aux contrôles.

David Richards, qui vient de quitter ses fonctions de président de l'IIA, plaide depuis longtemps en faveur des activités de conseil réalisées par l'audit interne. Lorsqu'il était responsable de l'audit interne chez First Energy, il a d'ailleurs noté ceci :

> *« Pour certains auditeurs internes, les concepts de conseil et d'audit s'opposent parce qu'ils considèrent que les activités de conseil placent l'auditeur dans une position trop proche des clients, ce*

Copyright © 2015 Eyrolles.

qui risque de compromettre son indépendance. En fait, le conseil fait partie de l'audit interne depuis des années […]. D'après la définition actuelle de l'audit interne, celui-ci doit englober à la fois des activités d'assurance et de conseil. À l'évidence, les auditeurs internes peuvent ajouter de la valeur aux missions de conseil en déployant les méthodes, les mécanismes de facilitation, l'attention, le savoir, la technologie, les meilleures pratiques et l'indépendance nécessaires pour aider à résoudre les problèmes des clients[1]. »

APPORTER UN POINT DE VUE DANS LE CADRE DE MISSIONS DE CONSEIL

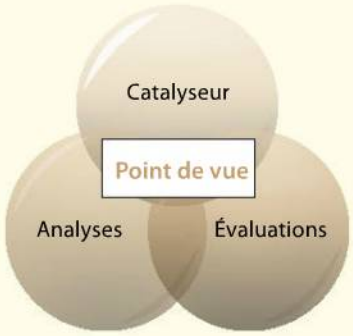
Point de vue

Le produit final (ou résultat) des missions d'assurance et de conseil réalisées par la fonction d'audit interne est destiné à apporter des informations et des éclairages précieux à l'audité ou au client.

Les activités de conseil réalisées par la fonction d'audit interne peuvent être considérées comme des catalyseurs potentiels d'amélioration pour la gestion des risques de l'organisation, *via* l'utilisation d'analyses et d'évaluations. Comme illustré dans l'encadré 15-2, le point de vue est l'une des principales composantes de la proposition de valeur de l'audit interne. Les auditeurs internes sont les mieux placés pour apporter à l'organisation des éclairages sur les techniques de gestion des risques et pour l'aider à améliorer ses contrôles et ses processus.

ENCADRÉ 15-2

PROPOSITION DE VALEUR DE L'AUDIT INTERNE POUR LES PARTIES PRENANTES



L'audit interne agit comme un catalyseur permettant d'améliorer l'efficacité et l'efficience d'une organisation, grâce à un point de vue et des recommandations fondés sur des analyses et des évaluations des informations et des processus opérationnels.

Comme nous l'avons vu au chapitre 1, *Introduction à l'audit interne*, le point de vue, intégré dans la proposition de valeur de l'audit interne, constitue l'une des caractéristiques majeures de la fonction. S'il est possible de donner un point de vue dans le cadre de missions d'assurance, ce sont principalement les missions de conseil qui permettent d'apporter un éclairage significatif à l'organisation. Les missions mixtes (qui comportent à la fois des éléments d'assurance et de conseil) offrent également cette possibilité, comme nous le verrons plus loin.

Copyright © 2015 Eyrolles.

La fonction d'audit interne occupe une position unique, qui lui permet de créer de la valeur ajoutée et d'influer sur l'organisation lors de ses missions de conseil. Les auditeurs internes étant souvent considérés comme les spécialistes des risques et du contrôle interne au sein d'une organisation, il est possible de mettre à profit leurs compétences pour aider l'organisation à surveiller les risques émergents. Ainsi, l'audit interne peut jouer un rôle de conseil en engageant des discussions visant à identifier l'impact éventuel de la crise économique sur la cartographie des risques. De plus, dans la mesure où les auditeurs internes connaissent très bien la plupart des domaines de l'organisation, voire tous, en raison des activités d'assurance qu'ils mènent à bien, ils sont parfaitement au courant des changements qui s'y produisent. Ils sont donc les mieux placés pour conseiller le management sur une gestion efficace de ces changements. L'environnement actuel des organisations offre, plus que jamais, de nombreuses opportunités aux auditeurs internes de proposer des activités de conseil qui sont source de valeur ajoutée à un moment crucial de l'évolution de l'organisation.

Pour ces raisons et pour d'autres (analysées de manière plus approfondie tout au long de ce chapitre), l'ajout d'activités de conseil aux prestations fournies par l'audit interne, ou la multiplication de ces activités, peut être très bénéfique pour l'organisation. De surcroît, les activités de conseil donnent aux auditeurs internes des opportunités de diversifier leurs compétences et de travailler dans un environnement dynamique et intéressant. Chacun trouve son intérêt à mettre davantage l'accent sur les activités de conseil, en particulier dans un environnement incertain.

Client

Filiale, unité opérationnelle, service, groupe, personne ou autre subdivision en place dans une organisation qui fait l'objet d'une mission de conseil.

DIFFÉRENCIATION ENTRE LES ACTIVITÉS D'ASSURANCE ET DE CONSEIL

Il existe plusieurs différences fondamentales entre les activités d'assurance et de conseil, définies à l'encadré 15-3 : le nombre de participants à la mission, les *Normes* applicables, la finalité de la mission et la communication des résultats. En outre, dans la mesure où les activités de conseil sont couramment réalisées sur demande, leur nature et leur périmètre font l'objet d'un accord avec les clients des missions.

Participants à la mission

Les activités de conseil font généralement intervenir deux parties :

- la personne ou l'entité qui demande et reçoit ces prestations, c'est-à-dire le client de la mission ;
- la personne ou l'entité qui propose les prestations de conseil, c'est-à-dire l'audit interne.

Copyright © 2015 Eyrolles.

Les activités d'assurance font, elles, généralement intervenir trois parties :

- la personne ou l'entité qui participe directement au processus, au système ou à un autre aspect, c'est-à-dire l'audité ;
- la personne ou l'entité qui effectue cette évaluation indépendante, c'est-à-dire l'audit interne ;
- la personne ou l'entité qui se fonde sur cette évaluation indépendante, c'est-à-dire l'utilisateur.

ENCADRÉ 15-3

DÉFINITIONS DES ACTIVITÉS DE CONSEIL ET D'ASSURANCE

Activités de conseil – Conseils et services y afférents rendus au client donneur d'ordre, dont la nature et le champ sont convenus au préalable avec lui. Ces activités ont pour objectifs de créer de la valeur ajoutée et d'améliorer les processus de gouvernement d'entreprise, de management des risques et de contrôle d'une organisation sans que l'auditeur interne n'assume aucune responsabilité de management. Quelques exemples : avis, conseil, assistance et formation.

Activités d'assurance – Il s'agit d'un examen objectif d'éléments probants, effectué en vue de fournir à l'organisation une évaluation indépendante des processus de gouvernement d'entreprise, de management des risques et de contrôle. Par exemple, des audits financiers, opérationnels, de conformité, de sécurité des systèmes et de *due diligence*.

The Institute of Internal Auditors, Cadre de référence international des pratiques professionnelles de l'audit interne (Paris, IIA/IFACI, 2014), p. 65.

Application des *Normes*

Même si les Normes de qualification et de fonctionnement s'appliquent à la fois aux activités d'assurance et aux activités de conseil, il existe un ensemble de Normes de mise en œuvre pour chaque type d'activité. Les différences entre ces deux ensembles reflètent celles entre les activités d'assurance et de conseil, et mettent notamment en avant les différences dans les attentes des parties prenantes. Étant donné que les activités de conseil ne font intervenir que les deux parties mentionnées ci-dessus (à savoir le client de la mission et l'audit interne), leur structure est moins complexe que celle des activités d'assurance, qui impliquent trois parties (l'audité, l'audit interne et le tiers utilisateur). Compte tenu de cette différence de structure, les Normes de mise en œuvre relatives à l'assurance sont plus strictes et plus nombreuses que les Normes de mise en œuvre relatives au conseil. Comme indiqué au chapitre 2, *Le Cadre de référence international des pratiques professionnelles : des lignes directrices incontournables pour l'audit interne*, les Normes de mise en œuvre spécifiques aux missions d'assurance sont identifiées par la lettre « A » après leur numéro (par exemple : Norme 1130.A1), celles concernant les missions de conseil par la lettre « C » (exemple : Norme 1130.C1).

Copyright © 2015 Eyrolles.

Finalité de la mission

Alors que les missions d'assurance ont pour objectif de procéder à des évaluations indépendantes, les missions de conseil sont menées dans le but d'émettre un avis, de réaliser une formation ou de faciliter un processus, et d'offrir le plus d'opportunités d'apporter un point de vue. Comme pour le périmètre d'une mission de conseil, ce sont l'audit interne et le client qui définissent, d'un commun accord, en fonction des besoins du client, quel type de mission sera le plus approprié pour satisfaire le service demandé. Comme le précise la Norme 2010.C1, lorsqu'on lui propose une mission de conseil, le responsable de l'audit interne, avant de l'accepter, devrait considérer dans quelle mesure elle est susceptible de créer de la valeur ajoutée en améliorant le management des risques et le fonctionnement de l'organisation. Dans la mesure où les missions de conseil spécifiques ne sont pas toujours connues lorsque le plan d'audit interne est élaboré, il est important que la fonction d'audit interne réserve du temps aux missions de conseil qu'il peut être nécessaire d'accomplir au cours de l'année. Le chapitre 9, *La gestion de l'audit interne*, examine plus en détail l'intégration des missions de conseil planifiées et ponctuelles dans le plan d'audit.

Communication des résultats de la mission

Les résultats des missions d'assurance sont toujours communiqués à des destinataires bien définis. Étant donné que les missions d'assurance ont pour finalité de produire une évaluation indépendante et qu'un tiers utilisera ces informations, les communications doivent être adressées à la fois à l'audité, à sa hiérarchie et aux utilisateurs tiers. De plus, comme le type d'informations communiquées est analogue pour toutes les missions d'assurance, le format des communications est relativement homogène. Les destinataires peuvent ainsi trouver plus facilement les informations qu'ils recherchent. En revanche, la communication des résultats des activités de conseil diffère selon le périmètre et la finalité de la mission. Elle peut être formelle ou informelle et diffusée sous de nombreux formats. On peut donc sélectionner le mode de diffusion en fonction de ce qui est le plus efficace et le plus efficient selon le contenu spécifique de la communication et le profil des destinataires. Certaines recommandations formulées à l'issue d'une mission de conseil peuvent être intégrées dans l'analyse *a posteriori* du management, qui comprend une liste exhaustive de problèmes spécifiques, plutôt que faire l'objet d'une communication de l'audit interne. Dans cette hypothèse, l'audit interne peut ne pas être expressément désigné comme la source du point de vue émis. En tant que membre à part entière de l'équipe, il peut néanmoins être fier de sa contribution à l'amélioration des processus qui en découle.

Copyright © 2015 Eyrolles.

TYPES D'ACTIVITÉS DE CONSEIL

Les activités de conseil englobent un large éventail de prestations, en fonction des besoins du management. On peut les adapter pour résoudre des problèmes spécifiques qui, d'après la direction générale, nécessitent une attention particulière, et ces activités peuvent viser, par nature, à formuler un avis, assurer une formation ou une assistance. Les missions de conseil qu'une fonction d'audit interne peut réaliser ne sont limitées que par les besoins de l'organisation et les ressources de l'audit interne, tant qu'elles ne portent pas atteinte à l'indépendance de ce dernier ou à l'objectivité des auditeurs internes.

Types de missions de conseil

– Missions destinées à formuler un avis.
– Missions axées sur la formation.
– Missions d'assistance.

Missions de conseil destinées à formuler un avis

Nombre de missions de conseil sont destinées à formuler un avis. Lorsqu'une organisation connaît des changements, tels que des compressions d'effectifs ou la refonte de processus opérationnels, l'audit interne peut être amené à donner son point de vue. Ainsi, le management peut lui demander d'aider à examiner l'efficacité et l'efficience de tel ou tel processus opérationnel, de recommander des améliorations, ou de participer à des projets d'assurance qualité précis.

Voici des exemples de missions de conseil, par nature destinées à émettre une opinion :

- formuler un avis sur la conception des contrôles ;
- conseiller lors de l'élaboration de règles et de procédures ;
- participer, à titre de consultant, à des projets sensibles, tels que le développement de systèmes d'information ;
- conseiller sur les violations de la sécurité ou l'interruption de l'activité ;
- conseiller sur certaines activités de gestion des risques de l'organisation.

Missions de conseil axées sur la formation

Comme mentionné précédemment, l'audit interne possède un savoir spécialisé dans de nombreux domaines différents qui sont importants pour l'organisation. Parce qu'ils proposent des activités d'assurance, les auditeurs internes connaissent la réglementation sectorielle spécifique, l'évaluation et la maîtrise des risques, la conception des contrôles, les bonnes pratiques, etc. Souvent, le management demande à l'audit interne de former les collaborateurs concernés à ces aspects et à d'autres. Pour ce faire, l'audit

Copyright © 2015 Eyrolles.

interne organise des sessions de formation spécifiques, fait des présentations thématiques à certains groupes ou personnes, ou travaille avec des membres de la direction générale.

Voici des exemples de missions de conseil axées sur la formation :

- former à la gestion des risques et au contrôle interne ;
- comparer des services internes à des services d'autres organisations similaires, afin de repérer les bonnes pratiques ;
- procéder à une analyse *a posteriori*, c'est-à-dire tirer les enseignements d'un projet une fois celui-ci achevé.

Auto-évaluation des contrôles

Méthode fondée notamment sur l'animation de réunions et sur des enquêtes, qui constitue pour les managers et les auditeurs internes un moyen utile de collaborer à l'évaluation des risques opérationnels et des dispositifs de contrôle interne.

Missions de conseil visant à apporter une assistance

Le management demande parfois à l'audit interne d'aller au-delà de la formation sur un sujet donné. Dans ce cas, l'audit interne remplit une fonction d'assistance. À cette fin, il doit participer davantage à l'activité concernée, et ne pas uniquement mettre à disposition le savoir dont un tiers a besoin pour cette activité. Ainsi, l'auto-évaluation des contrôles, analysée plus en détail au chapitre 9, *La gestion de l'audit interne*, est une activité dans laquelle l'audit interne peut apporter une assistance. Le savoir que les auditeurs internes possèdent dans ce domaine peut servir à faciliter des débats sur les processus opérationnels et les contrôles. Les auditeurs internes qui facilitent une discussion sur l'auto-évaluation des contrôles ne se limitent pas à informer le management sur ce processus, mais attirent son attention sur les objectifs de l'organisation et sur les processus opérationnels nécessaires pour soutenir leur réalisation. Les auditeurs internes guident ensuite le management non seulement à travers une analyse des écarts entre l'état existant et l'état attendu d'un processus, mais aussi à travers les étapes à mettre en œuvre pour réduire ces écarts. Comme le souligne l'ensemble de ce chapitre, les auditeurs internes doivent veiller à ne pas aller trop loin et à ne pas exercer de responsabilités managériales, ce qui enfreindrait les dispositions de la Norme 2120.C3 : « lorsque les auditeurs internes aident le management dans la conception et l'amélioration des processus de management des risques, ils doivent s'abstenir d'assumer une responsabilité opérationnelle en la matière. »

Voici des exemples de missions de conseil qui visent, de par leur nature, à apporter une assistance :

- faciliter le processus d'évaluation des risques de l'organisation ;
- faciliter l'auto-évaluation du contrôle interne par le management ;
- faciliter les activités d'un groupe de travail chargé de repenser les contrôles et procédures pour un domaine nouveau ou qui a évolué de manière significative ;

Copyright © 2015 Eyrolles.

- agir comme intermédiaire entre le management et les auditeurs externes, les organismes publics, les fournisseurs et les sous-traitants, en ce qui concerne les contrôles ;
- faciliter les discussions *a posteriori* concernant l'interruption de systèmes ou processus majeurs ;
- aider à la mise en place d'un dispositif de contrôle interne ou de gestion des risques.

Même si les différents types de missions de conseil décrits plus haut sont souvent bien délimités, ils ne s'excluent pas mutuellement. Ainsi, lors d'une mission de conseil visant à apporter une assistance, les auditeurs internes assurent, dans une certaine mesure, une formation, y compris s'ils facilitent le processus ou l'activité en question. De même, il y aura des chevauchements entre les missions de conseil destinées à formuler un avis et celles axées sur la formation, et ainsi de suite avec toute combinaison de différents types de missions. Le plus souvent, toutefois, l'objectif global de la mission relèvera de l'une des trois catégories mentionnées.

Dans l'ensemble, le processus de réalisation d'une mission de conseil est le même que pour une mission d'assurance : il comporte une phase de planification, une phase d'exécution et une phase de communication. Cependant, en fonction de la nature de la mission de conseil, les différentes étapes de chacune de ces phases seront ou non mises en œuvre. Le déroulement de la mission de conseil est détaillé plus loin dans ce chapitre.

Missions mixtes

Missions mixtes

Missions d'audit interne intégrant à la fois des éléments d'activités de conseil et d'assurance.

Il importe de souligner qu'une mission n'est pas toujours une mission soit d'assurance soit de conseil. Les auditeurs internes devraient reconnaître que les activités d'assurance et de conseil peuvent être parfois regroupées en une mission unique, souvent appelée « mission mixte ». Les missions mixtes intègrent à la fois des éléments d'activités de conseil et d'assurance. Toute mission associant une composante de prestations d'assurance, telle que l'évaluation indépendante d'un processus ou de contrôles, et une composante de prestations de conseil, par exemple la formulation d'un avis ou une assistance, est une mission mixte. Comme pour toute mission de conseil ou d'assurance, il faut veiller à ce que ni l'indépendance ni l'objectivité ne soient compromises. Même si ces missions comportent à la fois des éléments d'assurance et de conseil, il est souvent nécessaire de communiquer leurs résultats séparément, car la finalité et le périmètre des deux composantes différeront.

Les fonctions d'audit interne ne considèrent pas toutes que les missions d'assurance et de conseil peuvent ou doivent être combinées.

Copyright © 2015 Eyrolles.

Leur décision de structurer ainsi les missions dépend de la philosophie de l'organisation à l'égard de l'audit interne, et notamment ce qui figure dans la charte d'audit interne.

Comme le démontre l'encadré 15-4, il existe de nombreux exemples de missions mixtes. Certaines d'entre elles sont initialement des missions de conseil auxquelles des éléments d'assurance se sont ajoutés, et inversement. Si, au premier abord, l'assurance et le conseil semblent deux activités bien distinctes, cette distinction peut rapidement s'estomper lorsqu'elles sont combinées.

SÉLECTIONNER LES MISSIONS DE CONSEIL À RÉALISER

L'audit interne disposant de ressources limitées, il ne peut pas réaliser toutes les missions de conseil potentielles. Il sélectionne donc des missions en fonction de l'importance du risque ou de l'opportunité. Différentes méthodes permettent d'identifier des missions de conseil potentielles :

- des missions sont proposées lors du processus d'évaluation annuelle des risques et, si elles sont jugées prioritaires, intégrées dans le plan annuel d'audit interne ;
- des missions spécifiques sont demandées par le management ;
- des conditions nouvelles ou qui évoluent justifient que l'audit interne y prête attention.

Quelle que soit la façon dont les missions de conseil potentielles ont été identifiées, elles sont généralement soumises au processus d'évaluation des risques mis en œuvre par l'audit interne, afin de déterminer si le risque ou l'opportunité en question justifie de mobiliser les ressources d'audit interne.

Missions issues du plan annuel d'audit interne

Sources des missions de conseil

– Plan annuel d'audit interne.
– Demandes du management.
– Conditions nouvelles ou évolutions.

Le plus souvent, le plan d'audit interne est établi chaque année. Il englobe les domaines de l'organisation qui ont fait l'objet du processus d'évaluation des risques et qui ont été jugés prioritaires pour l'audit interne. Pour de nombreuses fonctions d'audit interne, ces priorités sont aussi bien des missions d'assurance que des missions de conseil. Même si les missions d'assurance forment l'essentiel du plan d'audit interne, certaines missions de conseil, telles que les projets de développement de systèmes, les *due diligence* et les grandes initiatives de changement, sont parfois déjà connues lorsque le plan d'audit interne est élaboré, et peuvent donc y être intégrées. De plus, un certain nombre d'heures peuvent être réservées, dans le plan d'audit interne, aux missions de conseil qu'il peut être nécessaire d'accomplir au cours de l'année. Bien que des

Copyright © 2015 Eyrolles.

EXEMPLES DE MISSIONS MIXTES

Exemples de missions	Exemples de composantes de prestations d'assurance	Exemples de composantes de prestations de conseil
Due diligence **:** L'audit interne réalise des activités d'assurance et de conseil à l'appui de l'évaluation par le management d'une acquisition potentielle.	• Évaluer l'adéquation des contrôles clés dans certains domaines. • Évaluer l'adéquation de la documentation qui étaye l'évaluation des contrôles par le management (ex. : Article 404 de la loi Sarbanes-Oxley). • Évaluer la rigueur du programme actuel de gestion des risques. • Déterminer si les autres fonctions impliquées dans le processus de *due diligence* ont correctement exercé les responsabilités qui leur avaient été assignées et si elles peuvent étayer les conclusions.	• Élaborer une checklist que les autres fonctions impliquées dans l'évaluation d'une acquisition potentielle pourront utiliser. • Faciliter les discussions avec le management concernant les critères d'évaluation d'une acquisition potentielle.
Développement de systèmes : L'audit interne réalise des activités d'assurance et de conseil pendant et après un projet significatif de conversion de systèmes.	• Déterminer si le processus de développement des systèmes prescrit par l'organisation est suivi tout au long du projet. • Déterminer si les recettes utilisateurs étaient suffisantes et si les résultats étayent la décision du management de poursuivre le projet. • Évaluer si le nouveau système, tel qu'il a été mis en œuvre, atteint les objectifs liés aux systèmes et répond aux besoins des utilisateurs.	• Faciliter le processus de définition des besoins des utilisateurs. • Formuler des conseils sur les meilleures pratiques de développement des systèmes. • Former les utilisateurs sur leurs rôles et responsabilités en matière de développement des systèmes.
Refonte de processus : L'audit interne réalise des activités d'assurance et de conseil pendant et après un projet de refonte de processus.	• Déterminer si l'équipe de refonte de processus a respecté les règles et procédures de refonte prescrites par le management. • Déterminer si les contrôles intégrés dans le nouveau processus sont conçus de manière adéquate.	• Formuler des conseils quant à la manière de mener un projet de refonte de processus avec efficacité et efficience. • Former les personnes impliquées dans le projet sur les étapes à réaliser, les techniques d'analyse et la documentation requise. • Formuler des conseils concernant les procédures spécifiques qui permettront d'améliorer la conception du projet.
Gestion des risques : L'audit interne réalise des activités d'assurance et de conseil à l'appui du programme de gestion des risques de l'organisation.	• Évaluer l'adéquation du programme de gestion des risques existant par rapport aux meilleures pratiques. • Évaluer l'exhaustivité de l'univers des risques de l'organisation et la vraisemblance des notes de risque. • Déterminer si les informations fournies par la direction générale au Conseil sont exactes, pertinentes et complètes.	• Faciliter le processus d'évaluation annuelle des risques. • Formuler des conseils concernant les diverses stratégies applicables pour gérer les principaux risques. • Former les propriétaires de risques sur leurs responsabilités en matière de gestion des risques. • Conseiller le management sur les étapes nécessaires pour initier un programme de gestion des risques à l'échelle de l'organisation.

Michael Head, Kurt Reding et Cris Riddle, « Blended Engagements », *Internal Auditor*, octobre 2010, p. 40-44.

Copyright © 2015 Eyrolles.

missions de conseil soient quelquefois identifiées après la conception du plan d'audit interne, elles restent habituellement soumises au processus d'évaluation des risques par l'audit interne avant d'être intégrées au plan.

Le nombre d'heures consacrées aux missions de conseil, prévu par le plan annuel d'audit ou ajouté ultérieurement, devrait augmenter en fonction du changement organisationnel. La plupart du temps, le complément d'heures consacrées aux missions de conseil remplace les heures allouées aux missions d'assurance dans le plan annuel d'audit. Néanmoins, lorsque l'organisation subit d'importants changements, il est souvent préférable que la fonction d'audit interne consacre son temps à apporter des conseils sur les nouveaux processus plutôt qu'à donner une assurance sur les procédures actuelles. En période de changements, le plan annuel d'audit devrait prendre en compte le temps alloué aux activités de conseil pour les domaines de l'organisation qui connaissent les changements les plus significatifs.

Missions issues de demandes du management

Dans de nombreux cas, il se produit des événements qui étaient imprévus au moment de l'élaboration du plan d'audit interne, ce qui peut amener le management à demander une mission de conseil. Les enquêtes sur une fraude, les projets spéciaux, les comités *ad hoc* et l'examen de nouvelles procédures sont des exemples d'événements imprévus. Ces demandes pèsent sur le budget d'audit interne planifié. Beaucoup de ces projets sont urgents et peuvent par conséquent être prioritaires par rapport aux missions d'assurance prévues dans le plan annuel d'audit interne. D'autres missions de conseil ne nécessitent pas d'efforts à temps plein et peuvent être réalisées parallèlement aux missions d'assurance, sans générer trop de perturbations. La sélection des missions de conseil par l'audit interne doit, bien sûr, être minutieuse, ce qui conduit fréquemment l'audit interne à effectuer une évaluation des risques pour déterminer quelles sont les missions de conseil, demandées par le management, qui sont suffisamment cruciales pour justifier la mobilisation des ressources.

Missions issues de conditions nouvelles ou d'évolutions

Les missions de conseil résultent souvent de conditions nouvelles ou d'évolutions. La fonction d'audit interne a alors la meilleure opportunité de créer de la valeur ajoutée en apportant son point de vue à l'organisation concernant les domaines qui connaissent les changements les plus significatifs. Bien que le management puisse demander des missions de conseil en raison de ces circonstances, il est fréquent que l'audit interne lui-même soit le mieux en mesure

Copyright © 2015 Eyrolles.

de définir des missions de conseil potentielles. L'audit interne étant présent dans tous les domaines de l'organisation, il est, dans de très nombreux cas, informé à l'avance de la réorganisation du management, de la restructuration d'un service, de nouvelles offres de produits, etc., qui peuvent justifier son intervention. De plus, les résultats d'une mission d'assurance peuvent inclure la nécessité de réaliser des activités de conseil. Par exemple, après avoir réalisé une mission d'assurance ayant trait à la planification de la continuité d'activité, l'audit interne peut être chargé d'une mission de conseil destinée à aider l'organisation à élaborer un plan de gestion visant à se préparer à de nouveaux risques. Comme avec d'autres méthodes d'identification, les missions de conseil potentielles ainsi définies sont souvent soumises au processus d'évaluation des risques, afin de déterminer le niveau réel de risque ou d'opportunité qu'elles représentent.

Évaluation des risques des missions de conseil potentielles

L'évaluation des risques de l'audit interne est similaire à l'évaluation du management et à la définition des priorités (voir le chapitre 4, *La gestion des risques*, et le chapitre 9, *La gestion de l'audit interne*). Elle détermine généralement les risques en se fondant sur de nombreux facteurs, sans se limiter à l'impact et à la probabilité d'occurrence des risques. Ces facteurs sont aussi, la plupart du temps, évalués individuellement, et définis au moyen d'une échelle. Certaines fonctions d'audit interne assignent non seulement une cotation du risque globale à chaque mission de conseil potentielle, mais assignent également une note de priorité subjective à chaque mission de conseil potentielle d'après l'importance que l'audit interne lui accorde. Les auditeurs internes tiennent compte des résultats de l'évaluation et de la définition des priorités par le management lorsqu'ils déterminent la note de priorité subjective. En outre, ils prennent en considération le volume des ressources et les compétences nécessaires à la réalisation de la mission de conseil, ainsi que les besoins et attentes du client.

En s'appuyant sur le processus de définition des priorités décrit ci-dessus, l'audit interne détermine quelles missions de conseil doivent être menées. Par ces missions de conseil, il cherche à maximiser la valeur apportée au management par rapport aux ressources engagées, à la maîtrise des risques perçus ou à la mise à profit des opportunités, et la rapidité des prestations fournies. Son objectif ultime est de donner au management les informations nécessaires pour maîtriser les risques et maximiser les opportunités inhérentes aux activités et initiatives qui visent à atteindre les objectifs stratégiques de l'organisation. Lorsque ces missions de conseil ont été déterminées, l'audit interne doit les programmer et leur assigner des ressources.

Copyright © 2015 Eyrolles.

LE DÉROULEMENT DE LA MISSION DE CONSEIL

Étant donné que les missions de conseil peuvent largement différer par leur nature et leur périmètre, le processus qui permet de les mener varie lui aussi d'une mission à l'autre. Parmi les trois types de missions de conseil présentées plus haut, les missions de conseil destinées à formuler un avis sont celles qui s'apparentent le plus aux missions d'assurance. En général, les trois phases d'une mission de conseil destinée à formuler un avis sont les mêmes que pour une mission d'assurance, comme le montre l'encadré 15-5. Il existe toutefois des différences dans la mise en œuvre des étapes composant chaque phase du déroulement d'une mission de conseil destinée à formuler un avis. Certaines étapes sont inutiles.

Rappelons une différence primordiale entre les missions de conseil et d'assurance : les missions de conseil n'imposent pas d'évaluation indépendante dont les résultats seraient utilisés par un tiers. De fait, elles ne font intervenir que deux parties : l'équipe d'audit interne, qui effectue la mission, et une personne ou un groupe (le client), qui demande des prestations indépendantes de conseil, de formation ou d'assistance. La nature et le périmètre des missions de formation et d'assistance étant très divers, ces types de missions

ENCADRÉ 15-5

LE DÉROULEMENT D'UNE MISSION DE CONSEIL DESTINÉE À FORMULER UN AVIS

Planifier	Réaliser	Communiquer
• Déterminer les objectifs et le périmètre de la mission. • Obtenir du client la validation finale des objectifs et du périmètre de la mission. • Comprendre l'environnement de la mission et les processus opérationnels concernés. • Comprendre les risques concernés, le cas échéant. • Comprendre les contrôles concernés, le cas échéant. • Évaluer la conception des contrôles, le cas échéant. • Déterminer l'approche retenue pour la mission. • Allouer des ressources à la mission.	• Rassembler des preuves et les évaluer. • Formuler un avis.	• Déterminer la nature et la forme des communications avec le client de la mission. • Examiner attentivement, avec le client de la mission, l'avis formulé. • Procéder à des communications intermédiaires et préliminaires. • Rédiger le rapport définitif de la mission. • Diffuser le rapport définitif de la mission. • Mettre en œuvre des procédures de surveillance et de suivi, le cas échéant.

Copyright © 2015 Eyrolles.

ne suivent pas un processus général unique. Les processus appliqués sont souvent adaptés à chaque mission. Cependant, les missions de conseil destinées à formuler un avis s'apparentent le plus à des missions d'assurance et suivent le plus souvent l'approche décrite dans l'encadré 15-5 et, par conséquent, constituent le thème central qui sera analysé tout au long de la présente section.

Planifier une mission de conseil destinée à formuler un avis

La planification d'une mission de conseil destinée à formuler un avis s'apparente très largement à celle d'une mission d'assurance, avec certaines exceptions. Premièrement, si elle est sélectionnée après finalisation du plan d'audit interne, sa planification est habituellement plus urgente et doit être achevée dans des délais stricts. Souvent, le calendrier de ce type de mission n'est pas flexible, en raison de circonstances sur lesquelles l'audit interne ne peut pas agir, ou parce que le retour d'informations doit être rapide. Deuxièmement, comme indiqué dans l'encadré 15-5, les étapes de la planification d'une mission d'assurance ne sont pas forcément toutes appropriées. Les circonstances dans lesquelles elles ne le sont pas sont analysées ci-dessous.

Déterminer les objectifs et le périmètre de la mission. La planification commence lorsque la mission de conseil destinée à formuler un avis a été définie et programmée. Un membre de l'équipe de management de l'audit interne doit engager les premières discussions portant sur le périmètre de la mission avec le client, afin de déterminer le niveau approprié des prestations à fournir, ainsi que les objectifs de la mission. Les auditeurs internes chargés de la mission doivent ensuite se réunir avec le client pour comprendre précisément ses attentes. La Norme 2300, Accomplissement de la mission, indique que « les auditeurs internes doivent identifier, analyser, évaluer et documenter les informations nécessaires pour atteindre les objectifs de la mission ». La réussite d'une mission de conseil destinée à formuler un avis est fortement dépendante de la capacité de l'audit interne à comprendre les attentes du client à l'égard de la mission.

Comme pour une mission d'assurance, il importe de formaliser les objectifs au début d'une mission de conseil destinée à formuler un avis. Cependant, ils ne sont pas toujours bien définis initialement et peuvent évoluer au cours de la mission, à mesure que les informations s'accumulent. En voici néanmoins des exemples :

- examiner la conception des contrôles et formuler des suggestions d'amélioration ;
- proposer des éléments à intégrer dans la conception d'un nouveau processus ;

Copyright © 2015 Eyrolles.

- examiner un nouveau système informatique avant sa mise en œuvre ;
- formuler un avis durant une *due diligence* dans la perspective d'une éventuelle fusion ou acquisition.

Étant donné que les missions de conseil destinées à formuler un avis sont souvent menées à la demande du management et que l'audit interne s'attache à répondre aux besoins du client, il est impératif d'établir un périmètre et un planning. Au cours de la mission, le périmètre peut changer, en fonction des informations recueillies et des informations supplémentaires qui émanent du client. Cependant, parce que les ressources d'audit interne sont limitées, il importe de fixer des limites en fonction du périmètre et du planning de la mission.

Obtenir du client la validation finale des objectifs et du périmètre de la mission. Les objectifs et le périmètre d'une mission de conseil destinée à formuler un avis doivent être validés par le client de la mission avant que celle-ci ne commence. Ainsi que l'indique la Norme 2201.C1, « les auditeurs internes doivent établir avec le client donneur d'ordre un accord sur les objectifs et le champ de la mission de conseil, les responsabilités de chacun et plus généralement sur les attentes du client donneur d'ordre. Pour les missions importantes, cet accord doit être formalisé. » Dans la plupart des missions de conseil, les auditeurs internes doivent formaliser le périmètre de la mission, ainsi que les responsabilités y afférentes, et les examiner avec le client de la mission avant de lancer les travaux. Cette façon de procéder permet d'éviter tout malentendu dans le déroulement ultérieur de la mission.

La discussion avec le client à propos des livrables constitue un autre aspect important de la mission de conseil destinée à formuler un avis. Il faut définir les attentes concernant la finalisation de la mission. Ces attentes peuvent différer suivant la nature et le périmètre de la mission et être traitées de manière formelle ou informelle.

Comprendre l'environnement de la mission et les processus opérationnels concernés. Comme au début d'une mission d'assurance, il est essentiel que les auditeurs internes chargés d'une mission de conseil destinée à formuler un avis rassemblent des informations sur le domaine de l'organisation dans lequel cette mission est effectuée. L'audit interne apporte de la valeur en s'appuyant sur la vue d'ensemble qu'il a de l'organisation, ce qui implique de comprendre pleinement le domaine couvert par la mission de conseil.

Comprendre les risques concernés, le cas échéant. Les auditeurs internes qui effectuent la mission doivent, le cas échéant, comprendre la nature des risques liés au domaine couvert par la

Copyright © 2015 Eyrolles.

mission. Lorsqu'ils formulent un avis à propos des risques et de leur gestion, ils doivent bien connaître la tolérance au risque à la fois de l'organisation et du client.

Comprendre les contrôles concernés, le cas échéant. Dans certaines missions de conseil destinées à formuler un avis, il peut être nécessaire de comprendre certains dispositifs de contrôle. Cette étape impose aux auditeurs internes d'utiliser leur capacité de jugement pour décider quels dispositifs de contrôle sont pertinents eu égard aux objectifs de la mission. Lorsque ces contrôles sont bien appréhendés, il convient de les associer aux risques correspondants, identifiés durant l'étape précédente.

Évaluer la conception des contrôles, le cas échéant. Il peut être nécessaire d'évaluer la conception des contrôles définis lors de l'étape précédente, si une telle évaluation est pertinente pour la mission de conseil destinée à formuler un avis. Par exemple, pour améliorer l'efficience d'un processus, il peut être nécessaire de déterminer si les dispositifs de contrôle en place ramènent les risques correspondants à un niveau acceptable, et avec efficience. Si l'auditeur interne recommande au client la suppression, la modification ou l'ajout de contrôles, il sera important de veiller à ce que le nouveau processus – plus efficient – continue de ramener à un niveau acceptable les risques correspondants.

Déterminer l'approche retenue pour la mission. L'approche doit être conçue de manière à permettre la réalisation des objectifs d'une mission de conseil destinée à formuler un avis. À cette fin, les auditeurs internes doivent déterminer la nature, le calendrier de collecte et l'étendue des preuves à recueillir, ainsi que les procédures nécessaires pour obtenir ces preuves. S'il est approprié de bien comprendre les risques et les contrôles, cette approche peut être analogue à celle d'une mission d'assurance telle que la décrit le chapitre 13, *Le déroulement de la mission d'assurance*. Ces missions peuvent être des missions mixtes, c'est-à-dire destinées à permettre la réalisation à la fois d'objectifs de conseil et d'objectifs d'assurance.

Allouer des ressources à la mission. Comme cela a déjà été indiqué, les missions de conseil destinées à formuler un avis sont souvent urgentes. En conséquence, si la mission demandée est acceptée, il est essentiel de veiller à ce que les auditeurs internes qui disposent de l'expérience et des compétences adéquates soient désignés rapidement et que la mission commence elle aussi au plus vite. La plupart du temps, ce sont des auditeurs internes plus expérimentés qui sont chargés de superviser les missions de conseil. Ils possèdent en effet l'expérience la plus fonctionnelle par rapport au domaine étudié.

Copyright © 2015 Eyrolles.

Aspects à prendre en compte dans l'affectation des ressources

– Expérience.
– Compétences.
– Ressources externes.
– Développement des collaborateurs.

Les ressources nécessaires aux missions de conseil sont allouées de la même façon que pour les missions d'assurance. Voici ce que recommande la Norme 2230, Ressources affectées à la mission : « les auditeurs internes doivent déterminer les ressources appropriées et suffisantes pour atteindre les objectifs de la mission. Ils s'appuient sur une évaluation de la nature et de la complexité de chaque mission, des contraintes de temps et des ressources disponibles. » De plus, la MPA 2230-1, Ressources affectées à la mission, précise : « pour déterminer le caractère approprié et suffisant des ressources, les auditeurs internes considèrent les éléments suivants :

- le nombre d'auditeurs internes et le niveau d'expérience de l'équipe d'audit ;
- les connaissances, le savoir-faire et autres compétences des auditeurs internes pour leur affectation à chaque mission d'audit ;
- la disponibilité de ressources externes dans les cas où des connaissances ou des compétences supplémentaires sont requises ;
- les besoins de formation des auditeurs internes pour chaque mission constituent un point de départ pour satisfaire le développement des connaissances nécessaires au niveau de l'audit interne. »

Exécution d'une mission de conseil destinée à formuler un avis

La réalisation d'une mission de conseil destinée à formuler un avis peut revêtir de nombreuses formes. Comme indiqué plus haut dans ce chapitre, une mission de conseil destinée à formuler un avis se compose en partie des mêmes étapes qu'une mission d'assurance. Néanmoins, une forte proportion des travaux destinés à élaborer une documentation et à tester les contrôles ne s'inscrit pas dans le cadre d'une telle mission, et celle-ci s'appuie parfois davantage sur la documentation fournie par le client de la mission. Même si les missions de conseil destinées à formuler un avis ne comportent pas toujours les mêmes étapes, elles peuvent inclure les démarches suivantes :

- compréhension des questions de management relatives au domaine examiné ;
- recueil d'informations ;
- procédures analytiques diverses ;
- examen des divers documents du service ou du département concerné, tels que les organigrammes, flux de processus et procédures ;
- utilisation de techniques d'audit informatisées ;

Copyright © 2015 Eyrolles.

- compréhension des principaux risques ;
- compréhension des contrôles et détermination de ceux qui doivent être améliorés ;
- évaluation de l'efficience des contrôles en place.

Suivant la nature de la mission, certaines de ces procédures peuvent être ou non applicables. Cependant, les deux étapes décrites dans l'encadré 15-5 en ce qui concerne la phase d'exécution de la mission sont pertinentes, sous une forme ou une autre, pour toutes les missions de conseil destinées à formuler un avis.

Rassembler des preuves et les évaluer. Les auditeurs internes qui réalisent des missions de conseil destinées à formuler un avis doivent recueillir des preuves suffisantes et adéquates pour étayer les objectifs de la mission. Ils évaluent ensuite les preuves rassemblées et déterminent la nature de l'avis à rendre. Il importe de présenter par écrit dans des papiers de travail élaborés à cette fin les procédures mises en œuvre, les preuves collectées et l'évaluation de ces preuves. Ces papiers de travail peuvent s'apparenter à ceux des missions d'assurance, décrits au chapitre 13, *Le déroulement de la mission d'assurance*.

Formuler un avis. Après avoir réuni des preuves et les avoir évaluées, les auditeurs internes formulent l'avis qu'ils doivent apporter au client de la mission. Il est essentiel de veiller à ce que cet avis soit pertinent pour les objectifs, compréhensible par le client et qu'il puisse être suivi d'actions. Il doit indiquer clairement au client que les améliorations souhaitées sont possibles. La forme qu'il doit revêtir sera décrite dans la section suivante, mais l'avis lui-même constitue le résultat ultime souhaité par le client de la mission.

Communication et suivi

La communication pour les missions de conseil est tout aussi importante que pour les missions d'assurance. Il existe de nombreuses similitudes entre la communication des résultats des deux types de missions, mais également des différences. Les étapes de la communication des résultats d'une mission de conseil sont présentées ci-après.

Déterminer la nature et la forme des communications avec le client de la mission. La communication dans le cadre d'une mission de conseil peut revêtir de nombreuses formes. Suivant la nature de la mission et les attentes du client, la communication des résultats de cette mission peut être moins formelle que celle d'une mission d'assurance : elle peut faire l'objet, par exemple, d'une présentation, d'une note ou d'un courriel. Dans d'autres cas, le management peut demander à l'audit interne d'exprimer un avis

Copyright © 2015 Eyrolles.

impromptu, par exemple, sur les avantages et inconvénients de l'internalisation ou de l'externalisation d'une fonction. À l'inverse, un rapport formel peut parfois être souhaité. Ainsi, l'audit interne peut être membre d'un comité ou d'une équipe-projet qui évalue un processus ou un produit, et son avis peut faire partie intégrante de la réussite de ce projet. Dans ce cas, un rapport formel peut être souhaité, afin que l'avis formulé soit approprié et rendu en temps opportun.

Examiner attentivement, avec le client de la mission, l'avis formulé. Bien que l'avis rendu puisse sembler approprié aux auditeurs internes qui réalisent la mission de conseil, il peut exister d'autres informations ou facteurs dont ces derniers n'ont pas connaissance et qui pourraient influer sur l'adéquation de l'avis. Il faut donc examiner de près l'avis avec le client, afin de s'assurer :

- qu'il est compris par celui-ci ;
- qu'il répond aux objectifs de la mission de conseil ;
- qu'il est pratique et qu'il peut être mis en œuvre avec un bon rapport coût-efficacité.

Procéder à des communications intermédiaires et préliminaires. En raison du caractère urgent de nombreuses missions de conseil destinées à formuler un avis, il convient de communiquer fréquemment avec le client au cours de la mission. Cette communication peut revêtir de nombreuses formes mais, lors des étapes intermédiaires de la mission, elle s'effectue souvent oralement, par téléconférence ou échange de courriels. Elle est souvent liée à des dates clés importantes tout au long de la mission et à des points de décision clés. De plus, à mesure que les détails du projet sont connus, ou que certains facteurs évoluent, les attentes relatives aux prestations de conseil peuvent changer et doivent donc être communiquées.

Rédiger le rapport définitif de la mission. Comme pour la communication intermédiaire, le rapport final de la mission peut varier par son format et son degré de formalisme. Ainsi que nous l'avons indiqué plus haut, il peut être peu formel (présentation, note ou courriel). Cependant, son format et son degré de formalisme dépendent aussi de ce qui a été convenu avec le client de la mission. Ainsi, celui-ci peut demander un feu vert oral avant la transformation d'un système ou le lancement d'une initiative majeure. L'audit interne peut être l'un des nombreux acteurs à intervenir dans ce type de décision (feu vert accordé ou rejeté) avant que l'organisation ne lance le processus. Si une surveillance ou un suivi sont nécessaires ou convenus avec le client de la mission, le rapport final peut indiquer qu'une telle action sera mise en œuvre. Les encadrés 15-6 et 15-7 sont des exemples de communication intermédiaire et finale concernant une mission de conseil destinée à formuler un avis.

Copyright © 2015 Eyrolles.

COMMUNICATION INTERMÉDIAIRE DANS LE CADRE D'UNE MISSION DE CONSEIL

De : Moritz, Lenny F.
Envoyé le : Jeudi 13 mars 20XX, 14 h 44
À : Fish, Kerry S.
Objet : Avancement du projet de conversion de données clients

Projet de conversion de données clients
Avancement de l'examen – Étapes suivantes

- **Examen préalable à la conversion**
  - Réalisation de la mission d'audit (2 mai 20XX).
  - Finalisation de la matrice de contrôles (COSO).
  - Surveillance continue.
  - Présentation du rapport final à Kerry Fish et Julie Sangren le 3 mai 20XX (ou à une date proche).
- **Examen lors de la conversion et ultérieurement**
  - Périmètre de l'examen.
  - Réalisation appropriée du plan d'exécution relatif au week-end consacré à la conversion, y compris la mise en œuvre des mesures critiques, des communications adéquates et la résolution des problèmes en temps opportun.
  - Exactitude et exhaustivité de la conversion de données clients.
  - Conversion de la conservation des titres (actions, obligations, fonds communs de placement, options, etc.), y compris la transition de la conservation physique et le déplacement autorisé et sécurisé des titres.
  - Conversion de la gestion de la trésorerie, y compris le transfert de propriété des comptes de trésorerie et le déplacement autorisé et sécurisé de la trésorerie.
  - Conformité réglementaire et respect des exigences connexes relatives au calcul des capitaux nets.
  - Validation des contrôles clés d'équilibrage et de rapprochement postérieurs à la conversion (comme les rapprochements liés aux dépôts).
  - Travaux sur site prévus au cours du week-end consacré à la conversion et ultérieurement.
  - Présentation du rapport final le 25 mai 20XX (ou à une date proche).

Projets prioritaires portant sur les écarts (finaux)

Projet	Responsable	Date du rapport	Note du rapport
Reconversion de la Banque de Chine	Braden House	28 juin 20XX	SATISFAISANT
Déploiement de l'infrastructure de la banque de détail	Stacie Waverly	22 septembre 20XX	SATISFAISANT
Portail client consolidé	Frank Daniels	20 octobre 20XX	SATISFAISANT
Évaluation de la valeur nette	Stacie Waverly	8 décembre 20XX	SATISFAISANT
Intégration de la TAO	Janis Pearlman	12 janvier 20XX	SATISFAISANT
Autorisation officielle	Stacie Waverly	9 mars 20XX	SATISFAISANT

Lenny Moritz
Manager Audit
Services financiers BUS
lmoritz@BUS.com

Copyright © 2015 Eyrolles.

ENCADRÉ 15-7

RAPPORT DÉFINITIF D'UNE MISSION DE CONSEIL

BUS

À : Comité de pilotage de la conversion,
Kerry Fish et Julie Sellers

De : Lenny Moritz, Manager Audit
Services financiers BUS

Objet : Projet de conversion de données clients de la Banque de Chine
Examen préalable effectué dans le cadre d'une mission de conseil destinée à formuler un avis

Date : 30 mai 20XX

Le service d'audit du groupe a achevé l'examen préalable effectué dans le cadre de la mission de conseil destinée à formuler un avis sur le projet de conversion de données clients de la Banque de Chine. Cet examen, terminé le 11 mai 20XX, a consisté à présenter au comité de pilotage de la conversion un avis quant à la capacité de cette institution à achever la conversion de ses données clients le 12 juin 20XX.

Le périmètre de la mission incluait, sans s'y limiter, un examen des activités suivantes préalables à la conversion.

- Identification et élimination de toutes les failles fonctionnelles entre les systèmes BUS patrimoniaux et les systèmes de la Banque de Chine.
- Évaluation des capacités des systèmes et des processus à permettre une conversion des données clients précise et rapide (comptes, actifs et utilisation des services Internet, notamment).
- Réception des autorisations officielles requises, afin de poursuivre le projet de conversion des données clients.
- Identification et gestion des risques liés au projet, à la technologie et aux opérations.

Résultats

Globalement, les activités de préconversion sont gérées et surveillées efficacement par le comité de pilotage de la conversion. Au cours de notre examen, plusieurs points ont attiré notre attention. Nous pensons qu'ils doivent être réglés avant le lancement de la conversion des données. En l'absence de solution appropriée, la réussite de la conversion sera compromise. Si une solution rapide n'est pas possible, il convient d'envisager de retarder cette conversion. Le comité de pilotage de la conversion doit s'attacher à régler ces problèmes en priorité.

Points préoccupants

Élimination des failles fonctionnelles – Plusieurs failles fonctionnelles subsistent, et sont considérées comme des raisons d'arrêter le projet de conversion des données clients. Le comité de pilotage de la conversion opère un suivi actif de ces dysfonctionnements et pense qu'ils seront réglés avant le week-end consacré à la conversion.

Test du système d'information du support client BUS – Le test intégral de validation du logiciel d'application du support client n'a pas été achevé et il subsiste des incohérences de format des données, qui empêchent le système d'accepter entièrement toutes les données de la Banque de Chine. Le comité de pilotage de la conversion pense que ce test sera achevé en temps voulu et que toutes les incohérences seront éliminées avant la conversion des données clients.

Autorisation officielle – L'autorisation officielle de poursuivre le projet de conversion des données clients n'a pas encore été reçue. Elle devrait être obtenue dans la semaine du 7 juin, et le comité de pilotage de la conversion pense qu'elle sera accordée avant le week-end consacré à la conversion.

Diffuser le rapport définitif de la mission. Contrairement aux missions d'assurance dans lesquelles, parmi les destinataires de la communication finale, figurent un certain nombre de personnes

Copyright © 2015 Eyrolles.

qui ont éventuellement un lien direct avec le domaine examiné, les résultats finaux d'une mission de conseil ne sont diffusés qu'au client auquel l'audit interne a fourni la prestation. Sauf si le rapport final porte sur une mission mixte incluant des activités d'assurance, c'est habituellement au client qu'il appartient d'élargir sa diffusion à d'autres parties.

Mettre en œuvre des procédures de surveillance et de suivi, le cas échéant. Dans une mission de conseil, les procédures de surveillance et de suivi peuvent ne pas être nécessaires dans la mesure où le management peut demander un certain nombre de choses qui ne nécessitent pas de suivi sous une forme ou une autre. Dans le cadre de la phase « clôturer la mission de conseil », l'audit interne doit informer le management et convenir avec lui de toute procédure de surveillance ou de suivi qui doit être mise en œuvre dans le domaine couvert par la mission. Le cas échéant, « l'audit interne doit surveiller la suite donnée aux résultats des missions de conseil conformément à l'accord passé avec le client donneur d'ordre » (Norme 2500.C1).

PAPIERS DE TRAVAIL D'UNE MISSION DE CONSEIL

Comme dans les missions d'assurance, et quel que soit leur type, les tâches effectuées dans le cadre d'une mission de conseil destinée à formuler un avis doivent être présentées dans des papiers de travail. La Norme 2330.C1 impose au responsable de l'audit interne de « définir des procédures concernant la protection et la conservation des dossiers de la mission de conseil ainsi que leur diffusion à l'intérieur et à l'extérieur de l'organisation. Ces procédures doivent être cohérentes avec les orientations définies par l'organisation et avec toute exigence réglementaire ou autre appropriée ». Le niveau de documentation requis pour les missions de conseil diffère d'une fonction d'audit interne à l'autre et selon la nature de la mission. Cependant, dans la plupart des cas, le volume et le temps consacré à cette documentation sont nettement inférieurs à ceux nécessaires pour une mission d'assurance. En général, l'accent est mis sur le rapport final et sur la formulation d'observations et de recommandations au management. Il convient d'établir une documentation suffisante pour étayer ces recommandations globales de l'audit interne.

Il importe de documenter les résultats des activités de conseil à mesure qu'ils sont connus. Il convient de garder des dossiers sur les travaux effectués pour étayer les avis communiqués au client. Plus précisément, cette documentation doit corroborer les postulats et hypothèses sous-tendant les avis. De plus, l'audit interne peut estimer qu'elle améliore l'efficacité et l'efficience de futures missions d'audit interne similaires.

Créer de la valeur ajoutée

Les activités d'assurance comme les activités de conseil apportent de la valeur ajoutée en contribuant à améliorer les opportunités de réaliser les objectifs de l'organisation, en identifiant les améliorations possibles sur le plan opérationnel, et/ou en réduisant l'exposition aux risques.

Copyright © 2015 Eyrolles.

Atteintes à l'indépendance ou à l'objectivité

Survenue de menaces risquant de limiter de manière significative, dans les faits ou en apparence, la capacité de l'auditeur interne à mener une mission sans parti pris ni entrave.

ÉVOLUTION DE L'ENVIRONNEMENT DES ACTIVITÉS DE CONSEIL

Traditionnellement, l'audit interne se concentre principalement sur les activités d'assurance, car c'est sur elles que s'appuient les organisations pour se fier aux possibilités de maîtriser suffisamment les risques qui menacent la réalisation de leurs objectifs. Le cadre de réglementation mondial actuel n'y est pas pour rien. Néanmoins, les organisations reconnaissent de plus en plus la valeur ajoutée que l'audit interne peut créer en réalisant des activités de conseil. Leurs connaissances et leurs compétences concernant la gouvernance, la gestion des risques et les contrôles ayant progressé ces dernières années, les auditeurs internes disposent de nombreuses opportunités pour mettre à profit ce savoir-faire et produire de la valeur ajoutée grâce à des activités de conseil.

Bien que la forte proportion des ressources d'audit interne allouée aux activités de conseil progresse, il reste beaucoup d'opportunités d'accroître la valeur ajoutée générée pour l'organisation par ces activités. L'accélération des changements à l'échelle mondiale offre d'excellentes opportunités pour l'élargissement des activités de conseil, car les organisations s'attachent en permanence à développer leur chiffre d'affaires et à maîtriser leurs coûts. Étant donné ses connaissances et ses compétences, l'audit interne est une source de première importance sur laquelle le management peut s'appuyer pour obtenir des conseils, une assistance ou une formation. Dans un nombre croissant d'organisations, les leaders qui savent anticiper reconnaissent cet atout et s'associent à l'audit interne de manière nouvelle et créative.

Lorsque le management d'une organisation ne perçoit pas une opportunité de tirer ainsi parti de l'audit interne, le responsable de l'audit interne doit l'informer de la valeur ajoutée qu'il peut créer en partenariat avec d'autres services de l'organisation pour atteindre des objectifs non liés à l'assurance. À mesure que les responsables de l'audit interne s'affirment comme les agents du changement au sein de leur organisation, ils doivent veiller à ce que la fonction d'audit interne qu'ils supervisent soit à même d'apporter des conseils à valeur ajoutée. Ils peuvent jeter les bases de ce partenariat avec d'autres services en :

- établissant des relations avec d'autres départements de l'organisation ;
- accroissant les compétences thématiques des auditeurs internes *via* :
  - la formation ;
  - leur passage dans des unités opérationnelles ;
- embauchant des collaborateurs venant d'autres unités opérationnelles ;

Copyright © 2015 Eyrolles.

- obtenant l'adhésion du comité d'audit et de la direction générale grâce à la présentation des avantages résultant de l'accroissement des activités de conseil.

CAPACITÉS NÉCESSAIRES

L'élargissement des opportunités résultant de ces évolutions encouragent les responsables de l'audit interne progressistes à faire en sorte que leur équipe dispose des compétences requises pour proposer des activités de conseil à valeur ajoutée. Ces responsables savent que, pour fournir efficacement ces prestations, les auditeurs internes doivent se montrer très polyvalents et à même d'apprendre rapidement. De plus, en fonction de la mission de conseil, les auditeurs internes peuvent avoir besoin d'une expérience et d'un savoir-faire importants en ce qui concerne la conception et l'ingénierie de processus, l'assistance, la réflexion stratégique, l'établissement d'un consensus et/ou la résolution créative de problèmes. En raison de la nature dynamique de leur profession en général, de nombreux auditeurs internes disposent déjà des compétences nécessaires pour agir comme consultants. Néanmoins, ceux qui procèdent par checklist et qui préfèrent utiliser des techniques d'audit courantes normalisées ont tendance à être moins à l'aise lorsqu'ils sont chargés d'activités de conseil, missions moins structurées et moins dynamiques.

Compétences et expérience requises

Les auditeurs internes qui souhaitent faire du conseil au sein du service d'audit interne dans lequel ils travaillent doivent acquérir des compétences spécifiques. Bien que nombre de ces compétences soient les mêmes que pour les missions d'assurance, elles doivent être encore plus affirmées chez les auditeurs internes qui accomplissent des missions de conseil. Voici, plus précisément, ce que l'on attend d'eux :

- des compétences en termes d'assistance et de travail en équipe ;
- une large expérience de la vie des organisations et la maîtrise d'une discipline spécifique (comptabilité, SI ou réglementation, par exemple) ;
- une aisance relationnelle et un grand sens des relations humaines ;
- un mode de pensée analytique et la capacité à résoudre des problèmes non structurés ;
- la capacité à apprendre et à s'adapter rapidement dans un environnement dynamique ;

Copyright © 2015 Eyrolles.

- la capacité à traiter l'information et à répondre rapidement aux demandes ;
- la capacité à exposer des résultats et à en rendre compte rapidement, que ce soit sous la forme de présentations, de communications écrites ou orales.

Sous-traitance

Parfois, l'audit interne ne dispose pas des compétences techniques spécialisées qui sont nécessaires pour certaines missions de conseil. Si tel est le cas, il peut avoir besoin de les obtenir auprès d'experts internes ou externes, comme indiqué dans la Norme 1210.C1 : « Le responsable de l'audit interne doit décliner une mission de conseil ou obtenir l'avis et l'assistance de personnes qualifiées si les auditeurs internes ne possèdent pas les connaissances, le savoir-faire et les autres compétences nécessaires pour s'acquitter de tout ou partie de la mission. » Les domaines dans lesquels il peut être nécessaire de recourir à des spécialistes extérieurs sont par exemple les suivants :

- reporting financier ;
- SI ;
- gestion de trésorerie ;
- enquêtes sur des fraudes ;
- ingénierie et respect des normes environnementales ;
- conformité à la réglementation.

Le type d'expert extérieur auquel il faut recourir dépend des connaissances spécialisées nécessaires pour telle ou telle mission. Les experts dont on peut solliciter un avis et une assistance sont notamment :

- les prestataires de services d'audit interne ;
- les comptables extérieurs ou les spécialistes de la fiscalité ;
- les spécialistes des systèmes d'information et de la sécurité ;
- les spécialistes des enquêtes sur les fraudes ;
- les actuaires, statisticiens et évaluateurs ;
- les ingénieurs, géologues et spécialistes de l'environnement ;
- les juristes.

Le responsable de l'audit interne doit vérifier que les ressources nécessaires sont disponibles au sein de l'organisation. Cependant, si ce n'est pas le cas, il est prudent de faire appel à des spécialistes extérieurs pour répondre à un besoin spécifique dans le cadre d'une

Copyright © 2015 Eyrolles.

mission de conseil. Quoi qu'il en soit, les *Normes* indiquent clairement qu'il faut davantage s'attacher à la qualité des prestations et à la valeur ajoutée ainsi créée pour l'organisation qu'à leur origine. Néanmoins, même lorsque des spécialistes extérieurs sont sollicités pour une mission, l'audit interne doit conserver le contrôle global et la responsabilité de supervision de la mission de conseil. Voir le chapitre 9, *La gestion de l'audit interne*, pour de plus amples informations sur le co-sourcing des activités d'audit interne.

OPPORTUNITÉS POUR UN POINT DE VUE DE L'AUDIT INTERNE

Comme indiqué tout au long de ce chapitre, les activités de conseil offrent aux auditeurs internes la possibilité de créer de la valeur ajoutée en apportant leur point de vue à l'organisation. L'encadré 15-8 en présente 10 opportunités.

ENCADRÉ 15-8

APPORTER SON POINT DE VUE DANS LE CADRE DE MISSIONS DE CONSEIL 10 OPPORTUNITÉS POUR L'AUDIT INTERNE

- Réaliser une évaluation des risques liée aux missions de conseil, et veiller à ce que la fonction d'audit interne participe aux initiatives les plus risquées pour l'organisation.
- Collaborer avec la direction générale pour impliquer l'audit interne lors de projets clés.
- Faciliter les principales activités de gestion des risques de l'organisation et dispenser une formation sur les contrôles et les risques de l'organisation.
- Formuler des recommandations informelles lorsque des possibilités d'amélioration des contrôles, d'économies de coûts et d'efficience sont identifiées dans certains domaines.
- Proposer l'expertise de la fonction d'audit interne lors des événements importants qui nécessitent une expertise supplémentaire (à savoir des sinistres, des violations de la sécurité et des fraudes).
- Employer des experts qui apportent des avis lorsque les ressources internes ne sont pas suffisantes au sein de l'organisation.
- Apporter des éclairages dans le cadre des initiatives de changement de l'organisation.
- Aider à la revue des nouvelles règles et procédures.
- Rester au fait de l'actualité et des problématiques réglementaires susceptibles d'influer sur l'organisation et évaluer cet impact potentiel pour le compte du management.
- Formuler des recommandations prospectives qui apportent un point de vue.

Copyright © 2015 Eyrolles.

RÉSUMÉ

Les organisations étant soumises à des pressions économiques de plus en plus fortes pour optimiser l'utilisation de leurs ressources, l'audit interne peut optimiser la valeur ajoutée qu'il crée pour l'organisation en réalisant davantage d'activités de conseil. Lorsque le nombre des missions de conseil réalisées augmente, tant l'organisation que l'audit interne peuvent en retirer de nombreux avantages, comme le montre ce chapitre.

En s'attachant à former les auditeurs internes et en adhérant aux lignes directrices énoncées dans les *Normes*, l'audit interne peut préserver son indépendance et les auditeurs internes conserver leur objectivité tout en réalisant des activités de conseil de grande qualité pour leur organisation. Un solide processus d'évaluation des risques permet aux auditeurs internes de sélectionner les missions de conseil qui créent le plus de valeur. En respectant le déroulement d'une mission de conseil destinée à formuler un avis, processus décrit dans ce chapitre, on peut répondre aux attentes spécifiques des clients.

Les activités de conseil offrent aux auditeurs internes de nombreuses opportunités d'étoffer leurs connaissances et leurs compétences dans des domaines qui ne font pas toujours partie intégrante de l'environnement d'une mission d'assurance. Plus l'audit interne alloue de ressources aux missions de conseil, plus les organisations prennent pleinement conscience de l'importance de l'audit interne.

Copyright © 2015 Eyrolles.

Questions de révision

1. En quoi l'audit interne est-il bien placé pour créer de la valeur en apportant son point de vue dans le cadre de ses activités de conseil ?

2. Quelles sont les différences entre une mission d'assurance et une mission de conseil ?

3. Quels sont les trois types de missions de conseil que l'audit interne peut accomplir ? Donnez un exemple de chacun d'entre eux.

4. Qu'est-ce qu'une mission mixte et quand celle-ci est-elle appropriée ?

5. Quelles sont les trois méthodes qui permettent d'identifier des missions de conseil potentielles ?

6. Comment sont intégrées les activités de conseil dans le plan annuel d'audit interne ?

7. Comment l'audit interne décide-t-il des missions de conseil à réaliser ?

8. Quelles sont les trois phases d'une mission de conseil destinée à formuler un avis ?

9. Quelles sont les étapes comprises dans une mission de conseil destinée à formuler un avis, au niveau de :
   a. la planification ?
   b. la réalisation ?
   c. la communication des résultats ?

10. Pourquoi est-il essentiel d'élaborer et de conserver de solides papiers de travail dans le cadre d'une mission de conseil ?

11. Comment le responsable de l'audit interne peut-il sensibiliser le management à l'importance des activités de conseil pour l'organisation ?

12. Quelles capacités l'audit interne doit-il posséder pour réaliser des activités de conseil à valeur ajoutée ?

13. Quelles compétences spécifiques un auditeur interne doit-il posséder pour effectuer des missions de conseil ?

14. Dans quels types de domaines peut-il être nécessaire de faire appel à des spécialistes extérieurs pour effectuer des missions de conseil de manière efficace ? À quels types de spécialistes extérieurs peut-on demander d'apporter une aide dans le cadre des missions de conseil ?

Copyright © 2015 Eyrolles.

Questions à choix multiples

Sélectionnez la meilleure réponse pour chacune des questions suivantes.

1. Laquelle des activités suivantes est typiquement une mission de conseil effectuée par l'audit interne ?
   a. La vérification de la conformité aux règles et procédures relatives aux comptes fournisseurs.
   b. La mise en place d'une mission destinée à tester les contrôles applicatifs des systèmes d'information.
   c. L'examen et le commentaire d'un projet de nouvelle politique de déontologie élaboré par l'organisation.
   d. La vérification de l'adéquation de la conception des contrôles portant sur la résiliation des contrats de travail des collaborateurs.

2. Lequel des aspects suivants de la compétence et de la conscience professionnelle n'est-il pas nécessaire de prendre en compte lorsque l'on décide d'accomplir une mission de conseil ?
   a. La disponibilité des qualifications et ressources adéquates pour mener à bien la mission.
   b. Les besoins et attentes du client de la mission.
   c. Le coût de la mission par rapport à ses avantages potentiels.
   d. L'impact potentiel sur l'audit financier effectué par l'auditeur externe.

3. La direction générale d'une organisation demande à l'audit interne d'aider à former les collaborateurs aux concepts relatifs au contrôle interne. De quel type de mission s'agit-il ?
   a. Mission d'assurance.
   b. Mission de conseil axée sur la formation.
   c. Mission de conseil visant à apporter une assistance.
   d. Mission de conseil destinée à formuler un avis.

4. Quel type d'activité l'audit interne devrait-il exécuter ? Compte tenu des propositions ci-après :
   a. Élaboration de contrôles portant sur un processus.
   b. Formulation d'une nouvelle politique relative aux lanceurs d'alerte.
   c. Examen d'une nouvelle application informatique avant sa mise en œuvre.
   d. Pilotage d'un projet de refonte de processus.

Copyright © 2015 Eyrolles.

Questions à choix multiples

5. Laquelle des tâches suivantes n'est pas susceptible de constituer une étape d'une mission de conseil ?
   a. Comprendre les objectifs d'un processus.
   b. Évaluer les risques liés à un processus.
   c. Présenter sous forme d'un diagramme de flux les principales étapes d'un processus.
   d. Rendre une conclusion sur l'adéquation de la conception et le fonctionnement effectif d'un processus.

6. La directrice de l'exploitation a demandé à l'audit interne de la conseiller sur un nouveau plan d'incitations, en cours d'élaboration, pour les commerciaux. Laquelle des tâches suivantes le responsable de l'audit interne doit-il refuser d'accomplir dans le cadre de cette mission de conseil ?
   a. Rechercher et comparer les plans d'incitations instaurés par d'autres organisations du même secteur.
   b. Déterminer le mode approprié de calcul des primes, pour intégration dans le plan d'incitations.
   c. Recommander des procédures de surveillance afin que les montants appropriés soient versés dans le cadre du plan de primes.
   d. Définir la meilleure façon de conserver les pièces justificatives des montants versés, afin de créer une piste d'audit suffisante.

7. L'équipe d'audit interne, lorsqu'elle est confrontée à la limitation du périmètre d'une mission suite à la perte ou l'absence d'exhaustivité de plusieurs données de production, réalise une mission de conseil destinée à améliorer l'efficience d'un processus de production. Dans cette limitation du périmètre de la mission, il convient que le responsable de l'audit interne :
   a. Arrête la mission de conseil et procède à une mission d'assurance distincte, afin de déterminer pourquoi les données n'étaient pas disponibles.
   b. Discute du problème avec le client et détermine avec lui s'il faut continuer la mission.
   c. Achève l'analyse sans les données mais inclut une limitation de son périmètre dans le rapport de la mission.
   d. Rende compte de la limitation du périmètre aux auditeurs externes.

8. Le comité d'audit a demandé à l'audit interne d'aider au processus d'évaluation annuelle des risques. À quel type de mission de conseil cette aide correspond-elle ?
   a. Une mission d'assurance.
   b. Une mission de conseil axée sur la formation.
   c. Une mission de conseil visant à apporter une assistance.
   d. Une mission de conseil destinée à formuler un avis.

Copyright © 2015 Eyrolles.

Thèmes de discussion

1. Expliquez comment l'audit interne peut préserver son indépendance tout en travaillant avec le management au déploiement de meilleures pratiques de gestion des risques et à l'amélioration du système de contrôle interne dans toute l'organisation.

2. Une fonction d'audit interne a accepté de réaliser une mission de conseil destinée à formuler un avis, dans le but d'évaluer l'efficience d'un processus. Au cours de cette mission, un auditeur interne détecte une faiblesse dans les contrôles qui pourrait avoir de graves conséquences pour l'organisation. Sachant qu'une mission de conseil fait intervenir deux parties, le client et l'auditeur, est-il obligatoire de révéler cette faiblesse à la direction générale et au comité d'audit ? Quels sont les avantages et les inconvénients de la communication de cette faiblesse par l'auditeur interne ?

3. Décrivez une situation dans laquelle l'auditeur interne pourrait être accusé de ne pas être suffisamment objectif lorsqu'il réalise des activités de conseil.

4. En général, une charte d'audit interne détermine la nature des prestations fournies par l'audit interne. Quels sont les avantages et les inconvénients à élaborer une charte qui n'autorise pas expressément la réalisation d'activités de conseil ?

5. Pourquoi est-il important que l'audit interne évalue les risques avant d'accepter une mission de conseil ? Votre réponse doit tenir compte des risques à la fois pour l'organisation et pour l'audit interne.

6. Les missions de conseil peuvent-elles être structurées de manière à donner aussi une assurance ? Pourquoi ?

7. Pour une organisation en cours d'acquisition, la participation de l'audit interne serait-elle considérée comme une activité d'assurance ou comme une activité de conseil ? Expliquez votre réponse.

8. Décrivez les principales étapes qu'un audit interne doit suivre s'il est chargé d'aider à l'évaluation des risques de l'organisation.

Copyright © 2015 Eyrolles.

ÉTUDES DE CAS

CAS N° 1

Vous travaillez pour une organisation nouvelle, dont l'activité principale est la vente de produits sur Internet et dont le modèle économique s'apparente à celui d'eBay. Cette société est régie par les mêmes principes qu'eBay et organise des enchères électroniques, mais offre en plus l'avantage de disposer d'un site commun qui traite avec les clients dans le monde entier. Son directeur général sait que la confidentialité des données personnelles est très importante dans les activités en ligne. Il a donc demandé à l'audit interne d'élaborer à l'intention de la clientèle une politique *ad hoc*, reposant sur les bonnes pratiques, car le slogan de cette nouvelle organisation est « la confidentialité des données personnelles est notre préoccupation ». L'entité n'a pas de responsable de la confidentialité des données personnelles, ni de la conformité, et n'envisage pas non plus d'en recruter un. Le directeur général attend du responsable de l'audit interne qu'il conduise ce projet et qu'il veille à ce que la campagne de promotion corresponde au slogan de l'organisation. La campagne publicitaire devant être lancée dans un mois, le directeur général souhaite que les documents relatifs à la confidentialité des données personnelles soient finalisés le plus rapidement possible.

1. Identifiez les principales sources traitant de la confidentialité des données personnelles sur lesquelles vous pouvez vous appuyer pour définir les bonnes pratiques.

2. Déterminez les étapes de la mission de conseil que vous devez mettre en œuvre et les services de l'organisation auxquels vous devez demander de participer au projet.

3. Identifiez les documents que vous devez élaborer dans le cadre de la mission de conseil et les informations que vous devez présenter au directeur général.

CAS N° 2

Une grande banque internationale envisage d'externaliser tous les aspects de sa fonction ressources humaines, notamment le recrutement, les prestations sociales, la paie, la formation, le développement des collaborateurs, la rémunération et les systèmes d'information. Elle a identifié trois prestataires potentiels. Sa fonction d'audit interne est chargée d'examiner le processus de sélection des fournisseurs et d'évaluer le système de contrôle interne de chacun. La direction générale souhaite prendre une participation de 10 % dans le capital du prestataire extérieur retenu.

Les modalités initiales de l'accord imposent de transférer 1 000 collaborateurs de la banque à la société qui sera *in fine* retenue. Ce prestataire devra alors évaluer les performances de ces collaborateurs et déterminer à l'issue d'une période de six mois lesquels feront l'objet d'un programme de reconversion en interne, organisé sur la base du volontariat.

Copyright © 2015 Eyrolles.

ÉTUDES DE CAS

Le prestataire peut déterminer quels systèmes informatiques sont utilisés. Le contrat sera conclu pour 5 ou 10 ans, en fonction de sa forme de tarification.

La banque espère que cet accord d'externalisation lui permettra de réaliser des gains financiers importants, y compris des réductions de coûts significatives liées à la conversion en applications classiques réalisée par le prestataire. Le prestataire extérieur devra tirer profit de ses systèmes, de ses processus et de ses collaborateurs, et être à même de dégager un bénéfice grâce aux économies d'échelle, en particulier au niveau des systèmes.

1. Quel rôle l'audit interne doit-il jouer dans la décision de la banque d'externaliser cette fonction ?

2. Quels sont les aspects spécifiques que l'audit interne doit examiner durant la phase de transition ?

3. Quels risques la banque doit-elle prendre en compte pendant la phase de transition ? Et après l'achèvement de la transition ?

4. Quels types d'activités de conseil effectués par l'audit interne, portant sur les ressources humaines externalisées, pourraient être appropriés après l'achèvement de la transition ?

Copyright © 2015 Eyrolles.

RÉFÉRENCES

CHAPITRE 1
Introduction à l'audit interne

1 *The Value Proposition of Internal Auditing and the Internal Audit Capability Model* (Altamonte Springs, Floride : *The Institute of Internal Auditors*, 2012), p. 4.

2 IIA /IFACI (trad.), *Cadre de référence international des pratiques professionnelles de l'audit interne* (Paris : IFACI, 2014), p. 15.

3 *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) / PwC/ IFACI (trad.), *Le management des risques de l'entreprise : Cadre de référence – Techniques d'application* (Paris : Éditions d'Organisation, 2005), pp. 44-45.

4 David Calloway, *Internal Auditing: A Guide for the New Auditor* (Altamonte Springs, Floride : The Institute of Internal Auditors, 1995), p. 1.

5 www.theiia.org.

6 Ibid.

7 *The Value Proposition of Internal Auditing and the Internal Audit Capability Model.*

8 www.theiia.org.

9 Ibid.

10 IIA /IFACI (trad.), *Cadre de référence international des pratiques professionnelles de l'audit interne*, pp. 8-9.

11 Ibid.

12 www.theiia.org.

13 Rudyard Kipling, « L'enfant d'éléphant », dans *Histoires comme ça* (Paris : Gallimard Jeunesse, 2008).

CHAPITRE 2
Le Cadre de référence international des pratiques professionnelles : des lignes directrices incontournables pour l'audit interne

1 Sridhar Ramamoorti, « Internal Auditing: History, Evolution, and Prospects », in Bailey et al. *Research Opportunities in Internal Auditing* (Altamonte Springs, Floride : The Institute of Internal Auditors, 2003), p. 5.

2 *Independence and Objectivity: A Framework for Internal Auditors* (Altamonte Springs, Floride : The Institute of Internal Auditors, 2001), p. 15.

3 David R. Plumlee, « The Standard of Objectivity for Internal Auditors: Memory and Bias Effects », *Journal of Accounting Research* (automne 1985), pp. 683-699.

4 Le programme de cours (« *Exam content* ») de préparation à l'examen du CIA est disponible sur le site internet de l'IIA, à la rubrique « Certification ».

Copyright © 2015 Eyrolles.

RÉFÉRENCES

5 *A Vision for the Future: Guiding the Internal Audit Profession to Excellence – Report from The IIA's Vision for the Future Task Force* (Altamonte Springs, Floride : The Institute of Internal Auditors, 2007), p. 11.

6 *Treasury Regulations for Departments, Constitutional Institutions and Public Entities* (Le Cap et Pretoria : Trésor national, République d'Afrique du Sud, novembre 2012, sections 5.1.4 et 5.1.5).

7 Institute of Directors in Southern Africa, *King Report on Governance for South Africa 2009, (King III Report)* (Johannesburg : IOD, 2009, section 7.1.4).

8 *Audit interne au niveau local et régional*, Rapports de pratique européenne : Démocratie locale et régionale (Paris : Conseil de l'Europe, 2007), p. 41.

9 *Standard 1.3 Internal Governance Organisation of Activities* (Helsinki : Finnish Financial Supervisory Authority, 2008, section 5.6, § 100).

10 *Normes relatives à la vérification interne au sein du gouvernement du Canada* (Ottawa, Ontario : Secrétariat du Conseil du Trésor du Canada, 1er octobre 2012).

11 ISACA, Ensemble des normes, directives et procédures d'assurance et d'audit des SI à l'usage des professionnels de l'audit et du contrôle, http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Pages/Standards-for-IT-Audit-and-Assurance.aspx.

12 A. Davis, « SEC Case Claims Profit 'Management' by Grace », *The Wall Street Journal* (7 avril 1999), C1.

13 Adapté du Cas 37, « Comstock Industries », par G. Thomas Friedlob et E. Lewis Bryan, dans *Case Studies in Internal Auditing : Volume 2,* compilé par M. Dittenhofer et R. A. Roy, et publié par *l'Academic Relations Committee de l'Institute of Internal Auditors*, mars 1994.

CHAPITRE 3
La gouvernance

1 Organisation de Coopération et de Développement Économiques, Préambule aux *Principes de gouvernement d'entreprise de l'OCDE*, version révisée 2004.

2 IIA /IFACI (trad.), *Cadre de référence international des pratiques professionnelles de l'audit interne* (Paris : IFACI, 2014), p. 69.

3 U.S. Foreign Corrupt Practices Act, Section 78m.(b) (2)(a). Disponible à l'adresse http://www.usdoj.gov/criminal/fraud/fcpa/.

4 *Brief Summary of the Dodd-Frank Wall Street Reform and Consumer Protection Act* (Disponible en anglais à l'adresse http://banking.senate.gov/public/_files/070110_Dodd_Frank_Wall_Street_Reform_comprehensive_summary_Final.pdf).

Copyright © 2015 Eyrolles.

CHAPITRE 4
La gestion des risques

1 Peter L. Bernstein, *Against the Gods: The Remarkable Story of Risk* (Indianapolis, Indiana : John Wiley & Sons, 1996). *Plus fort que les dieux. La remarquable histoire du risque* (Paris : Flammarion, 1998).

2 Ibid.

3 COSO /PwC /IFACI (trad.), *Référentiel intégré de contrôle interne – Principes de mise en œuvre et de pilotage* (Paris : Eyrolles, 2014), p. 21.

4 ISO 31000:2009(F), *Management du risque – Principes et lignes directrices* (Genève : ISO, 2009), p. 1.

5 *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) / PwC/ IFACI (trad.), *Le management des risques de l'entreprise : Cadre de référence* – Techniques d'application.

6 Ibid., p. 7.

7 Ibid., p. 32.

8 Ibid., p. 40.

9 Ibid., p. 53.

10 Ibid., p. 63.

11 Ibid., p. 65.

12 Ibid, p. 66.

13 Ibid., p. 73.

14 Ibid., p. 83.

15 Ibid, p. 84.

16 Ibid., p. 93.

17 Ibid., p. 97.

18 Ibid., p. 103.

19 Ibid.

20 Ibid., p. 117.

21 Ibid., p. 131.

22 Ibid., p. 136.

23 Ibid., p. 21.

24 ISO 31000:2009(F), *Management du risque – Principes et lignes directrices*, pp. 7-8.

25 D'après ISO 31000:2009(F), *Management du risque – Principes et lignes directrices,* pp. 9-13.

26 Ibid., p. 6.

27 Ibid., pp. 13-21.

28 IIA /IFACI (trad.), *Cadre de référence international des pratiques professionnelles de l'audit interne* (Paris : IFACI, 2014), p. 50.

29 IIA /IFACI (trad.), *Le rôle de l'audit interne dans le management des risques de l'entreprise*, (Paris : IFACI, 2004).

30 Ibid.

31 Ibid.

32 Ibid.

33 Ibid.

34 IIA /IFACI (trad.), *Cadre de référence international des pratiques professionnelles de l'audit interne*, p. 166.

35 Ibid., p. 167.

36 Ibid., p. 45.

37 Ibid., p. 130.

38 *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) / PwC/ IFACI (trad.), *Le management des risques de l'entreprise : Cadre de référence – Techniques d'application*, p. 5.

Copyright © 2015 Eyrolles.

RÉFÉRENCES

CHAPITRE 5
Les processus et les risques

1 Paul Sobel, *Auditor's Risk Management Guide*, édition de 2007 (Chicago, Illinois : CCH, Inc., 2007), 7.04–7.05.

2 Ibid.

3 IIA /IFACI (trad.), *Cadre de référence international des pratiques professionnelles de l'audit interne* (Paris : IFACI, 2014), p. 45.

4 Adaptée, avec autorisation, à partir d'une méthode développée par l'*Office of the Dean of Students*, Université du Texas à Austin.

CHAPITRE 6
Le contrôle interne

1 *A Vision for the Future: Professional Practices Framework for Internal Auditing* (Altamonte Springs, Floride : The Institute of Internal Auditors, 1999), p. 54.

2 IIA /IFACI (trad.), *Cadre de référence international des pratiques professionnelles de l'audit interne* (Paris : IFACI, 2014), p. 7.

3 *U.S. Securities and Exchange Commission. Final Rules 2003 (Rule 33-823)*. Disponible à l'adresse http://www.sec.gov.

4 Ibid.

5 Ibid.

6 COSO /PwC /IFACI (trad.), *Référentiel intégré de contrôle interne – Principes de mise en œuvre et de pilotage* (Paris : Eyrolles, 2014), p. 229.

7 COSO /PwC /IFACI (trad.), *Référentiel intégré de contrôle interne – Application au reporting financier externe* (Paris : Eyrolles, 2014), p. 116.

8 COSO /PwC /IFACI (trad.), *Référentiel intégré de contrôle interne – Principes de mise en œuvre et de pilotage*, Synthèse (Paris : Eyrolles, 2014), p. 22.

9 Ibid.

10 *A Vision for the Future: Professional Practices Framework for Internal Auditing*, p. 9.

11 COSO /PwC /IFACI (trad.), *Référentiel intégré de contrôle interne – Principes de mise en œuvre et de pilotage*, p. 30.

12 Ibid.

13 Ibid.

14 Ibid., p. 31.

15 IIA /IFACI (trad.), *Cadre de référence international des pratiques professionnelles de l'audit interne*, p. 66.

Copyright © 2015 Eyrolles.

16 COSO /PwC /IFACI (trad.), *Référentiel intégré de contrôle interne – Principes de mise en œuvre et de pilotage*, p. 39.

17 Ibid., p. 31.

18 Ibid.

19 Ibid., p. 38.

20 Ibid., p. 75.

21 Ibid., p. 107.

22 Ibid., p. 141.

23 Ibid., p. 149.

24 Ibid., p. 188.

25 Ibid., p. 185.

26 Ibid., p. 60.

27 Ibid., p. 23.

28 Ibid., p. 214.

29 Ibid., p. 222.

30 Ibid.

31 Ibid., p. 221.

32 Ibid., p. 27.

33 *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) / PwC/ IFACI (trad.), *Le management des risques de l'entreprise : Cadre de référence – Techniques d'application* (Paris : Éditions d'Organisation, 2005), p. 62.

34 COSO /PwC /IFACI (trad.), *Référentiel intégré de contrôle interne – Principes de mise en œuvre et de pilotage*, p. 146.

35 *Public Company Accounting Oversight Board. Auditing and Related Professional Practice Standards: Auditing Standard No. 5: An Audit of Internal Control Over Financial Reporting That is Integrated with an Audit of Financial Statements.* 12 juin 2007, paragraphe 24.

36 COSO /PwC /IFACI (trad.), *La pratique du contrôle interne* (Paris : Éditions d'Organisation, 2004), p. 76.

37 Ibid.

38 COSO /PwC /IFACI (trad.), *Référentiel intégré de contrôle interne– Application au reporting financier externe*, p. 19.

39 Ibid., pp. 19-20.

40 Adapté du projet Snap A Control, créé par le Dr Glenn Sumners.

CHAPITRE 7
Les risques et les contrôles des systèmes d'information

1 Peter Scott and Mike Jacka, *Auditing Social Media: A Governance and Risk Guide* (Altamonte Springs, Floride : *The Institute of Internal Auditors Research Foundation*, 2011), p. 36.

2 Ibid., pp. 89-95.

3 COBIT 5.0 Executive Summary (Rolling Meadows, Illinois : ISACA, 2012), p. 13.

4 IIA /IFACI (trad.), *Cadre de référence international des pratiques professionnelles de l'audit interne* (Paris : IFACI, 2014), p. 49.

5 *Global Technology Audit Guide – Auditing IT Governance* (Altamonte Springs, Floride : The Institute of Internal Auditors, 2012), p. 15.

6 IIA /IFACI (trad.), *Cadre de référence international des pratiques professionnelles de l'audit interne*, p. 68.

Copyright © 2015 Eyrolles.

RÉFÉRENCES

7 *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) / PwC/ IFACI (trad.), *Le management des risques de l'entreprise : Cadre de référence – Techniques d'application* (Paris : Éditions d'Organisation, 2005), p. 22.

8 IIA /IFACI (trad.), *Guide pratique d'audit des technologies de l'information – Les contrôles et le risque des systèmes d'information*, 2e édition (Paris : IFACI, 2013), p. 22.

9 Ibid.

10 Ibid., p. 23.

11 Ibid., p. 24.

12 Ibid, p. 25.

13 Ibid., p. 26.

14 Ibid.

15 Ibid, p. 27.

16 Ibid.

17 Ibid.

18 Ibid., p. 24.

19 Ibid., p. 28.

20 Ibid., p. 29.

21 Ibid.

22 Ibid., p. 30.

23 Ibid.

24 IIA /IFACI (trad.), *Guide pratique d'audit des technologies de l'information – Audit continu : Répercussions sur l'assurance, le pilotage et l'évaluation des risques* (Paris : IFACI, 2005), p. 10.

25 Ibid., p. 7.

26 *The Institute of Internal Auditors*, https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides, consulté le 23 octobre 2014.

27 Ibid.

28 28.« *Le contrôle interne du système d'information des organisations – Guide opérationnel d'application du cadre de référence AMF relatif au contrôle interne* », document rédigé conjointement entre l'IFACI et le CIGREF.

CHAPITRE 8
Les risques de fraude et d'actes illégaux

1 Association of Certified Fraud Examiners, *Report to the Nation on Occupational Fraud and Abuse*, p. 4–5. ACFE, Occupation Fraud: a study of the impact of an Economic Recession, 2009 (téléchargeable en anglais sur www.acfe.com).

2 *Managing the Business Risk of Fraud: A Practical Guide*, The Institute of Internal Auditors, The American Institute of Certified Public Accountants, et the Association of Certified Fraud Examiners. Téléchargeable sur www.theiia.org, p. 5.

3 Ibid., p. 10.

4 Ibid., p. 11.

5 Ibid., p. 14.

6 Ibid., p. 26.

7 Ibid., p. 28.

8 Federico Goudie and Ana Spiguel, *Doing Business in Latin America* (Hughes Hubbard & Reed LLP, 2009), p. 26.

Copyright © 2015 Eyrolles.

9 Matthew Friedrich, Conférence de presse – Siemens AG et trois de ses filiales plaident coupable de violations du Foreign Corrupt Practices Act, décembre 2008, transcription disponible à l'adresse : http://www.justice.gov/opa/pr/2008/December/08-opa-1112.html.

10 *Doing Business in Latin America*.

11 Ibid.

12 *Managing the Business Risk of Fraud: A Practical Guide*, p. 41.

13 Ibid., p. 33.

14 Ibid., p. 39.

15 Ibid., p. 40.

16 Ibid., p. 41.

17 B. Ballou, D. L. Heitger et C. L. Landes, « The Future of Corporate Sustainability Reporting », *Journal of Accountancy* (décembre 2006).

18 I. Cohen et M. Felsen, « Social Change and Crime Rate Trends: A Routine Activity Approach », *American Sociological Review*, Vol. 44, 1979, pp. 588-608.

CHAPITRE 9
La gestion de l'audit interne

1 IIA /IFACI (trad.), *Guide pratique d'audit des technologies de l'information – Audit continu : Répercussions sur l'assurance, le pilotage et l'évaluation des risques* (Paris : IFACI, 2005), p. 7.

CHAPITRE 10
Les preuves d'audit et les papiers de travail

1 *American Institute of Certified Public Accountants, AU Section 326, Audit Evidence*. Disponible à l'adresse suivante : http://www.aicpa.org/Research/Standards/AuditAttest/Pages/SAS.aspx (consulté le 29 octobre 2014).

2 Disponible à l'adresse suivante : http://www.isaca.org/glossary (consulté le 29 octobre 2014).

3 *Global Technology Audit Guide – Data Analysis Technologies* (Altamonte Springs, Floride : The Institute of Internal Auditors, 2011), p. 14.

4 Protiviti, *Senior Audit School Participant Guide* (Protiviti, Inc., 2006).

CHAPITRE 11
L'échantillonnage en audit

1 *Audit and Accounting Guide: Audit Sampling* (New York, American Institute of Certified Public Accountants, 2008), p. 33.

2 *Audit Sampling, AU Section* 350, disponible à l'adresse : http://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AU-00350.pdf (consulté le 29 octobre 2014).

3 Protiviti, *Senior Audit School Participant Guide* (Protiviti, Inc., 2006).

Copyright © 2015 Eyrolles.

RÉFÉRENCES

4 Richard L. Ratliff et Kurt F. Reding, *Introduction to Auditing: Logic, Principles, and Techniques* (Altamonte Springs, Floride : The Institute of Internal Auditors, 2002).

CHAPITRE 12
Introduction au processus d'audit

1 D'après Richard L. Ratliff et Kurt F. Reding, *Introduction to Auditing: Logic, Principles, and Techniques* (Altamonte Springs, Floride : The Institute of Internal Auditors, 2002).

CHAPITRE 13
Le déroulement de la mission d'assurance

1 Stephen Covey, *Les sept habitudes des gens efficaces* (Montréal : Coffragants, 1989).

2 D'après Richard L. Ratliff et Kurt F. Reding, *Introduction to Auditing : Logic, Principles, and Techniques* (Altamonte Springs, Floride : The Institute of Internal Auditors, 2002).

3 D'après Protiviti, *Senior Audit School Participant Guide* (Protiviti, Inc., 2006).

4 D'après *Introduction to Auditing: Logic, Principles, and Techniques.*

CHAPITRE 14
La communication des résultats d'une mission d'assurance et les procédures de suivi

1 COSO /PwC /IFACI (trad.), *Référentiel intégré de contrôle interne – Principes de mise en œuvre et de pilotage* (Paris : Eyrolles, 2014), p. 31.

2 *Statement of Financial Accounting Standards No. 5: Accounting for Contingencies (Norwalk, Connecticut: Financial Accounting Standards Board of the Financial Accounting Foundation*, 1975), p. 4.

3 IIA /IFACI (trad.), *Guide pratique – Formuler et exprimer une opinion d'audit interne* (Paris : IFACI, 2009), p. 6.

4 *Practical Considerations Regarding Internal Auditing Expressing an Opinion on Internal Control* (Altamonte Springs, Floride : The Institute of Internal Auditors), p. 8.

5 Mark Watson, *Moody's Special Comment, Report Number : 99909* (New York, Moody's Investor Services, Inc.), p. 3.

CHAPITRE 15
La mission de conseil

1 David Richards, « Consulting Auditing – Charting a Course », *Internal Auditor*, décembre 2001, pp. 30-35.

Copyright © 2015 Eyrolles.

GLOSSAIRE



NOTE : Nombre des définitions présentes dans ce glossaire sont issues du glossaire des Normes professionnelles de l'audit interne de l'IIA, certaines ont été adaptées afin d'être harmonisées avec les descriptions du présent manuel.

Actes illégaux

Activités menées par une entité en violation des lois et règlements auxquels elle est soumise dans une juridiction donnée.

Activités d'assurance

Examen objectif d'éléments probants, effectué en vue de fournir à l'organisation une évaluation indépendante des processus de gouvernement d'entreprise, de management des risques et de contrôle. Par exemple, des audits financiers, de performance, de conformité, de sécurité des systèmes et de *due diligence*.

Activités de conseil

Conseils et services y afférents rendus au client donneur d'ordre, dont la nature et le champ sont convenus au préalable avec lui. Ces activités ont pour objectif d'améliorer les processus de gouvernement d'entreprise, de management des risques et de contrôle d'une organisation sans que l'auditeur interne n'assume aucune responsabilité de management. Quelques exemples : avis, conseil, assistance et formation.

Analyse de données

Processus d'examen, de tri, de transformation et de modélisation des données dans le but de faire ressortir les informations utiles, de faciliter les conclusions et d'accompagner la prise de décision.

Appétence pour le risque

Niveau de risque global qu'une organisation est prête à accepter en vue de la réalisation de ses objectifs. L'appétence pour le risque tient compte du niveau de risque que le management accepte consciemment après avoir évalué les coûts et les avantages des contrôles.

Approche ascendante (*Bottom-up*)

Approche qui commence par une revue de tous les processus au niveau des activités, et se poursuit par l'agrégation des processus identifiés dans l'ensemble de l'organisation.

Approche descendante (*Top-down*)

Approche qui commence au niveau de l'entité, avec les objectifs de l'organisation, et se poursuit par l'identification des principaux processus critiques pour atteindre chacun de ces objectifs.

Copyright © 2015 Eyrolles.

GLOSSAIRE

Assurance combinée

Alignement des diverses activités d'assurance au sein d'une organisation pour s'assurer qu'il n'existe aucune lacune, que la duplication et les chevauchements sont limités et que le risque reste cependant géré conformément aux attentes du Conseil et de la direction générale.

Assurance raisonnable

Niveau d'assurance étayé par des procédures et des jugements d'audit généralement acceptés. Il peut concerner l'efficacité du contrôle interne, la maîtrise des risques, la réalisation des objectifs ou d'autres conclusions relatives à la mission.

Atteintes à l'indépendance ou à l'objectivité

Survenue de menaces risquant de limiter de manière significative, dans les faits ou en apparence, la capacité de l'auditeur interne à mener une mission sans parti pris ni entrave.

Audit continu

Recours à des techniques informatisées qui permettent d'auditer en permanence le traitement des transactions d'une organisation.

Audité

Filiale, unité opérationnelle, service, groupe ou autre subdivision en place dans une organisation qui fait l'objet d'une mission d'assurance.

Auditeur externe

Cabinet d'experts-comptables agréé, chargé par le Conseil ou la direction générale de l'organisation de procéder à un audit des états financiers et de donner une assurance sous la forme d'une attestation écrite, indiquant son opinion quant à la sincérité des états financiers et à leur conformité aux principes comptables généralement admis.

Base de données

Vaste ensemble de données, habituellement stockées dans de nombreux fichiers reliés entre eux d'une manière qui permette d'y accéder, de les récupérer et de les manipuler facilement.

Big Data

Terme qui désigne le grand nombre d'informations numériques qui circulent en permanence, l'augmentation considérable des capacités de stockage de ces importants volumes de données, et la puissance de traitement des données nécessaire pour gérer, interpréter et analyser ces importants volumes d'informations numériques.

Copyright © 2015 Eyrolles.

Cadre de référence (ou référentiel)

Ensemble de principes directeurs qui forment une matrice par rapport à laquelle les organisations peuvent évaluer une multitude de pratiques. Ces principes se composent de divers concepts, valeurs, hypothèses et pratiques dont le but est de fournir un étalon à l'aune duquel une organisation peut évaluer une structure, un processus ou un environnement, ou encore un groupe de pratiques ou de procédures.

Cartographie des services donnant une assurance

Illustration des différentes fonctions et activités d'assurance au sein d'une organisation. Une telle cartographie peut permettre d'identifier les lacunes ou les chevauchements et d'évaluer si le risque est géré conformément aux attentes du Conseil et de la direction générale.

Cause

Raison de la différence entre les situations attendues et existantes.

Charte d'audit interne

Document officiel qui précise la mission, les pouvoirs et les responsabilités de cette activité. La charte doit (a) définir la position de l'audit interne dans l'organisation ; (b) autoriser l'accès aux documents, aux biens et aux personnes nécessaires à la bonne réalisation des missions ; (c) définir le champ des activités d'audit interne.

Client

Filiale, unité opérationnelle, service, groupe, personne ou autre subdivision en place dans une organisation qui fait l'objet d'une mission de conseil.

Cloud computing

Utilisation de diverses ressources informatiques – matérielles et logicielles – par le biais d'un réseau tel qu'Internet. Le *cloud* peut être configuré pour différentes options de services, ainsi que pour différentes configurations de réseau. Il permet une grande flexibilité en termes d'utilisation du matériel informatique, des logiciels et des réseaux. Le *cloud computing* donne également la possibilité de stocker des données ou d'utiliser des applications à distance.

Code de Déontologie

Le Code de Déontologie de l'Institut comprend les principes applicables à la profession et à la pratique de l'audit interne, ainsi que les règles de conduite décrivant le comportement attendu des auditeurs internes. Le Code de Déontologie s'applique à la fois aux personnes et aux organismes qui fournissent des services d'audit interne. Il a pour but de promouvoir une culture de l'éthique au sein de la profession d'audit interne.

Copyright © 2015 Eyrolles.

GLOSSAIRE

Conflit d'intérêts

Toute relation qui n'est pas ou ne semble pas être dans l'intérêt de l'organisation. Un conflit d'intérêts peut nuire à la capacité d'une personne à assumer de façon objective ses devoirs et responsabilités.

Conformité

Respect des lois et règlements applicables (définition du COSO), et adhésion aux règles, plans, procédures, contrats ou autres exigences.

Conseil

Organe de gouvernance d'une organisation. Il peut s'agir d'un Conseil d'administration, d'un Conseil de surveillance, de l'organe délibérant d'un organisme public ou d'une association ou de tout autre organe y compris le Comité d'audit auquel le responsable de l'audit interne peut être rattaché sur le plan fonctionnel.

Conséquences

Le risque ou le danger encouru par l'organisation ou d'autres, du fait que les situations diffèrent du référentiel (l'impact de la différence).

Contrôle

Toute mesure prise par le management, le Conseil et d'autres parties afin de gérer les risques et d'accroître la probabilité que les buts et objectifs fixés seront atteints. Les managers planifient, organisent et dirigent la mise en oeuvre de mesures suffisantes pour donner une assurance raisonnable que les buts et objectifs seront atteints. Voir également Contrôle interne et Système de contrôle interne.

Contrôle à l'échelle de l'entité

Contrôle au niveau de toute une entité et qui, par conséquent, n'est ni lié ni associé à un processus en particulier.

Contrôle au niveau des processus

Activité opérée au sein d'un processus spécifique dans le but d'atteindre les objectifs au niveau du processus.

Contrôle clé (ou contrôle primaire)

Activité destinée à réduire les risques associés à un objectif critique de l'organisation.

Copyright © 2015 Eyrolles.

Contrôle compensatoire

Activité qui, si les contrôles clés ne fonctionnent pas de manière effective, peut contribuer à réduire le risque considéré. Un contrôle compensatoire peut venir renforcer ou dupliquer des contrôles multiples et opère souvent sur des processus et des risques multiples. Un contrôle compensatoire ne peut pas, en tant que tel, ramener le risque à un niveau acceptable.

Contrôle conçu de manière adéquate

Caractéristique des activités de contrôle ou du système de contrôle interne permettant d'affirmer que le management les a planifiés et organisés (conçus) de manière à donner une assurance raisonnable quant à la possibilité de ramener à un niveau acceptable les risques à l'échelle de l'entité et des processus.

Contrôle détectif

Activité destinée à mettre au jour des événements non souhaitables qui sont déjà survenus. Pour être jugé efficace, un contrôle détectif doit être appliqué rapidement (avant que l'événement en question ait eu un impact négatif sur l'organisation).

Contrôle fonctionnant de manière effective

Caractéristique des activités de contrôle ou du système de contrôle interne permettant d'affirmer que le management les a exécutés (opérés) de manière à donner l'assurance raisonnable que les risques à l'échelle de l'entité et des processus sont gérés efficacement et que les buts et les objectifs de l'organisation seront atteints de manière efficiente et économique.

Contrôle interne

Processus mis en œuvre par le conseil, le management et les collaborateurs de l'entité afin d'obtenir une assurance raisonnable quant à la réalisation des objectifs suivants :

- la réalisation et l'optimisation des opérations ;
- la fiabilité du reporting financier ;
- la conformité aux lois et règlements applicables.

Contrôle préventif

Activité destinée à empêcher la survenance d'événements non souhaités.

Contrôle secondaire

Activité destinée soit à réduire les risques associés aux objectifs de l'organisation qui ne sont pas critiques pour la survie ou pour la réussite de l'organisation, soit à appuyer un contrôle clé.

Copyright © 2015 Eyrolles.

GLOSSAIRE

Contrôles généraux des systèmes d'information

Contrôles au niveau de tous les SI mis en place pour veiller à l'intégrité, à la fiabilité et à la précision des systèmes applicatifs. Ils constituent également un exemple de contrôle à l'échelle de l'entité.

Corruption

Acte par lequel une personne exerce une influence indue lors d'une transaction commerciale, afin d'en tirer un avantage pour elle-même ou pour un tiers (par exemple, pots-de-vin, délits d'initié ou conflits d'intérêts), en violation de ses obligations vis-à-vis de son employeur ou des droits d'un tiers.

Détournement d'actifs

Acte consistant à voler ou à utiliser à mauvais escient les actifs d'une organisation (par exemple, écrémage des recettes, vols dans les stocks, dépenses de personnel fictives).

Échantillonnage à l'aveuglette

Technique de sondage non statistique utilisée pour sélectionner un échantillon qui doit être représentatif de la population, sans choisir délibérément d'inclure ou d'exclure tel élément.

Échantillonnage aléatoire

Prélèvement d'un échantillon tel que tous les éléments de la population ont une probabilité de sélection égale.

Échantillonnage d'attributs

Méthode d'échantillonnage statistique reposant sur la loi binomiale (loi de Bernoulli), qui permet d'aboutir à une conclusion grâce au calcul d'un taux d'occurrence dans une population.

Échantillonnage de variables classique

Méthode d'échantillonnage statistique qui s'appuie sur la distribution de Gauss (aussi appelée distribution normale). Elle est utilisée pour obtenir des conclusions concernant des valeurs monétaires.

Échantillonnage en audit

Application d'une procédure d'audit à moins de 100 % des éléments d'une population afin d'en tirer une conclusion pour l'ensemble de la population.

Échantillonnage par unités monétaires (EUM)

Variante de l'échantillonnage d'attributs utilisée pour obtenir des conclusions concernant des valeurs monétaires plutôt que des taux d'occurrence.

Copyright © 2015 Eyrolles.

Environnement de contrôle

Attitude et actions du Conseil et du management au regard de l'importance du (dispositif de) contrôle dans l'organisation. L'environnement de contrôle constitue le cadre et la structure nécessaires à la réalisation des objectifs primordiaux du système de contrôle interne. L'environnement de contrôle englobe les éléments suivants :

- intégrité et valeurs éthiques ;
- philosophie et style de direction ;
- structure organisationnelle ;
- attribution des pouvoirs et responsabilités ;
- politiques et pratiques relatives aux ressources humaines ;
- compétence du personnel.

Évaluation des risques

Identification et analyse (généralement en termes d'impact et de probabilité d'occurrence) des risques susceptibles d'affecter la réalisation des objectifs d'une organisation, de façon à déterminer comment ces risques doivent être gérés.

Exemplarité au plus haut niveau

Les cadres supérieurs d'une organisation font preuve d'exemplarité de par leur intégrité et leur sensibilisation au contrôle dans l'ensemble d'une organisation. Voir également Environnement de contrôle.

Exploitation informatique

Service ou secteur au sein d'une organisation (personnes, processus et matériel) assurant le fonctionnement des systèmes informatiques et des différents appareils qui permettent la réalisation des objectifs et des activités de l'organisation.

Externalisation de processus opérationnels

Transfert d'une partie des processus opérationnels d'une organisation à un prestataire extérieur, afin de réduire les coûts et d'accroître l'efficacité ou l'efficience de l'exploitation, tout en améliorant la qualité du service.

Faits

Preuves factuelles identifiées par l'auditeur interne au cours de son examen (la situation actuelle).

Copyright © 2015 Eyrolles.

GLOSSAIRE

Fonction d'audit interne

Assurée par un service, une division, une équipe de consultants ou tout autre praticien, c'est une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée.

Fraude

Tout acte illégal caractérisé par la tromperie, la dissimulation ou la violation de la confiance sans qu'il y ait eu violence ou menace de violence. Les fraudes sont perpétrées par des personnes et des organisations afin d'obtenir de l'argent, des biens ou des services, ou de s'assurer un avantage personnel ou commercial.

Gestion des risques

Processus piloté par le management qui consiste à appréhender et à traiter les incertitudes (risques et opportunités) susceptibles d'affecter la capacité de l'organisation à atteindre ses objectifs.

Gouvernance (ou gouvernement d'entreprise)

Dispositif comprenant les processus et les structures mis en place par le Conseil afin d'informer, de diriger, de gérer et de piloter les activités de l'organisation en vue de réaliser ses objectifs.

Gouvernance des systèmes d'information

Englobe les dirigeants ainsi que les structures et processus organisationnels qui veillent à ce que les systèmes d'information permettent la réalisation des stratégies et des objectifs de l'organisation.

Indépendance

Capacité de l'audit interne à n'être exposé à aucune situation susceptible d'altérer, en réalité ou en apparence, l'objectivité. Les atteintes à l'indépendance doivent être appréhendées à différents niveaux :

- au niveau de l'auditeur interne ;
- au niveau de la conduite de la mission ;
- au niveau de l'audit interne et de son positionnement dans l'organisation. Voir également Indépendance dans l'organisation.

Indépendance organisationnelle

Caractéristique du niveau hiérarchique dont relève le responsable de l'audit interne au sein de l'organisation, et qui permet au service d'audit interne d'exercer ses responsabilités sans subir la moindre ingérence. Voir également Indépendance.

Copyright © 2015 Eyrolles.

Indicateur clé de performance

Donnée chiffrée ou toute autre forme de mesure permettant de déterminer si un processus ou une tâche donnés respectent les seuils de tolérance fixés.

Limites inhérentes au contrôle interne

Limitations qui concernent les limites inhérentes au jugement humain, les contraintes en matière de ressources, la nécessité d'étudier le ratio coût/bénéfice des contrôles, le fait que des dysfonctionnements soient plausibles, et l'éventualité d'un contournement des contrôles par le management ou d'une collusion.

Maîtrise des risques

Mesure ou ensemble de mesures prises par le management pour ramener l'impact et/ou la probabilité d'occurrence d'un risque à un niveau plus bas et donc plus acceptable.

Management des risques de l'entreprise (ERM – Entreprise Risk Management)

Voir Gestion des risques.

Mission

Une mission ou un projet d'audit interne particulier qui englobe de multiples tâches ou activités menées pour atteindre un ensemble déterminé d'objectifs qui s'y rapportent. Voir également Activités d'assurance et Activités de conseil.

Mission d'audit

Voir Activités d'assurance.

Norme

Document d'ordre professionnel promulgué par « *the International Internal Auditing Standards Board* » (Comité interne à l'IIA chargé d'élaborer les *Normes*) afin de définir les règles applicables à un large éventail d'activités d'audit interne et utilisables pour l'évaluation de ses performances.

Objectifs

Ce qu'une organisation souhaite réaliser. On parle alors des objectifs de l'organisation. Ces objectifs peuvent être liés à la stratégie, aux opérations, au reporting et à la conformité. Lorsque l'on désigne ce que l'audit souhaite réaliser, on parle des objectifs de l'audit ou des objectifs de la mission.

Copyright © 2015 Eyrolles.

GLOSSAIRE

Objectifs stratégiques

Ce qu'une organisation souhaite réaliser via les décisions de création de valeur prises par le management pour le compte des parties prenantes de l'organisation.

Objectivité

Voir Objectivité individuelle.

Objectivité individuelle

Attitude impartiale qui permet aux auditeurs internes d'accomplir leurs missions de telle sorte qu'ils soient certains de la qualité de leurs travaux menés sans le moindre compromis. L'objectivité implique que les auditeurs internes ne subordonnent pas leur propre jugement à celui d'autres personnes.

Observation

Conclusion, déduction ou jugement découlant des résultats de tests effectués par l'auditeur interne dans le cadre d'une mission d'assurance ou de conseil. Également appelé constat ou constatation.

Observation critique

Une ou plusieurs observations sont jugées critiques si l'activité de contrôle en question présente une probabilité de défaillance raisonnable et que cette éventuelle défaillance aurait non seulement un impact significatif, mais dépasserait aussi le seuil d'importance relative des états financiers.

Observation d'audit

Toute différence identifiée et validée, dans le cadre d'une mission d'assurance, entre l'état actuel et l'état souhaité.

Observation significative

Une ou plusieurs observations sont jugées significatives si l'activité de contrôle en question présente une probabilité de défaillance raisonnable ou si cette éventuelle défaillance aurait un impact significatif.

Opportunité

Événement susceptible d'avoir un impact positif sur la réalisation des objectifs.

Pilotage

Processus qui évalue la mise en place et le fonctionnement de la gouvernance, de la gestion des risques et des contrôles au fil du temps.

Copyright © 2015 Eyrolles.

Point de vue

Le produit final (ou résultat) des missions d'assurance et de conseil réalisées par la fonction d'audit interne, destiné à apporter des informations et des éclairages précieux à l'audité ou au client. Il peut s'agir par exemple : d'identifier l'origine, à l'échelle de l'entité, de déficiences du contrôle interne ; d'identifier des risques émergents ; de formuler des suggestions pour améliorer le processus de gouvernance de l'organisation.

Politique « Apportez vos outils personnels » (*Bring Your Own Device*, BYOD)

Politique par laquelle une organisation autorise ses collaborateurs à accéder à leur messagerie électronique professionnelle, à leur agenda et à d'autres données via leur ordinateur personnel, leur smartphone, leur tablette ou d'autres appareils.

Prestataire externe

Personne physique ou morale extérieure à l'organisation, qui mène des activités d'assurance et/ou de conseil pour cette dernière.

Preuve suffisante

Toute preuve ou ensemble de preuves collectées durant une mission qui justifie de manière pertinente et fiable les jugements et conclusions de celle-ci.

Preuves adéquates

Tout élément de preuve ou ensemble de preuves recueilli au cours d'une mission, qui étaye d'une manière pertinente et fiable les jugements et conclusions formulés pendant cette mission.

Processus opérationnel

Ensemble d'activités reliées entre elles qui ont pour but d'atteindre un ou plusieurs objectifs.

Programme de travail de la mission

Document énumérant les procédures à mettre en œuvre, conçu pour réaliser le plan de mission.

Référentiels

Normes, mesures ou exigences requises, utilisées pour évaluer ou vérifier une observation (ce qui devrait être).

Reporting financier frauduleux

Actes comprenant la falsification des états financiers d'une organisation (par exemple, une surestimation du chiffre d'affaires ou une sous-estimation du passif et des charges).

Copyright © 2015 Eyrolles.

GLOSSAIRE

Réseau

Configuration qui permet aux ordinateurs et aux périphériques de communiquer et d'être reliés aux fins du transfert des données et des opérations.

Responsable de l'audit interne

Désigne une personne, occupant un poste hiérarchique de haut niveau, qui a la responsabilité de gérer l'activité d'audit interne. Dans le cas où les activités d'audit interne sont confiées à des prestataires de services extérieurs, le responsable de l'audit interne est la personne chargée de surveiller l'exécution du contrat de services et l'assurance de la qualité d'ensemble de ces activités, et qui rend compte à la direction générale et au Conseil. Ce terme recouvre également des titres tels qu'auditeur général, chef de l'audit interne, directeur de l'audit interne ou inspecteur général.

Risque

Possibilité qu'un événement survienne et ait un impact défavorable sur la réalisation des objectifs.

Risque d'audit

Risque d'aboutir à une conclusion d'audit non valide et/ou d'apporter un conseil inadéquat sur la base des travaux d'audit menés.

Risque d'échantillonnage

Risque que les conclusions que l'auditeur interne tire du test d'un échantillon diffèrent de celles qu'il aurait tirées si la procédure d'audit avait été appliquée à la totalité de la population. Également appelé risque aléatoire.

Risque de non-contrôle

Possibilité que les activités de contrôle ne permettent pas de ramener le risque maîtrisable à un niveau acceptable.

Risque discrétionnaire

Risque qui survient du fait d'une mauvaise sélection, application ou interprétation d'une procédure d'audit de la part de l'auditeur interne.

Risque inhérent

Combinaison de facteurs de risque internes et externes à leur état d'origine, en l'absence de contrôle, ou risque brut s'il n'existe aucun dispositif de contrôle interne.

Copyright © 2015 Eyrolles.

Risque maîtrisable

Part du risque inhérent que le management peut réduire via des opérations et des activités de gestion quotidiennes.

Risque résiduel

Part du risque inhérent qui subsiste après prise en compte des modalités de traitement des risques mises en œuvre par le management (on parle parfois de risque net).

Scepticisme professionnel

État d'esprit consistant à ne rien tenir pour acquis. Les auditeurs internes remettent constamment en question ce qu'ils entendent et voient, et portent un regard critique sur les preuves d'audit.

Stratégie

Manière dont la direction générale prévoit de réaliser les objectifs de l'organisation.

Stratégie de niveaux d'assurance

Technique consistant à coordonner de multiples activités d'assurance, conçue pour maîtriser un risque donné en le ramenant à un niveau requis ou souhaité, dans le respect d'un certain seuil de tolérance au risque.

Système de contrôle interne

Système englobant les cinq composantes du contrôle interne – à savoir l'environnement de contrôle, l'évaluation des risques, les activités de contrôle, l'information/la communication et le pilotage – mises en place pour gérer les risques associés aux objectifs de l'organisation liés au reporting financier, à la conformité et aux opérations. Voir également Contrôle interne.

Systèmes d'application (ou systèmes applicatifs)

Ensembles de programmes conçus pour les utilisateurs finaux, tels que la gestion de la paie, les créances clients et, dans certains cas, applications plus larges comme les progiciels de gestion intégrés (PGI) qui assurent de nombreuses fonctions.

Systèmes d'exploitation

Programmes logiciels qui font fonctionner l'ordinateur et exécutent des tâches élémentaires, comme la reconnaissance des éléments saisis sur le clavier, l'envoi des données de sortie vers l'imprimante, la sauvegarde des fichiers et répertoires et le contrôle de divers périphériques.

Copyright © 2015 Eyrolles.

GLOSSAIRE

Techniques d'audit informatisées

Techniques d'audit assistées par ordinateur, comme les logiciels d'audit généralisés, les logiciels utilitaires, les données de test, les outils de traçage logique et de cartographie de logiciels d'application, et les systèmes experts d'audit, qui aident l'auditeur interne à tester directement les contrôles intégrés dans les systèmes d'information informatisés et les données contenues dans les fichiers informatiques.

Tolérance au risque

Niveau de risque et d'écart acceptable entre les objectifs et la performance réelle ; elle doit être en adéquation avec l'appétence pour le risque de l'organisation.

Traitement des risques

Mesure ou ensemble de mesures prises par le management pour déployer la stratégie de gestion des risques définie. Le traitement des risques consiste à éviter, réduire, partager ou accepter les risques. L'exploitation d'opportunités qui, à leur tour, permettent la réalisation des objectifs est également une réponse aux risques. Dans la norme ISO 31000, cette étape de la gestion des risques se nomme le traitement des risques.

Transparence

Fait de communiquer d'une manière considérée par une personne prudente comme juste, suffisamment claire et complète pour répondre aux besoins de l'interlocuteur.

Trois lignes de maîtrise

Modèle d'assurance dans lequel la première ligne de maîtrise en matière de gestion des risques correspond aux contrôles effectués par le management, la deuxième aux diverses fonctions de contrôle des risques et de conformité mises en place par le management, et la troisième à l'obtention d'une assurance indépendante.

Univers d'audit

Ensemble des filiales, unités opérationnelles, services, groupes, processus ou autres subdivisions en place dans une organisation qui gèrent un ou plusieurs risques opérationnels.

Valeur ajoutée

Les activités d'assurance comme les activités de conseil apportent de la valeur ajoutée en contribuant à améliorer les opportunités de réaliser les objectifs de l'organisation, en identifiant les améliorations possibles sur le plan opérationnel, et/ou en réduisant l'exposition aux risques.

Copyright © 2015 Eyrolles.

ANNEXE A
CODE DE DÉONTOLOGIE DE L'*INSTITUTE OF INTERNAL AUDITORS*

Le Code de Déontologie de l'Institut a pour but de promouvoir une culture de l'éthique au sein de la profession d'audit interne.

> *L'audit interne est une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée. Il aide cette organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle, et de gouvernement d'entreprise, et en faisant des propositions pour renforcer leur efficacité.*

Compte tenu de la confiance placée en l'audit interne pour donner une assurance objective sur les processus de gouvernement d'entreprise, de management des risques, et de contrôle, il était nécessaire que la profession se dote d'un tel code.

Le Code de Déontologie va au-delà de la définition de l'audit interne et inclut deux composantes essentielles :

- des principes fondamentaux pertinents pour la profession et pour la pratique de l'audit interne ;
- des règles de conduite décrivant les normes de comportement attendues des auditeurs internes. Ces règles sont une aide à la mise en œuvre pratique des principes fondamentaux et ont pour but de guider la conduite éthique des auditeurs internes.

On désigne par « auditeurs internes » les membres de l'Institut, les titulaires de certifications professionnelles de l'IIA ou les candidats à celles-ci, ainsi que les personnes proposant des services entrant dans le cadre de la définition de l'audit interne.

Champ d'application et caractère obligatoire du Code de Déontologie

Le Code de Déontologie s'applique aux personnes et aux entités qui fournissent des services d'audit interne.

Toute violation du Code de Déontologie par des membres de l'IIA, des titulaires de certifications professionnelles de l'IIA ou des candidats à celles-ci, fera l'objet d'une évaluation et sera traitée en accord avec les statuts de l'Institut et ses directives administratives. Le fait qu'un comportement donné ne figure pas dans les règles de conduite ne l'empêche pas d'être inacceptable ou déshonorant et peut donc entraîner une action disciplinaire à l'encontre de la personne qui s'en est rendue coupable.

Copyright © 2015 Eyrolles.

ANNEXES

Principes fondamentaux

Il est attendu des auditeurs internes qu'ils respectent et appliquent les principes fondamentaux suivants :

- **Intégrité**

  L'intégrité des auditeurs internes est à la base de la confiance et de la crédibilité accordées à leur jugement.

- **Objectivité**

  Les auditeurs internes montrent le plus haut degré d'objectivité professionnelle en collectant, évaluant et communiquant les informations relatives à l'activité ou au processus examiné. Les auditeurs internes évaluent de manière équitable tous les éléments pertinents et ne se laissent pas influencer dans leur jugement par leurs propres intérêts ou par autrui.

- **Confidentialité**

  Les auditeurs internes respectent la valeur et la propriété des informations qu'ils reçoivent ; ils ne divulguent ces informations qu'avec les autorisations requises, à moins qu'une obligation légale ou professionnelle ne les oblige à le faire.

- **Compétence**

  Les auditeurs internes utilisent et appliquent les connaissances, les savoir-faire et expériences requis pour la réalisation de leurs travaux.

Règles de conduite

- **Intégrité**

  Les auditeurs internes :

  - Doivent accomplir leur mission avec honnêteté, diligence et responsabilité.
  - Doivent respecter la loi et faire les révélations requises par les lois et les règles de la profession.
  - Ne doivent pas sciemment prendre part à des activités illégales ou s'engager dans des actes déshonorants pour la profession d'audit interne ou leur organisation.
  - Doivent respecter et contribuer aux objectifs éthiques et légitimes de leur organisation.

- **Objectivité**

  Les auditeurs internes :

  - Ne doivent pas prendre part à des activités ou établir des relations qui pourraient compromettre ou risquer de compromettre le caractère impartial de leur jugement. Ce principe vaut également pour les activités ou relations d'affaires qui pourraient entrer en conflit avec les intérêts de leur organisation.

Copyright © 2015 Eyrolles.

- Ne doivent rien accepter qui pourrait compromettre ou risquer de compromettre leur jugement professionnel.
- Doivent révéler tous les faits matériels dont ils ont connaissance et qui, s'ils n'étaient pas révélés, auraient pour conséquence de fausser le rapport sur les activités examinées.

- **Confidentialité**

  Les auditeurs internes :

  - Doivent utiliser avec prudence et protéger les informations recueillies dans le cadre de leurs activités.
  - Ne doivent pas utiliser ces informations pour en retirer un bénéfice personnel, ou d'une manière qui contreviendrait aux dispositions légales ou porterait préjudice aux objectifs éthiques et légitimes de leur organisation.

- **Compétence**

  Les auditeurs internes :

  - Ne doivent s'engager que dans des travaux pour lesquels ils ont les connaissances, le savoir-faire et l'expérience nécessaires.
  - Doivent réaliser leurs travaux d'audit interne dans le respect des *Normes Internationales pour la Pratique Professionnelle de l'Audit Interne*.
  - Doivent toujours s'efforcer d'améliorer leur compétence, l'efficacité et la qualité de leurs travaux.

ANNEXE B
NORMES INTERNATIONALES POUR LA PRATIQUE PROFESSIONNELLE DE L'AUDIT INTERNE

Normes de qualification

1000 – Mission, pouvoirs et responsabilités

La mission, les pouvoirs et les responsabilités de l'audit interne doivent être formellement définis dans une charte d'audit interne, être cohérents avec la définition de l'audit interne, le Code de Déontologie ainsi qu'avec les *Normes*. Le responsable de l'audit interne doit revoir périodiquement la charte d'audit interne et la soumettre à l'approbation de la direction générale et du Conseil.

Interprétation

La charte d'audit interne est un document officiel qui précise la mission, les pouvoirs et les responsabilités de cette activité. La charte définit la position de l'audit interne dans l'organisation y compris la nature de la relation fonctionnelle entre le responsable de l'audit interne

Copyright © 2015 Eyrolles.

et le Conseil ; autorise l'accès aux documents, aux personnes et aux biens, nécessaires à la réalisation des missions ; définit le champ des activités d'audit interne. L'approbation finale de la charte d'audit interne relève de la responsabilité du Conseil.

1000.A1 – La nature des missions d'assurance réalisées pour l'organisation doit être définie dans la charte d'audit interne. S'il est prévu d'effectuer des missions d'assurance à l'extérieur de l'organisation, leur nature doit être également définie dans la charte d'audit interne.

1000.C1 – La nature des missions de conseil doit être définie dans la charte d'audit interne.

1010 – Reconnaissance de la définition de l'audit interne, du Code de Déontologie ainsi que des *Normes* dans la charte d'audit interne

Le caractère obligatoire de la définition de l'audit interne, du Code de Déontologie ainsi que des *Normes* doit être reconnu dans la charte d'audit interne. Le responsable de l'audit interne présente la définition de l'audit interne, le Code de Déontologie ainsi que les *Normes* à la direction générale et au Conseil.

1100 – Indépendance et objectivité

L'audit interne doit être indépendant et les auditeurs internes doivent effectuer leurs travaux avec objectivité.

Interprétation

L'indépendance c'est la capacité de l'audit interne à assumer, de manière impartiale, ses responsabilités. Afin d'atteindre un degré d'indépendance nécessaire et suffisant à l'exercice de ses responsabilités, le responsable de l'audit interne doit avoir un accès direct et non restreint à la direction générale et au Conseil. Cet objectif peut être atteint grâce à un double rattachement. Les atteintes à l'indépendance doivent être appréhendées à différents niveaux :

- au niveau de l'auditeur interne ;
- au niveau de la conduite de la mission ;
- au niveau de l'audit interne et de son positionnement dans l'organisation.

L'objectivité est une attitude impartiale qui permet aux auditeurs internes d'accomplir leurs missions de telle sorte qu'ils soient certains de la qualité de leurs travaux menés sans le moindre compromis. L'objectivité implique que les auditeurs internes ne subordonnent pas leur propre jugement à celui d'autres personnes. Comme pour l'indépendance, les atteintes à l'objectivité doivent être appréhendées au niveau de :

- l'auditeur interne ;
- la conduite de la mission ;
- l'audit interne et de son positionnement dans l'organisation.

Copyright © 2015 Eyrolles.

1110 – Indépendance dans l'organisation

Le responsable de l'audit interne doit relever d'un niveau hiérarchique suffisant au sein de l'organisation pour permettre au service d'audit interne d'exercer ses responsabilités. Le responsable de l'audit interne doit confirmer au Conseil, au moins annuellement, l'indépendance de l'audit interne au sein de l'organisation.

Interprétation

- *L'indépendance au sein de l'organisation est atteinte lorsque le responsable de l'audit interne rapporte fonctionnellement au Conseil. Les relations fonctionnelles impliquent, par exemple, que le Conseil :*
  - *approuve la charte d'audit interne ;*
  - *approuve le plan d'audit interne fondé sur l'approche par les risques ;*
  - *approuve le budget et les ressources prévisionnels de l'audit interne ;*
  - *soit destinataire des informations adressées par le responsable d'audit relatives à la réalisation du plan d'audit ou de tout autre sujet afférent à l'audit interne ;*
  - *approuve les décisions liées à la nomination et à la révocation du responsable de l'audit interne ;*
  - *approuve la rémunération du responsable de l'audit interne ;*
  - *demande des informations pertinentes au management et au responsable de l'audit interne pour déterminer l'adéquation du périmètre et des ressources de l'audit interne.*

1110.A1 – L'audit interne ne doit subir aucune ingérence lors de la définition de son champ d'intervention, de la réalisation du travail et de la communication des résultats.

1111 – Relation directe avec le Conseil

Le responsable de l'audit interne doit pouvoir communiquer et dialoguer directement avec le Conseil.

1120 – Objectivité individuelle

Les auditeurs internes doivent avoir une attitude impartiale et dépourvue de préjugés, et éviter tout conflit d'intérêt.

Interprétation

Est considérée comme un conflit d'intérêt, une situation dans laquelle un auditeur interne, qui jouit d'une position de confiance, a un intérêt personnel ou professionnel venant en concurrence avec ses devoirs et responsabilités. De tels intérêts peuvent empêcher l'auditeur d'exercer ses responsabilités de façon impartiale. Un conflit d'intérêt peut exister même si aucun acte contraire à l'éthique ou malhonnête n'a été commis. Un conflit d'intérêt peut créer une situation susceptible d'entamer la confiance en l'auditeur interne, vis-à-vis du service

Copyright © 2015 Eyrolles.

d'audit interne et en la profession. Un conflit d'intérêt peut compromettre la capacité d'un individu à conduire ses activités et exercer ses responsabilités de manière objective.

1130 – Atteinte à l'indépendance ou à l'objectivité

Si l'indépendance ou l'objectivité des auditeurs internes sont compromises dans les faits ou même en apparence, les parties concernées doivent en être informées de manière précise. La forme de cette communication dépendra de la nature de l'atteinte à l'indépendance.

Interprétation

Parmi les atteintes à l'indépendance du service d'audit interne et à l'objectivité individuelle, peuvent figurer les conflits d'intérêts personnels, les limitations du champ d'un audit, les restrictions d'accès aux dossiers, aux personnes et aux biens, ainsi que les limitations de ressources telles que des limitations financières.

L'identification des parties qui devraient être informées d'une atteinte à l'objectivité et à l'indépendance dépend d'une part des attentes de la direction générale et du Conseil, telles que décrites dans la charte d'audit interne, en termes de responsabilités de l'audit interne et du responsable d'audit interne, et d'autre part de la nature de cette atteinte.

1130.A1 – Les auditeurs internes doivent s'abstenir d'auditer des opérations particulières dont ils étaient auparavant responsables. L'objectivité d'un auditeur interne est présumée altérée lorsqu'il réalise une mission d'assurance pour une activité dont il a eu la responsabilité au cours de l'année précédente.

1130.A2 – Les missions d'assurance concernant des fonctions dont le responsable de l'audit a la charge doivent être supervisées par une personne ne relevant pas de l'audit interne.

1130.C1 – Les auditeurs internes peuvent être amenés à réaliser des missions de conseil liées à des opérations dont ils ont été auparavant responsables.

1130.C2 – Si l'indépendance ou l'objectivité des auditeurs internes sont susceptibles d'être compromises lors des missions de conseil qui leur sont proposées, ils doivent en informer le client donneur d'ordre avant de les accepter.

1200 – Compétence et conscience professionnelle

Les missions doivent être conduites avec compétence et conscience professionnelle.

1210 – Compétence

Les auditeurs internes doivent posséder les connaissances, le savoir-faire et les autres compétences nécessaires à l'exercice de leurs responsabilités individuelles. L'équipe d'audit interne doit collectivement posséder ou acquérir les connaissances, le savoir-faire et les autres compétences nécessaires à l'exercice de ses responsabilités.

Copyright © 2015 Eyrolles.

Interprétation

Les connaissances, le savoir-faire et les autres compétences sont une expression générique utilisée pour décrire la capacité professionnelle dont les auditeurs internes doivent disposer pour pouvoir exercer efficacement leurs responsabilités professionnelles. Les auditeurs internes sont encouragés à démontrer leurs compétences en obtenant des certifications et qualifications professionnelles appropriées telles que le CIA (Certified Internal Auditor) *et tout autre diplôme promu par l'IIA ou par d'autres organisations professionnelles appropriées.*

1210.A1 – Le responsable de l'audit interne doit obtenir l'avis et l'assistance de personnes qualifiées si les auditeurs internes ne possèdent pas les connaissances, le savoir-faire et les autres compétences nécessaires pour s'acquitter de tout ou partie de leur mission.

1210.A2 – Les auditeurs internes doivent posséder des connaissances suffisantes pour évaluer le risque de fraude et la façon dont ce risque est géré par l'organisation. Toutefois, ils ne sont pas censés posséder l'expertise d'une personne dont la responsabilité première est la détection et l'investigation des fraudes.

1210.A3 – Les auditeurs internes doivent posséder une connaissance suffisante des principaux risques et contrôles relatifs aux technologies de l'information, et des techniques d'audit informatisées susceptibles d'être mises en œuvre dans le cadre des travaux qui leur sont confiés. Toutefois, tous les auditeurs internes ne sont pas censés posséder l'expertise d'un auditeur dont la responsabilité première est l'audit informatique.

1210.C1 – Le responsable de l'audit interne doit décliner une mission de conseil ou obtenir l'avis et l'assistance de personnes qualifiées si les auditeurs internes ne possèdent pas les connaissances, le savoir-faire et les autres compétences nécessaires pour s'acquitter de tout ou partie de la mission.

1220 – Conscience professionnelle

Les auditeurs internes doivent apporter à leur travail la diligence et le savoir-faire que l'on peut attendre d'un auditeur interne raisonnablement averti et compétent. La conscience professionnelle n'implique pas l'infaillibilité.

1220.A1 – Les auditeurs internes doivent apporter tout le soin nécessaire à leur pratique professionnelle en prenant en considération les éléments suivants :

- l'étendue du travail nécessaire pour atteindre les objectifs de la mission ;
- la complexité relative, la matérialité ou le caractère significatif des domaines auxquels sont appliquées les procédures propres aux missions d'assurance ;
- l'adéquation et l'efficacité des processus de gouvernement d'entreprise, de management des risques et de contrôle ;
- la probabilité d'erreurs significatives, de fraudes ou de non-conformité ;
- le coût de la mise en place des contrôles par rapport aux avantages escomptés.

Copyright © 2015 Eyrolles.

1220.A2 – Pour remplir ses fonctions avec conscience professionnelle, l'auditeur interne doit envisager l'utilisation de techniques informatiques d'audit et d'analyse des données.

1220.A3 – Les auditeurs internes doivent exercer une vigilance particulière à l'égard des risques significatifs susceptibles d'affecter les objectifs, les opérations ou les ressources. Toutefois, les procédures d'audit seules, même lorsqu'elles sont menées avec la conscience professionnelle requise, ne garantissent pas que tous les risques significatifs seront détectés.

1220.C1 – Les auditeurs internes doivent apporter à une mission de conseil toute leur conscience professionnelle, en prenant en considération les éléments suivants :

- les besoins et attentes des clients, y compris sur la nature, le calendrier et la communication des résultats de la mission ;
- la complexité de celle-ci et l'étendue du travail nécessaire pour atteindre les objectifs fixés ;
- son coût par rapport aux avantages escomptés.

1230 – Formation professionnelle continue

Les auditeurs internes doivent améliorer leurs connaissances, savoir-faire et autres compétences par une formation professionnelle continue.

1300 – Programme d'assurance et d'amélioration qualité

Le responsable de l'audit interne doit élaborer et tenir à jour un programme d'assurance et d'amélioration qualité portant sur tous les aspects de l'audit interne.

Interprétation

Un programme d'assurance et d'amélioration qualité est conçu de façon à évaluer : la conformité de l'audit interne avec la définition de l'audit interne et les Normes *; le respect du Code de Déontologie par les auditeurs internes. Ce programme permet également de s'assurer de l'efficacité et de l'efficience de l'activité d'audit interne et d'identifier toutes opportunités d'amélioration.*

1310 – Exigences du programme d'assurance et d'amélioration qualité

Le programme d'assurance et d'amélioration qualité doit comporter des évaluations tant internes qu'externes.

1311 – Évaluations internes

Les évaluations internes doivent comporter :

- une surveillance continue de la performance de l'audit interne ;
- des évaluations périodiques, effectuées par auto-évaluation ou par d'autres personnes de l'organisation possédant une connaissance suffisante des pratiques d'audit interne.

Copyright © 2015 Eyrolles.

Interprétation

La surveillance continue fait partie intégrante de la supervision quotidienne, de la revue et du suivi de l'activité d'audit interne. La surveillance continue est intégrée dans les procédures et les pratiques courantes de gestion du service d'audit interne. Ce contrôle utilise les processus, les outils et les informations nécessaires à l'évaluation du service d'audit interne en termes de conformité à la définition de l'audit interne, au Code de Déontologie et aux Normes.

Les évaluations périodiques sont conduites pour apprécier également la conformité du service d'audit interne à la définition de l'audit interne, au Code de Déontologie et aux Normes.

Une connaissance suffisante des pratiques d'audit interne suppose au moins la compréhension de l'ensemble des éléments du Cadre de référence international des pratiques professionnelles.

1312 – Évaluations externes

Des évaluations externes doivent être réalisées au moins tous les cinq ans par un évaluateur ou une équipe d'évaluateurs qualifiés, indépendants et extérieurs à l'organisation. Le responsable de l'audit interne doit s'entretenir avec le Conseil au sujet :

- des modalités et de la fréquence de l'évaluation externe ; et
- des qualifications de l'évaluateur ou de l'équipe d'évaluation externes ainsi que de leur indépendance y compris au regard de tout conflit d'intérêt potentiel.

Interprétation

Les évaluations externes peuvent prendre la forme d'une évaluation entièrement externalisée ou d'une auto-évaluation avec validation indépendante externe.

Un évaluateur ou une équipe d'évaluateurs qualifiés possèdent des compétences dans deux domaines : la pratique professionnelle de l'audit interne et le processus d'évaluation externe. Ces compétences peuvent être démontrées à travers une combinaison d'expériences professionnelles et de connaissances théoriques. L'expérience acquise dans des organisations de taille, de complexité, de secteur d'activité ou d'industrie, et de problématiques techniques similaires est à privilégier. Dans le cadre d'une équipe d'évaluation, il n'est pas nécessaire que chaque membre de l'équipe possède toutes les compétences requises ; c'est l'équipe dans son ensemble qui est qualifiée. Le responsable de l'audit interne doit se servir de son jugement professionnel pour apprécier si un évaluateur ou une équipe d'évaluation possède suffisamment de compétences pour pouvoir mener à bien la mission d'évaluation.

La personne ou l'équipe qui procèdent à l'évaluation doivent être indépendantes de l'organisation dont le service d'audit interne fait partie et ne pas se trouver en situation de conflit d'intérêt réel ou apparent.

Copyright © 2015 Eyrolles.

1320 – Rapports relatifs au programme d'assurance et d'amélioration qualité

Le responsable de l'audit interne doit communiquer les résultats du programme d'assurance et d'amélioration qualité à la direction générale ainsi qu'au Conseil.

Interprétation

La forme, le contenu ainsi que la fréquence des communications relatives aux résultats du programme d'assurance et d'amélioration qualité sont définis lors de discussions avec la direction générale et le Conseil, et tiennent compte des responsabilités de l'audit interne et de celles du responsable de l'audit interne comme définies dans la charte d'audit interne. Pour démontrer la conformité à la définition de l'audit interne, au Code de Déontologie et aux Normes*, les résultats des évaluations internes périodiques et des évaluations externes doivent être communiqués dès l'achèvement de ces évaluations. Les résultats de la surveillance continue sont quant à eux communiqués au moins une fois par an. Ces résultats incluent l'appréciation de l'évaluateur ou de l'équipe d'évaluation sur le degré de conformité de l'activité d'audit interne.*

1321 – Utilisation de la mention « conforme aux *Normes internationales pour la pratique professionnelle de l'audit interne* »

Le responsable de l'audit interne peut indiquer que l'activité d'audit interne est conduite conformément aux *Normes internationales pour la pratique professionnelle de l'audit interne* seulement si les résultats du programme d'assurance et d'amélioration qualité l'ont démontré.

Interprétation

Le service d'audit interne est en conformité avec les Normes *lorsqu'il respecte les exigences de la Définition de l'audit interne, du Code de Déontologie et des* Normes*. Les résultats du programme d'assurance et d'amélioration qualité incluent les résultats des évaluations internes et des évaluations externes. Tout service d'audit interne disposera de résultats d'évaluations internes. Les services d'audit interne qui ont plus de cinq ans d'ancienneté disposeront également des résultats de leurs évaluations externes.*

1322 – Indication de non-conformité

Quand la non-conformité de l'activité d'audit interne avec la définition de l'audit interne, le Code de Déontologie ou encore les *Normes* a une incidence sur le champ d'intervention ou sur le fonctionnement de l'audit interne, le responsable de l'audit interne doit informer la direction générale et le Conseil de cette non-conformité et de ses conséquences.

Copyright © 2015 Eyrolles.

Normes de fonctionnement

2000 – Gestion de l'audit interne

Le responsable de l'audit interne doit gérer efficacement cette activité de façon à garantir qu'elle apporte une valeur ajoutée à l'organisation.

Interprétation

L'activité d'audit interne est gérée efficacement quand :

- *les résultats des travaux de l'audit interne répondent aux objectifs et responsabilités définis dans la charte d'audit interne ;*
- *l'audit interne est exercé conformément à la définition de l'audit interne et aux* Normes *;*
- *les membres de l'équipe d'audit agissent en respectant le Code de Déontologie et les* Normes.

Le service d'audit interne apporte de la valeur ajoutée à l'organisation (ainsi qu'à ses parties prenantes) lorsqu'il fournit une assurance objective et pertinente et qu'il contribue à l'efficience ainsi qu'à l'efficacité des processus de gouvernement d'entreprise, de management des risques et de contrôle interne.

2010 — Planification

Le responsable de l'audit interne doit établir un plan d'audit fondé sur les risques afin de définir des priorités cohérentes avec les objectifs de l'organisation.

Interprétation

Il incombe au responsable de l'audit interne de développer un plan d'audit fondé sur les risques. Pour ce faire, le responsable de l'audit interne prend en compte le système de management des risques défini au sein de l'organisation, il tient notamment compte de l'appétence pour le risque définie par le management pour les différentes activités ou branches de l'organisation. Si ce système de management des risques n'existe pas, le responsable de l'audit interne doit se baser sur sa propre analyse des risques après avoir pris en considération le point de vue de la direction générale et du Conseil. Le responsable de l'audit interne doit, le cas échéant, réviser et ajuster le plan afin de répondre aux changements dans les activités, les risques, les opérations, les programmes, les systèmes et les contrôles de l'organisation.

2010.A1 – Le plan d'audit interne doit s'appuyer sur une évaluation des risques documentée et réalisée au moins une fois par an. Les points de vue de la direction générale et du Conseil doivent être pris en compte dans ce processus.

Copyright © 2015 Eyrolles.

2010.A2 – Le responsable de l'audit interne doit identifier et prendre en considération les attentes de la direction générale, du Conseil et des autres parties prenantes concernant les opinions et d'autres conclusions de l'audit interne.

2010.C1 – Lorsqu'on lui propose une mission de conseil, le responsable de l'audit interne, avant de l'accepter, devrait considérer dans quelle mesure elle est susceptible de créer de la valeur ajoutée, d'améliorer le management des risques et le fonctionnement de l'organisation. Les missions de conseil qui ont été acceptées doivent être intégrées dans le plan d'audit.

2020 – Communication et approbation

Le responsable de l'audit interne doit communiquer à la direction générale et au Conseil son plan d'audit et ses besoins, pour examen et approbation, ainsi que tout changement important susceptible d'intervenir en cours d'exercice. Le responsable de l'audit interne doit également signaler l'impact de toute limitation de ses ressources.

2030 – Gestion des ressources

Le responsable de l'audit interne doit veiller à ce que les ressources affectées à cette activité soient adéquates, suffisantes et mises en œuvre de manière efficace pour réaliser le plan d'audit approuvé.

Interprétation

On entend par ressources adéquates, la combinaison de connaissances, savoir-faire et autres compétences nécessaires à la réalisation du plan d'audit. On entend par ressources suffisantes, la quantité de ressources nécessaires à la réalisation du plan d'audit. Les ressources sont mises en œuvre efficacement quand elles sont utilisées de manière à optimiser la réalisation du plan d'audit.

2040 – Règles et procédures

Le responsable de l'audit interne doit établir des règles et procédures fournissant un cadre à l'activité d'audit interne.

Interprétation

La forme et le contenu des règles et procédures dépendent de la taille, de la manière dont est structuré l'audit interne et de la complexité de ses travaux.

2050 – Coordination

Afin d'assurer une couverture adéquate et d'éviter les doubles emplois, le responsable de l'audit interne devrait partager des informations et coordonner les activités avec les autres prestataires internes et externes d'assurance et de conseil.

Copyright © 2015 Eyrolles.

2060 – Rapports à la direction générale et au Conseil

Le responsable de l'audit interne doit rendre compte périodiquement à la direction générale et au Conseil des missions, des pouvoirs et des responsabilités de l'audit interne, ainsi que du degré de réalisation du plan d'audit. Il doit plus particulièrement rendre compte : de l'exposition aux risques significatifs (y compris des risques de fraude) et des contrôles correspondants ; des sujets relatifs au gouvernement d'entreprise et ; de tout autre problème répondant à un besoin ou à une demande de la direction générale ou du Conseil.

Interprétation

La fréquence et le contenu de ces rapports sont déterminés lors de discussions avec la direction générale et le Conseil et dépendent de l'importance des informations à communiquer et de l'urgence des actions correctives devant être entreprises par la direction générale et le Conseil.

2070 – Responsabilité de l'organisation en cas de recours à un prestataire externe pour ses activités d'audit interne

Lorsque l'activité d'audit interne est réalisée par un prestataire de service externe, ce dernier doit alerter l'organisation qu'elle reste responsable du maintien d'un audit interne efficace.

Interprétation

Cette responsabilité est démontrée par le programme d'assurance et d'amélioration qualité, lequel évalue la conformité avec la Définition de l'audit interne, le Code de Déontologie et les Normes.

2100 – Nature du travail

L'audit interne doit évaluer les processus de gouvernement d'entreprise, de management des risques et de contrôle, et contribuer à leur amélioration sur la base d'une approche systématique et méthodique.

2110 – Gouvernement d'entreprise

L'audit interne doit évaluer le processus de gouvernement d'entreprise et formuler des recommandations appropriées en vue de son amélioration. À cet effet, il détermine si le processus répond aux objectifs suivants :

- promouvoir des règles d'éthique et des valeurs appropriées au sein de l'organisation ;
- garantir une gestion efficace des performances de l'organisation, assortie d'une obligation de rendre compte ;

Copyright © 2015 Eyrolles.

- communiquer aux services concernés de l'organisation les informations relatives aux risques et aux contrôles ;
- fournir une information adéquate au Conseil, aux auditeurs internes et externes et au management, et assurer une coordination de leurs activités.

2110.A1 – L'audit interne doit évaluer la conception, la mise en oeuvre et l'efficacité des objectifs, des programmes et des activités de l'organisation liés à l'éthique.

2110.A2 – L'audit interne doit évaluer si la gouvernance des systèmes d'information de l'organisation soutient la stratégie et les objectifs de l'organisation.

2120 – Management des risques

L'audit interne doit évaluer l'efficacité des processus de management des risques et contribuer à leur amélioration.

Interprétation

Afin de déterminer si les processus de management des risques sont efficaces, les auditeurs internes doivent s'assurer que :

- *les objectifs de l'organisation sont cohérents avec sa mission et y contribuent ;*
- *les risques significatifs sont identifiés et évalués ;*
- *les modalités de traitement des risques retenues sont appropriées et en adéquation avec l'appétence pour le risque de l'organisation ;*
- *les informations relatives aux risques sont recensées et communiquées en temps opportun au sein de l'organisation pour permettre aux collaborateurs, à leur hiérarchie et au Conseil d'exercer leurs responsabilités.*

Pour étayer cette évaluation, l'audit interne peut s'appuyer sur des informations issues de différentes missions. Une vision consolidée des résultats de ces missions permet une compréhension du processus de management des risques de l'organisation et de son efficacité.

Les processus de management des risques sont surveillés par des activités de gestion permanente, par des évaluations spécifiques ou par ces deux moyens.

2120.A1 – L'audit interne doit évaluer les risques afférents au gouvernement d'entreprise, aux opérations et aux systèmes d'information de l'organisation au regard de :

- l'atteinte des objectifs stratégiques de l'organisation ;
- la fiabilité et l'intégrité des informations financières et opérationnelles ;
- l'efficacité et l'efficience des opérations et des programmes ;
- la protection des actifs ;
- le respect des lois, règlements, règles, procédures et contrats.

Copyright © 2015 Eyrolles.

2120.A2 – L'audit interne doit évaluer la possibilité de fraude et la manière dont ce risque est géré par l'organisation.

2120.C1 – Au cours des missions de conseil, les auditeurs internes doivent couvrir les risques liés aux objectifs de la mission et demeurer vigilants vis-à-vis de l'existence de tout autre risque susceptible d'être significatif.

2120.C2 – Les auditeurs internes doivent utiliser leurs connaissances des risques acquises lors de missions de conseil pour évaluer les processus de management des risques de l'organisation.

2120.C3 – Lorsque les auditeurs internes aident le management dans la conception et l'amélioration des processus de management des risques, ils doivent s'abstenir d'assumer une responsabilité opérationnelle en la matière.

2130 – Contrôle

L'audit interne doit aider l'organisation à maintenir un dispositif de contrôle approprié en évaluant son efficacité et son efficience et en encourageant son amélioration continue.

2130.A1 – L'audit interne doit évaluer la pertinence et l'efficacité du dispositif de contrôle choisi pour faire face aux risques relatifs au gouvernement d'entreprise, aux opérations et systèmes d'information de l'organisation. Cette évaluation doit porter sur les aspects suivants :

- l'atteinte des objectifs stratégiques de l'organisation ;
- la fiabilité et l'intégrité des informations financières et opérationnelles ;
- l'efficacité et l'efficience des opérations et des programmes ;
- la protection des actifs ;
- le respect des lois, règlements, règles, procédures et contrats.

2130.C1 – Les auditeurs internes doivent utiliser leurs connaissances des dispositifs de contrôle acquises lors de missions de conseil lorsqu'ils évaluent les processus de contrôle de l'organisation.

2200 – Planification de la mission

Les auditeurs internes doivent concevoir et documenter un plan pour chaque mission. Ce plan de mission précise les objectifs, le champ d'intervention, la date et la durée de la mission, ainsi que les ressources allouées.

Copyright © 2015 Eyrolles.

2201 – Considérations relatives à la planification

Lors de la planification de la mission, les auditeurs internes doivent prendre en compte :

- les objectifs de l'activité soumise à l'audit et la manière dont elle est maîtrisée ;
- les risques significatifs liés à l'activité, ses objectifs, les ressources mises en œuvre et ses tâches opérationnelles, ainsi que les moyens par lesquels l'impact potentiel du risque est maintenu à un niveau acceptable ;
- la pertinence et l'efficacité des processus de gouvernement d'entreprise, de management des risques et de contrôle de l'activité, en référence à un cadre ou modèle de contrôle approprié ;
- les opportunités d'améliorer de manière significative les processus de gouvernement d'entreprise, de management des risques et de contrôle de l'activité.

2201.A1 – Lorsqu'ils planifient une mission pour des tiers extérieurs à l'organisation, les auditeurs internes doivent élaborer avec eux un accord écrit sur les objectifs et le champ de la mission, les responsabilités et les attentes respectives, et préciser les restrictions à observer en matière de diffusion des résultats de la mission et d'accès aux dossiers.

2201.C1 – Les auditeurs internes doivent établir avec le client donneur d'ordre un accord sur les objectifs et le champ de la mission de conseil, les responsabilités de chacun et plus généralement sur les attentes du client donneur d'ordre. Pour les missions importantes, cet accord doit être formalisé.

2210 – Objectifs de la mission

Les objectifs doivent être précisés pour chaque mission.

2210.A1 – Les auditeurs internes doivent procéder à une évaluation préliminaire des risques liés à l'activité soumise à l'audit. Les objectifs de la mission doivent être déterminés en fonction des résultats de cette évaluation.

2210.A2 – En détaillant les objectifs de la mission, les auditeurs internes doivent tenir compte de la probabilité qu'il existe des erreurs significatives, des cas de fraudes ou de non-conformité et d'autres risques importants.

2210.A3 – Des critères adéquats sont nécessaires pour évaluer le gouvernement d'entreprise, le management des risques et le dispositif de contrôle. Les auditeurs internes doivent déterminer dans quelle mesure le management et/ou le Conseil a défini des critères adéquats pour apprécier si les objectifs et les buts ont été atteints. Si ces critères sont adéquats, les auditeurs internes doivent les utiliser dans leur évaluation. S'ils sont inadéquats, les auditeurs internes doivent travailler avec le management et/ou le Conseil pour élaborer des critères d'évaluation appropriés.

Copyright © 2015 Eyrolles.

2210.C1 – Les objectifs d'une mission de conseil doivent porter sur les processus de gouvernement d'entreprise, de management des risques et de contrôle dans la limite convenue avec le client.

2210.C2 – Les objectifs de la mission de conseil doivent être en cohérence avec les valeurs, la stratégie et les objectifs de l'organisation.

2220 – Champ de la mission

Le champ doit être suffisant pour atteindre les objectifs de la mission.

2220.A1 – Le champ de la mission doit couvrir les systèmes, les documents, le personnel et les biens concernés, y compris ceux qui se trouvent sous le contrôle de tiers.

2220.A2 – Lorsqu'au cours d'une mission d'assurance apparaissent d'importantes opportunités en termes de conseil, un accord écrit devrait être conclu pour préciser les objectifs et le champ de la mission de conseil, les responsabilités et les attentes respectives. Les résultats de la mission de conseil sont communiqués conformément aux Normes applicables à ces missions.

2220.C1 – Quand ils effectuent une mission de conseil, les auditeurs internes doivent s'assurer que le champ d'intervention permet de répondre aux objectifs convenus. Si, en cours de mission, les auditeurs internes émettent des réserves sur ce périmètre, ils doivent en discuter avec le client donneur d'ordre afin de décider s'il y a lieu de poursuivre la mission.

2220.C2 – Au cours des missions de conseil, les auditeurs internes doivent examiner les dispositifs de contrôle relatifs aux objectifs de la mission et être attentifs à l'existence de tout problème de contrôle significatif.

2230 – Ressources affectées à la mission

Les auditeurs internes doivent déterminer les ressources appropriées et suffisantes pour atteindre les objectifs de la mission. Ils s'appuient sur une évaluation de la nature et de la complexité de chaque mission, des contraintes de temps et des ressources disponibles.

2240 – Programme de travail de la mission

Les auditeurs internes doivent élaborer et documenter un programme de travail permettant d'atteindre les objectifs de la mission.

2240.A1 – Les programmes de travail doivent faire référence aux procédures à appliquer pour identifier, analyser, évaluer et documenter les informations lors de la mission. Le programme de travail doit être approuvé avant sa mise en œuvre. Les ajustements éventuels doivent être approuvés rapidement.

Copyright © 2015 Eyrolles.

2240.C1 – Les programmes de travail des missions de conseil peuvent varier, dans leur forme et leur contenu, selon la nature de la mission.

2300 – Accomplissement de la mission

Les auditeurs internes doivent identifier, analyser, évaluer et documenter les informations nécessaires pour atteindre les objectifs de la mission.

2310 – Identification des informations

Les auditeurs internes doivent identifier les informations suffisantes, fiables, pertinentes et utiles pour atteindre les objectifs de la mission.

Interprétation

Une information suffisante est factuelle, adéquate et probante, de sorte qu'une personne prudente et informée pourrait parvenir aux mêmes conclusions que l'auditeur. Une information fiable est une information concluante et facilement accessible par l'utilisation de techniques d'audit appropriées. Une information pertinente conforte les constatations et recommandations de l'audit, et répond aux objectifs de la mission. Une information utile aide l'organisation à atteindre ses objectifs.

2320 – Analyse et évaluation

Les auditeurs internes doivent fonder leurs conclusions et les résultats de leur mission sur des analyses et évaluations appropriées.

2330 – Documentation des informations

Les auditeurs internes doivent documenter les informations pertinentes pour étayer les conclusions et les résultats de la mission.

2330.A1 – Le responsable de l'audit interne doit contrôler l'accès aux dossiers de la mission. Il doit, si nécessaire, obtenir l'accord de la direction générale et/ou l'avis d'un juriste avant de communiquer ces dossiers à des parties extérieures.

2330.A2 – Le responsable de l'audit interne doit arrêter des règles en matière de conservation des dossiers de la mission et ce, quel que soit le support d'archivage utilisé. Ces règles doivent être cohérentes avec les orientations définies par l'organisation et avec toute exigence réglementaire ou autre.

2330.C1 – Le responsable de l'audit interne doit définir des procédures concernant la protection et la conservation des dossiers de la mission de conseil ainsi que leur diffusion à l'intérieur et à l'extérieur de l'organisation. Ces procédures doivent être cohérentes avec les orientations définies par l'organisation et avec toute exigence réglementaire ou autre appropriée.

Copyright © 2015 Eyrolles.

2340 – Supervision de la mission

Les missions doivent faire l'objet d'une supervision appropriée afin de garantir que les objectifs sont atteints, la qualité assurée et le développement professionnel du personnel effectué.

Interprétation

L'étendue de la supervision est fonction de la compétence et de l'expérience des auditeurs internes, ainsi que de la complexité de la mission. Le responsable de l'audit interne a l'entière responsabilité de la supervision des missions qui sont réalisées par ou pour le compte du service d'audit interne, mais il peut désigner d'autres membres de l'équipe d'audit interne possédant l'expérience et la compétence nécessaires pour réaliser cette supervision. La preuve de la supervision doit être documentée et conservée dans les papiers de travail.

2400 – Communication des résultats

Les auditeurs internes doivent communiquer les résultats des missions.

2410 – Contenu de la communication

La communication doit inclure les objectifs et le champ de la mission, ainsi que les conclusions, recommandations et plans d'actions.

2410.A1 – La communication finale des résultats de la mission doit, lorsqu'il y a lieu, contenir l'opinion des auditeurs internes et/ou leurs conclusions. Lorsqu'une opinion ou une conclusion sont émises, elles doivent prendre en compte les attentes de la direction générale, du Conseil et des autres parties prenantes. Elles doivent également s'appuyer sur une information suffisante, fiable, pertinente et utile.

Interprétation

Les opinions au niveau d'une mission peuvent être formulées sous forme d'échelle de notation, de conclusions ou de toute autre description des résultats. Une telle mission peut être liée aux contrôles d'un processus, de risques ou d'une unité opérationnelle spécifique. La formulation de ces opinions exige de prendre en compte les résultats de la mission et leur caractère significatif.

2410.A2 – Les auditeurs internes sont encouragés à faire état des forces relevées, lors de la communication des résultats de la mission.

2410.A3 – Lorsque les résultats de la mission sont communiqués à des destinataires ne faisant pas partie de l'organisation, les documents communiqués doivent préciser les restrictions à observer en matière de diffusion et d'exploitation des résultats.

Copyright © 2015 Eyrolles.

2410.C1 – La communication sur l'avancement et les résultats d'une mission de conseil variera dans sa forme et son contenu en fonction de la nature de la mission et des besoins du client donneur d'ordre.

2420 – Qualité de la communication

La communication doit être exacte, objective, claire, concise, constructive, complète et émise en temps utile.

Interprétation

Une communication exacte ne contient pas d'erreur ou de déformation, et est fidèle aux faits sous-jacents. Une communication objective est juste, impartiale, non biaisée et résulte d'une évaluation équitable et mesurée de tous les faits et circonstances pertinents. Une communication claire est facilement compréhensible et logique. Elle évite l'utilisation d'un langage excessivement technique et fournit toute l'information significative et pertinente. Une communication concise va droit à l'essentiel et évite tout détail superflu, tout développement non nécessaire, toute redondance ou verbiage. Une communication constructive aide l'audité et l'organisation, et conduit à des améliorations lorsqu'elles sont nécessaires. Une communication complète n'omet rien qui soit essentiel aux destinataires cibles. Elle intègre toute l'information significative et pertinente, ainsi que les observations permettant d'étayer les recommandations et conclusions. Une communication émise en temps utile est opportune et à propos, elle permet au management de prendre les actions correctives appropriées en fonction du caractère significatif de la problématique.

2421 – Erreurs et omissions

Si une communication finale contient une erreur ou une omission significative, le responsable de l'audit interne doit faire parvenir les informations corrigées à tous les destinataires de la version initiale.

2430 – Utilisation de la mention « conduit conformément aux Normes internationales pour la pratique professionnelle de l'audit interne »

Les auditeurs internes peuvent indiquer dans leur rapport que leurs missions sont « conduites conformément aux *Normes internationales pour la pratique professionnelle de l'audit interne* » seulement si les résultats du programme d'assurance et d'amélioration qualité le démontrent.

Copyright © 2015 Eyrolles.

2431 – Indication de non-conformité

Lorsqu'une mission donnée n'a pas été conduite conformément à la Définition de l'audit interne, au Code de Déontologie ou aux *Normes,* la communication des résultats doit indiquer :

- les principes ou les règles de conduite du Code de Déontologie, ou les *Normes* avec lesquelles la mission n'a pas été en conformité ;
- la ou les raisons de la non-conformité ;
- l'incidence de la non-conformité sur la mission et sur les résultats communiqués.

2440 – Diffusion des résultats

Le responsable de l'audit interne doit diffuser les résultats aux destinataires appropriés.

Interprétation

Le responsable de l'audit interne a la responsabilité de la revue et de l'approbation du rapport définitif avant qu'il ne soit émis, et décide à qui et de quelle manière il sera diffusé. Lorsque le responsable de l'audit interne délègue ces fonctions, il/elle en garde l'entière responsabilité.

2440.A1 – Le responsable de l'audit interne est chargé de communiquer les résultats définitifs aux destinataires à même de garantir que ces résultats recevront l'attention nécessaire.

2440.A2 – Sauf indication contraire de la loi, de la réglementation ou des statuts, le responsable de l'audit doit accomplir les tâches suivantes avant de diffuser les résultats à des destinataires ne faisant pas partie de l'organisation :

- évaluer les risques potentiels pour l'organisation ;
- consulter la direction générale et/ou, selon les cas, un conseil juridique ;
- maîtriser la diffusion en imposant des restrictions quant à l'utilisation des résultats.

2440.C1 – Le responsable de l'audit interne est chargé de communiquer les résultats définitifs des missions de conseil à son client donneur d'ordre.

2440.C2 – Au cours des missions de conseil, il peut arriver que des problèmes relatifs aux processus de gouvernement d'entreprise, de management des risques et de contrôle soient identifiés. Chaque fois que ces problèmes sont significatifs pour l'organisation, ils doivent être communiqués à la direction générale et au Conseil.

2450 – Les opinions globales

Lorsqu'une opinion globale est émise, elle doit prendre en compte les attentes de la direction générale, du Conseil et des autres parties prenantes. Elle doit également s'appuyer sur une information suffisante, fiable, pertinente et utile.

Copyright © 2015 Eyrolles.

Interprétation

La communication précisera :

- *le périmètre, y compris la période concernée par l'opinion ;*
- *les limitations de périmètre ;*
- *le fait de prendre en compte d'autres travaux connexes, y compris ceux d'autres services donnant une assurance sur la maîtrise des activités ;*
- *le référentiel des risques ou de contrôle interne ou tout autre critère utilisé pour formuler l'opinion globale ;*
- *l'opinion globale, l'avis ou la conclusion donnée.*

Les causes de la formulation d'une opinion globale défavorable doivent être explicitées.

2500 – Surveillance des actions de progrès

Le responsable de l'audit interne doit mettre en place et tenir à jour un système permettant de surveiller la suite donnée aux résultats communiqués au management.

2500.A1 – Le responsable de l'audit interne doit mettre en place un processus de suivi permettant de surveiller et de garantir que des mesures ont été effectivement mises en œuvre par le management ou que la direction générale a accepté de prendre le risque de ne rien faire.

2500.C1 – L'audit interne doit surveiller la suite donnée aux résultats des missions de conseil conformément à l'accord passé avec le client donneur d'ordre.

2600 – Communication relative à l'acceptation des risques

Lorsque le responsable de l'audit interne conclut que le management a accepté un niveau de risque qui pourrait s'avérer inacceptable pour l'organisation, il doit examiner la question avec la direction générale. Si le responsable de l'audit interne estime que le problème n'a pas été résolu, il doit soumettre la question au Conseil.

Interprétation

L'identification du niveau de risque accepté par le management peut résulter d'une mission d'assurance, d'une mission de conseil, du suivi des plans d'actions du management à la suite de missions d'audit interne antérieures, ou d'autres moyens. La réponse au risque ne relève pas du responsable d'audit interne.

Copyright © 2015 Eyrolles.

INDEX

A

Acceptation, modalité de traitement des risques 5-17

ACL (*Audit Command Language*) 10-16

Actes illégaux, risques d'~
  questions et thèmes de discussion 8-56

Actes illégaux, traitement des ~ 8-31

Actes malveillants 7-14

Actifs, détournement d'~ 8-11, 8-26

Actionnaires et investisseurs, partie prenante . 3-7

Actions, discours 6-17

Activités d'assurance
  définition 3-15
  planification 9-11
  spécificités 15-8

Activités de conseil
  évolutions 15-27
  spécificités 15-8
  types d'~ 15-12

Adéquation de la conception, définition 13-39

American Institute of Certified Public Accountants (AICPA) 2-43
  adéquation d'une preuve 10-3

Analyse comparative (*benchmarking*) externe, définition 10-12

Analyse comparative (*benchmarking*) interne, définition 10-12

Analyse de ratios 10-11

Analyse des données, techniques d'audit informatisées (utilisation) 13-16

Analyse de tendance 10-11

Approche ascendante (*bottom-up*) 5-9
  définition 5-8
  déroulement 5-9

Approche descendante (*top-down*), définition 5-5

Association of Certified Fraud Examiners (ACFE) 2-23
  rapport de l'ACFE 8-17
  typologie des fraudes et abus 8-11

Assurance
  activités d'~ 3-17
  assurance négative 14-24
  assurance positive 14-23
  composante de la proposition de valeur de l'audit interne 1-2
  coordination des travaux d'~ 9-21
  valeur ajoutée/amélioration 1-7

Assurance qualité, définition 9-28

Assurance raisonnable 10-3
  définition 8-24, 10-2, 13-40

Audit
  audit continu 7-30, 10-14
  audit intégré 7-29
  relation entre l'~ et la comptabilité 1-10

Audit Command Language (ACL)
  définition 10-16

Audité
  assertions de l'~, définition 12-7
  comprendre l'~ 13-27
  objectifs de l'~
    définition 12-7, 13-10
    détermination des objectifs de l'~ 13-13

Auditeur, compréhension 12-7

Auditeur interne senior (ou chef de mission) . 9-13

Auditeur(s) externe(s)
  définition 9-18
  responsabilités dans le cadre de l'ERM 4-18
  rôles et responsabilités en matière de contrôle interne 6-31

Auditeurs internes 9-13
  compétence, Code de Déontologie 2-11
  compétences 1-25
  confidentialité 2-11
  connaissances, savoir-faire et références .. 1-24
  contrôle interne 6-31
    rôles et responsabilités des~ 6-25
  ERM, responsabilités des ~ 4-20
  évolution de carrière 1-25
  intégrité 2-9
  objectivité 2-9
  procédures analytiques, utilisation 13-15

Copyright © 2015 Eyrolles.

INDEX

qualités personnelles 1-22
SI, impacts pour les ~ 7-30
Audit intégré 7-29
définition 7-29
Audit interne
assurance, ERM 4-29
carrières dans l'~ 1-27
charte d'~, définition 9-5
gestion de l'~ 2-27
indépendance 1-7, 2-17
mission(s) d'~
catégories de mission(s) d'~ 12-3
communication des résultats, responsabilité du responsable de l'audit interne 2-31
normes 2-32
objectivité 2-17
plan d'~
définition 9-9
plan annuel d'~ 15-14
principaux rôles de l'~ 4-25
profession d'~ 1-13
lignes directrices, historique 2-5
rôles
à éviter 4-27
garde-fous 4-26
services d'~
nature/périmètre 1-15
recours à des prestataires de services d'~ 1-16
Audit interne (*Internal Auditing*)
composantes de la proposition de valeur de l'~ 1-3
définition 1-2, 1-3, 2-2, 2-7
parcours professionnels 1-26
questions et thèmes de discussion 1-32
Audit interne, principaux rôles 4-25
Auto-évaluation des contrôles, définition 15-10
Autorités de régulation et de supervision, parties prenantes 3-8
Avis 15-9
avis, formulation 15-21
exécution d'une mission de conseil 15-20
planifer une mission de conseil 15-17
preuves, recueil et évaluation 15-21

B

Banque mondiale 2-39
Base(s) de données 7-8
administrateur de ~, responsabilités 7-9
définition 7-7
BEAC (*Board of Environmental, Health, and Safety Auditor Certifications*), définition 2-43
Big Data, définition 7-8
BYOD (*Bring Your Own Device* - « Apportez vos outils personnels »), définition 7-2

C

Cadre de Référence International des Pratiques Professionnelles (CRIPP) 1-17, 2-2
actualisation du ~ 2-41
définition 2-5
études de cas 2-57
questions et thèmes de discussion 2-50
Cartographie générale des processus, utilisation 5-10
CBOK, *Common Body of Knowledge* (socle commun de connaissances) 2-3
CCSA (*Certification in Control Self-Assessment*, certification en auto-évaluation des contrôles) 2-23
Certifications proposées par l'IIA 2-23
CFE (*Certified Fraud Examiner*) 2-23
certification 8-46
définition 8-47
CFSA (*Certified Financial Services Auditor*, certification en audit des services financiers) . 2-23
CGAP (*Certified Governmental Audit Professional*, certification en audit des organisations publiques) 2-23
Chef de mission, *Voir* Auditeur interne senior
CIA (*Certified Internal Auditor*, auditeur interne certifié) 2-23
certification 1-18
programme de certification 2-3
définition 1-18

Copyright © 2015 Eyrolles.

INDEX

CISA (*Certified Information Systems Auditor*, certification en audit des systèmes d'information) 2-23
Client(s) de l'organisation
  définition 15-6
  parties prenantes 3-7
Code de Déontologie 2-12
Collaborateurs
  facteurs de risque 4-10
  rôles et responsabilités en matière de contrôle interne 6-26
  rôles et responsabilités en matière de gestion du risque de fraude 8-21
Collusion, définition 8-35
Comité de Bâle sur le contrôle bancaire 2-44
Communication
  contenu de la ~, définition 2-31
  déterminer l'obligation de ~ 14-5
  qualité de la ~ 14-32
    définition 2-31
Communication finale
  définition 14-20
  diffusion 15-25
  élaboration 14-25
  formelle
    diffusion 14-29
  informelle
    diffusion 14-27, 14-29
Communications intermédiaires 12-12
  procéder à des ~ 14-20, 15-22
Communications préliminaires 12-12
  procéder à des ~ 14-20, 15-22
Communications provisoires, *Voir* Communications intermédiaires
Compétence 2-24
  Code de Déontologie 2-11
    définition 2-11
  définition 1-22, 2-21
  engagement de l'organisation 4-8
Conclusion, définition 14-22
Confidentialité
  définition 2-10
  risque lié à la violation de la ~ 7-13
Confirmation (ou circularisation) 10-12
Conformité, résultats 3-9
Conscience professionnelle 2-24, 9-9
  définition 2-22, 8-45
Conseil (*Consulting*)
  activités de ~ 2-16
    planification 9-11
  activités de ~, valeur ajoutée/amélioration 1-7
  déroulement de la mission de ~ 12-16
    accomplissement de la mission 12-16
Conseil (d'administration) 4-8
  définition 3-5, 9-20
  responsabilités dans le cadre de l'ERM 4-15
  rôles et responsabilités dans la gestion du risque de fraude 8-20
  rôles et responsabilités en matière de contrôle interne 6-25
Contrôle au niveau des processus 6-34
  définition 6-34
Contrôle au niveau des transactions 6-34
  définition 6-34
Contrôle compensatoire 6-35
Contrôle détectif 6-36
  définition 8-37
Contrôle interne 3-3
  activités de contrôle 6-17
  approches du ~ 6-32
  classification dans plusieurs catégories 6-37
  composantes du ~ 6-11, 6-13
  contrôle à l'échelle de l'entité 6-34
  contrôle au niveau des processus 6-34
  contrôle clé 6-35
  contrôle compensatoire 6-35
  contrôle détectif 6-36
  contrôle préventif 6-36
  contrôle secondaire 6-35
  définition 6-9
  environnement de contrôle 6-13
  évaluation des risques 6-15
  évaluation du système de ~ 6-39
  information et communication 6-18
  limites du ~ 6-30
  objectifs 6-12, 11-7
  pilotage 6-20

Copyright © 2015 Eyrolles.

INDEX

principes du ~ 6-23
questions et thèmes de discussion 6-46
référentiels de ~ 6-9
rôles et responsabilités en matière de ~ ... 6-26
transactions 6-34
typologie des contrôles 6-37
Contrôle préventif 6-36
définition 8-34
Contrôle(s), *Voir* Contrôle interne
activités de ~ 4-12, 7-17
auto-évaluation des ~, définition 9-34
catégories de ~ 13-36
conception des ~ 12-9, 13-39
contournement des ~ par le management 8-25
écart, déviation 11-6
environnement ~, définition 8-21
processus de ~, efficacité (évaluation, amélioration) 1-7
risque de non-contrôle 11-4
risque de sous-estimation du risque de non-contrôle 11-9
tests
détermination 13-41
échantillonnage non statistique 11-21
échantillonnage statistique 11-18
Contrôles à l'échelle de l'entité 6-34
analyse 13-16
définition 4-22, 6-32, 13-16
Contrôle(s) clé(s) 6-35
définition 12-8
distinguer les ~ 13-36
identifier les ~ 13-37
Contrôles des données d'entrée 7-23
Contrôles des données de sortie 7-23
Contrôles du traitement 7-23
Contrôles physiques 4-12
Contrôles secondaires 6-35
Corruption 8-26
définition 8-5
COSO (*Committee of Sponsoring Organizations of the Treadway Commission*) 1-10, 2-44
catégories d'objectifs proposées par le ~ . 14-7
définitions du risque 4-5
ERM, management des risques de l'entreprise
cadre de référence ERM relatif au management des risques de l'entreprise 4-20
CRMA (*Certification in Risk Management Assurance*, certification en évaluation de la gestion des risques) 2-23

D

Décision d'audit, sur la base d'un échantillonnage 11-18
Déclaration sur l'honneur 8-22
Détection de la fraude par anticipation 8-36
Diagrammes de flux
définition 13-17
~ détaillés 13-23
~ macro 13-18
Diagrammes de flux macro 13-18
Directeur de mission 9-13
Directeur des risques
définition 4-16
responsabilités, selon le COSO 4-17
Direction financière, responsabilités dans le cadre de l'ERM 4-17
Direction générale 3-13
Discours, actions 6-17
Dispositifs d'alerte 8-36
Dispositions
dispositions fortement recommandées 2-37
dispositions obligatoires 2-32
Dodd-Frank Act 3-29
Données personnelles 7-13
DSI (Directeur des systèmes d'information), responsabilités relatives aux SI 7-9

E

Échanges de données informatisées (EDI) 7-11
définition 7-10

Copyright © 2015 Eyrolles.

INDEX

Échantillonnage à l'aveuglette, définition 11-18
Échantillonnage aléatoire, définition 11-12
Échantillonnage d'attributs
  analyser les résultats 11-18
  définition 11-5
  élaborer un plan d'~, exécuter ce plan 11-18
  méthodes d'~ 11-5
Échantillonnage d'attributs stratifié 11-5
Échantillonnage de dépistage 11-6
Échantillonnage de variables classique 11-24
  définition 11-23
  échantillonnage par unités monétaires (EUM) 11-23
    définition 11-22
    échantillonnage de variables classique, spécificités 11-24
    spécificités 11-25
Échantillonnage en audit
  approches de l'~ 11-3
  échantillonnage non statistique 11-21
  échantillonnage statistique 11-18
  études de cas 11-33
  introduction à l'~ 11-4
  questions et thèmes de discussion 11-32
Échantillonnage *stop-or-go* (ou séquentiel) .. 11-5
Échantillonnage statistique 11-18
Éléments de l'échantillon, auditer/dénombrer les écarts 11-12
Entretien de départ d'un collaborateur, fraude 8-33
ERM - Management des risques de l'entreprise 4-20
  audit interne, rôle dans l'~ 4-28
  définition par le COSO 4-5
  éléments de l'utilisation 4-14
  impact de l'~ 4-29
  organisations dotées d'un dispositif d'~ ... 4-28
  rôles et responsabilités dans le cadre du ~ 4-20
ERM piloté par l'audit interne 4-28
Erreur, définition 14-32
Établissements financiers, partie prenante 3-9
Évaluation des risques 4-10, 7-17, 12-8
  application des concepts 5-32
  contrôle interne 6-13
  définition 5-17, 8-17, 13-30
  impact (ou gravité) / probabilité d'occurrence 5-13
  utilisation 13-35, 15-15
Événements, identification 4-9, 7-17
Évitement, modalité de traitement des risques 5-17
Externalisation de processus opérationnels 5-29
  définition 5-27
Externalisation (ou co-traitance), définition 9-16, 13-46
Extraire l'échantillon 11-12

F

Facteurs économiques 4-9
Facteurs environnementaux 4-9
Facteurs externes (COSO) 4-9
Facteurs politiques 4-9
Facteurs sociaux 4-9
FCPA (*Foreign Corrupt Practices Act*) ... 3-28, 8-30
Federal Deposit Insurance Corporation Improvement Act (FDICIA) de 1991 3-28
Fonction d'audit interne, *Voir* Audit Interne
  ajustement des effectifs 9-16
  approbation 9-12
  budget 9-17
  communication 9-12
  compétence 9-9
  conscience professionnelle 9-9
  Conseil, communications 9-23
  contrôle 9-29
  coordination des travaux d'assurance 9-21
  définition du rôle de la ~ 4-26
  Direction générale, communications 9-23
  efficacité 3-16
  externalisation (ou co-traitance) 9-16
  formation et tutorat 9-16
  gestion de la ~ 9-1

Copyright © 2015 Eyrolles.

INDEX

gestion des carrières/développement professionnel 9-17
gestion des ressources 9-18
gestion des risques 9-28
gouvernance 9-25
indicateurs de performance 9-34
non-conformité 9-34
planification 9-11, 9-17
positionnement 9-9
pratiques d'embauche 9-16
prévisions d'effectifs 9-15
programmes d'assurance qualité et d'amélioration 9-34
questions et thèmes de discussion 9-45
règles et procédures 9-18
ressources humaines 9-15
rôle de la ~, ERM 4-28
structure hiérarchique 9-12
systèmes d'information 9-38

Fonctionnement effectif, définition 13-57

Fonctions d'audit interne à structure hiérarchique 9-12

Fondamentaux de l'audit interne 1-18

Formation à la lutte contre la fraude 8-33

Fournisseurs, partie prenante 3-7

Fraude
actions correctives 8-40
allégations de ~
évaluer les allégations 8-38
réception des allégations 8-38
aperçu des cas de ~ 8-6
causes à l'origine de la ~ 8-14
définitions de la ~ 8-12
détection de la ~ 8-37
définition 8-19
détection de la fraude par anticipation 8-36
enquête(s) 8-40
mettre en place des protocoles d'enquête 8-40
processus d'enquête 8-23
fraude en entreprise 8-14
fraudeurs
définition 8-42
signaux d'alerte 8-6
mesures disciplinaires et/ou correctives 8-23
moyens techniques 8-45
notification d'une ~, enquête et suivi 8-19
prévention de la ~ 8-35
prévention/détection de la ~ 8-18
processus de lutte contre la ~ 8-23
recours à des spécialistes de la lutte contre la ~ 8-47
résultats d'un audit portant sur une ~, communication 8-47
scepticisme/jugement professionnel 8-45
sensibilisation à la ~, définition 8-23
triangle de la ~ 8-13

Fraude en entreprise, définition 8-14

Fraudeurs, comprendre les ~ 8-42

G

GAIN (*Global Audit Information Network*) ... 1-19

GAIT (*Guides to the Assessment of IT Risk*) 7-30

GAO (*U.S. Government Accountability Office*), définition 2-41

Gestion des risques 9-28
activités de ~, réévaluation 3-14
culture du risque 4-7
définition 9-25
efficacité des processus de ~, évaluation/amélioration 1-7
études de cas 4-39
finalités 9-26
gouvernance 3-2
présentation de la ~ 4-5
programme de ~ 3-17
questions et thèmes de discussions 4-38

Gestion des risques, communication 3-11

Gestion du risque de fraude
principes de la ~ 8-19
programme de ~
éléments d'un programme de 8-23
gouvernance d'un programme de 8-23
rôles et responsabilités associés 8-22

Global Ethics Committee (Comité mondial de déontologie) 2-38

Copyright © 2015 Eyrolles.

INDEX

Gouvernance (ou gouvernement d'entreprise)
attentes concernant la ~, réévaluation 3-11
Comité, instauration 3-10
concepts liés à la ~ 3-19
Conseil et ses comités, rôles et responsabilités au sein de la ~ 3-11
définition 8-17
études de cas 3-35
évolution de la ~ 3-20
gouvernance des SI 7-15
opportunités d'intervention pour l'audit interne 3-22
principaux éléments de la ~ 3-2
processus de ~, efficacité (évaluation/amélioration) 1-7
questions et thèmes de discussion 3-34
responsabilités de la direction générale en matière de ~ 3-13

Gouvernement d'entreprise, *Voir* Gouvernance

GTAG (*Global Technology Audit Guides*)
contenu 7-14
définition 7-30

Guides pratiques, définition 2-35

H

Health Care Compliance Association (HCCA) 2-44

I

IAASB (*International Auditing and Assurance Standards Board*, Conseil des normes internationales d'audit et d'assurance) 2-43

IDEA (*Interactive Data Extraction and Analysis*) 10-16
définition 10-16

IFAC (*International Federation of Accountants*) 2-43
définition 2-44

IIA (*Institute of Internal Auditors*)
adhérents 1-2
certifications professionnelles proposées 1-18, 2-23
Code de Déontologie 1-8
devise de l'IIA 1-16
Global Audit Information Network (GAIN) 1-19
Global Ethics Committee (Comité mondial de déontologie) 2-38
lignes directrices à l'intention des professionnels 1-17
mission de l'IIA 1-17
Normes internationales pour la pratique professionnelle de l'audit interne 1-8, 2-13
définition 2-12
glossaire des *Normes* 3-4
types de *Normes* 2-13
organisation de l'IIA 1-17
Professional Issues Committee (PIC, Comité des questions professionnelles) 2-38
Statement of the Responsibilities of the Internal Auditor (Énoncé des responsabilités de l'auditeur interne) (publication) 2-3
Vision for the Future Task Force (groupe de travail Vision pour le futur) 2-39

IIARF (Fondation pour la recherche de l'IIA), création 1-19
mission 1-19

Impact, définition 8-27, 13-30

Indépendance
atteintes à l'~, définition 4-27, 15-26
conflit d'intérêts 2-18
définition 1-7
menaces 2-19

Indépendance dans l'organisation, définition . 9-6

Indicateurs clés de performance 5-9
définition 13-25
identifier les ~ 13-26

Information(s) 7-9
catégories et sources d'~ 13-14
communication 7-17
contrôles de la sécurité de l'~ 7-25
intégrité de l'~ 7-13
sources d'~ externes 5-5
systèmes d'~

Copyright © 2015 Eyrolles.

INDEX

collaborateurs, acteurs des SI 7-10
composantes des systèmes d'~ 7-10
traitement de l'~ 4-12
Informatique
logiciels 7-8
matériel ~ 7-6
Infrastructure 4-10
Intégrité 2-9, 4-8
contrôles d'~ 7-23
International Auditing Education Partnership (IAEP) 1-21
International Internal Auditing Standards Board (Conseil international sur les normes d'audit interne) 2-38
INTOSAI (*International Organisation of Supreme Audit Institutions*) 2-39, 2-42
ISA (*International Standard on Auditing*), fraude 8-12
ISACA (anciennement connu sous le nom d'*Information Systems Audit and Control Association*) 1-18, 2-23, 2-43
définition 2-42
ISO (Organisation internationale de normalisation)
définitions du risque 4-5
ISO 31000 4-23
cadre organisationnel de la norme ISO 31000 4-21
principes de la norme ISO 31000 4-20
processus de la norme ISO 31000 4-22
normalisation 2-43

L

Législateur/régulateur, responsabilités dans le cadre de l'ERM 4-18
Lien primaire, définition 5-19
Lien secondaire, définition 5-19
Logiciel d'audit généralisé 10-12
déploiement, obstacles 10-16
utilisation, bénéfices 10-16

M

Management
contrôle interne 6-31
rôles et responsabilités en matière de contrôle interne 6-23
processus de supervision 5-4
programme de gestion du risque de fraude, rôles et responsabilités 8-21
responsabilités dans le cadre de l'ERM 4-16
traçabilité 7-23
Mission
budgétisation 13-46
définition 1-8
élaborer un programme de travail 12-9
établir un plan de test 12-9
finalité de la ~ 13-5
intervenants de la ~ 15-7
motivation d'une ~ 13-6
objectifs
définition 13-6
déterminer le périmètre de la ~ 13-8, 13-10, 15-18
déterminer les objectifs de la ~ 15-18
obligation de communication des résultats d'une ~ 14-6
observations et recommandations de la ~ 14-17
planification de la ~ 1-9
ressources
allocation 12-9, 13-48
définition 13-45
Missions centrées sur les contrôles, définition 12-3
Missions centrées sur les performances, définition 12-3
Mission(s) d'assurance
allocation des ressources 13-48
analyse des contrôles de l'échelle de l'entité 13-16
analyse des données, techniques d'audit informatisées 13-16
audit des SI, intégration 7-29
budgétisation 13-46
communication des résultats des ~ 12-15
complexité des ~ 2-15

Copyright © 2015 Eyrolles.

INDEX

contrôles clés, identification 13-37
définition d'une ~ 5-24, 13-2
diagramme de flux macro 13-18
étude de cas 13-71
évaluer l'adéquation de la conception des contrôles 13-39
finalité 13-5
indicateurs clés de performance, identification 13-26
informations
  catégories et sources 13-14
  recueil 13-13
méthode de test
  définir une méthode de test 13-41
  documenter la méthode de test 13-42
motivations d'une ~ 13-6
notes narratives 13-24
objectifs, définition 13-7
observations, formulation 13-55
périmètre (ou champ) 13-8
plan des tests, établissement 13-42
planification des ~ 12-9
preuves
  évaluation/ conclusions 13-50
  recueil, tests 13-50
procédures analytiques 13-15
procédures de surveillance et de suivi, mise en œuvre 12-14
processus
  flux de ~, documentation 13-17
  ~, présentation 12-15
processus opérationnels et risques, utilisation dans les ~ 5-27, 5-28
programme de travail, élaboration 13-45
questions et thèmes de discussion 13-68
rapport définitif, rédaction 12-12
recommandations, formulation 13-55
responsabilités relatives aux SI 7-28
ressources humaines, allocation 13-46
résultats attendus 13-10
résultats définitifs, communication formelle et informelle 12-14
risques
  identifier et évaluer les risques 13-35
  impact et probabilité, évaluation 13-33
  tolérance au risque 13-35
  risques au niveau des processus
    définition des ~ 13-30
    scénarios, identification des ~ 13-29
Mission(s) de conseil
  client, examen de l'avis formulé 15-22
  communication des résultats 15-8, 15-25
  communications intermédiaires et préliminaires 15-22
  compétences / expérience requises 15-28
  demandes du management 15-14
  déroulement d'une mission 15-25
  études de cas 15-36
  évaluation des risques des ~ 15-15
  exécution d'une mission 15-21
  finalité de la mission 15-8
  missions de conseil axées sur la formation 15-10
  missions de conseil destinées à formuler un avis 15-9
    planification 15-20
    réalisation 15-21
  missions de conseil visant à apporter une assistance 15-11
  Normes, application 15-7
  objectifs/périmètre, validation 15-18
  papiers de travail d'une ~ 15-26
  point de vue 15-29
  questions et thèmes de discussion 15-33
  rapport définitif, diffusion 15-25
  ressources
    allocation 15-20
  ressources nécessaires 15-29
  sous-traitance 15-29
  suivi 15-25
  sujets émergents et changements 15-15
Missions internes d'assurance, approche 1-9
Missions mixtes 15-13
  définition 15-11
Modalités de traitement des risques, détermination 5-25
Modalités Pratiques d'Application 2-33

Copyright © 2015 Eyrolles.

INDEX

N

NACD (*National Association of Corporate Directors*) 2-39
NASDAQ (*National Association of Securities Dealers Automated Quotations*) 3-29
Non-conformité, indication de ~ 9-34
Non-conformité, législation 8-26
Non-conformité, réglementation 8-26
Normes, Voir *Institute of Internal Auditors*
Normes américaines de cotation en bourse ... 3-29
Normes de fonctionnement 2-13, 2-32
Normes de mise en œuvre 2-13
Normes de qualification 2-13, 2-26
Normes, types de ~ 2-13
Note(s) narrative(s) 13-17, 13-24
  motivations d'une ~ 13-19
Notification des conflits 8-22
NYSE (*New York Stock Exchange*) 3-29

O

Objectifs
  catégories d'~ 4-8, 13-13
  définition 5-3
  fixation des ~ 4-9, 7-17
Objectifs, typologie du COSO 1-4
Objectivité 2-10
  atteintes à l'~, définition 4-27
  composante de la proposition de valeur de l'audit interne 1-2
  conflits d'intérêts 2-18
  définition 1-8
  menaces 2-19
Objectivité individuelle, définition 9-6
Observation critique, définition 14-11
Observation non significative, définition 14-11
Observation(s)
  définition 12-11
  éléments d'une ~ 14-12
  faire des ~ 12-11
  processus d'évaluation 12-11, 14-18
  remontée de l'information 12-11
Observation significative, définition 14-11
OCDE (Organisation de coopération et de développement économiques) 2-39
  gouvernance (ou gouvernement d'entreprise), définition 3-4
Organisations
  atteinte des objectifs 2-3
  ~ dotées d'un dispositif ERM piloté par l'audit interne 4-28

P

Papiers de travail 10-1, 10-20
  finalités et contenu des ~ 10-17
  questions et thèmes de discussion 10-29
  règles relatives à l'élaboration des ~ 10-20
  types de ~ 10-19
Partage (ou transfert), modalité de traitement des risques 5-17
Parties prenantes externes, rôles et responsabilités en matière de contrôle interne 6-32
Parties prenantes, types de ~ 3-11
PCAOB (*Public Company Accounting Oversight Board*), définition 2-43
Performance(s)
  évaluation des ~ 8-33
  indicateurs de ~ 4-12
Périmètre (ou champ), définition 14-22
Pilotage 7-18
  activités de ~ 6-20
  définition 4-13
  surveillance des actions de progrès, définition 12-15
Piste d'audit ascendante (*vouching*), définition 10-10
Piste d'audit descendante (*tracing*), définition 10-10
Plan annuel d'audit interne 15-14

Copyright © 2015 Eyrolles.

INDEX

Point de vue
composante de la proposition de valeur de l'audit interne 1-2
définition 15-5
Population, définir la ~ 11-8
Pratiques professionnelles de l'audit interne . 1-18
Preuves d'audit 10-5
caractère convaincant des ~ 10-5
définition 10-3
évaluer les ~ 12-10
questions et thèmes de discussion 10-29
Prises de position 2-35
définition 2-34
Probabilité, définition 8-27, 13-31
Procédures analytiques, définition 10-11
Procédures d'audit 10-16
calendrier d'application des ~ 10-7
d'audit manuelles 10-12
définition 10-5
étendue des ~ 10-6
nature des ~ 10-6
Processus
cartographie des ~, définition 5-10, 13-17
conception, évaluation 13-39
contrôles des ~ 8-36
description des ~ 5-10
documentation des flux de ~ 13-17
évaluation et amélioration des ~ 8-23
matrice risques/processus 5-19
note descriptive 13-17, 13-24
Processus d'audit 1-9, 12-1
études de cas 12-23
questions et thèmes de discussion 12-22
Processus opérationnels 5-10
analyse 5-17
classification générique 5-6
comprendre les ~ 5-10
définition 5-2
description écrite des ~ 5-11
propriétaire du processus/collaborateurs, compréhension 5-9
utilisation des ~ 5-27, 5-28
Processus support 5-4
Professional Issues Committee (PIC, Comité des questions professionnelles) 2-38
Progiciel de gestion intégré (PGI), définition . 7-11
Programme de gestion des risques établi par le management 3-17
Programme de travail
définition 13-42
élaborer un ~ 12-9, 13-45
format 13-42
Programmes d'assurance qualité et d'amélioration 2-26
Prospective, analyse d'information 10-11

Q

Qualité de la communication, définition 14-31

R

Recommandation, définition 14-18
Réduction, option de traitement des risques . 5-17
Réexécution (de contrôles, d'autres procédures, ou de calculs) 10-10
Réglementation, synthèse des principaux textes en vigueur aux États-Unis 3-29
Relations personnelles/conflits d'intérêts 2-20
Reporting financier
activités d'assurance 1-12
~ frauduleux 8-26
Réseaux 7-7
Responsable de l'audit interne 9-14
définition 1-26, 9-3
rattachements 1-1
responsabilités 2-20, 2-31, 9-15
rôle 15-4
Ressources, critères 15-20
Ressources humaines 13-30
allocation des ~ 13-46
politique de ~ 4-8
Résultats
seuils de tolérance, évaluation 13-35
types de ~ 3-9

Copyright © 2015 Eyrolles.

INDEX

Résultats d'échantillonnage
évaluer les ~ 11-18
prendre en compte les aspects qualitatifs des ~ 11-17
Résultats d'une mission d'assurance et procédures de suivi
communication
normes 14-29
qualité de la communication 14-32
communications finales 14-25
communications finales formelles, diffusion 14-29
communications finales informelles, diffusion 14-29
communications intermédiaires et préliminaires 14-20
éléments d'une observation 14-12
erreurs et omissions 14-32
études de cas 14-45
évaluation des observations/remontée de l'information
catégories d'objectifs, COSO 14-7
classification 14-7
déficience significative 14-11
faiblesse importante 14-13
observation, impact/probabilité 14-10
observation non significative 14-11
observation, réaliser l'évaluation et la remontée de l'information 14-18
recommandations 14-18
référentiels/faits/causes/conséquences 14-18
normes relatives à la communication des résultats d'une mission 14-6
observations/recommandations 14-17
questions et thèmes de discussion 14-43
surveillance et suivi 14-34
systèmes de notation 14-25
Résultats financiers 3-9
Résultats opérationnels 3-10
Résultats stratégiques 3-10
Revues du management 4-12
Risque d'audit 11-4
définition 10-3, 11-3
Risque d'échantillonnage 11-4
définition 11-4
marge de tolérance 11-14
Risque de déploiement 7-12
Risque de développement/d'acquisition 7-12
Risque de sélection 7-12
Risque d'indisponibité 7-13
Risque discrétionnaire, défintion 11-4
Risque inhérent, définition 4-10, 12-8
Risque lié au manque de fiabilité du système 7-13
Risque lié aux accès 7-13
Risque maîtrisable, définition 6-30
Risque résiduel, définition 4-11, 6-30
Risque(s)
appétence pour le ~ 4-8
définition 3-10
catégories de ~ 7-14
conséquences des ~ 13-33
définitions du ~ 4-5, 5-16
directeur des ~, responsabilités dans le cadre de l'ERM 4-17
élaborer un profil de ~ 5-13
évaluation des ~ 5-25
évaluer la probabilité d'occurrence des ~ 5-14, 13-33
facteurs de ~
combinaison 5-22
définir des facteurs de ~ 5-20
importance relative (poids ou pondération) 5-20
historique de la notion de ~ 4-4
identifier les ~ 12-9, 13-35
impact
estimer la probabilité 8-27
évaluer l'impact 8-27
matrice risques/processus 5-19
propriétaires de ~ 3-15
risque inhérent 4-10
risque maîtrisable, définition 6-30
risque résiduel 4-11, 6-30
tolérance au ~
comprendre la tolérance au ~ 13-35
définition 3-10, 13-33

Copyright © 2015 Eyrolles.

INDEX

traitement des ~ 7-17
définition 8-18
différentes modalités de traitement 4-11, 5-17
vision descendante du ~ 4-23
Risque(s) au niveau du (des) processus
définir les ~ 13-30
évaluation des ~ 13-33
identifier les scenarios de ~ 13-29
Risque(s) de fraude
classification des ~ 8-25
entretien de départ d'un collaborateur 8-33
évaluation des ~ 8-17, 8-29
évaluation des ~ au niveau des processus 13-27
gouvernance du ~ 8-15
identification des ~ 8-27
impact
définition 8-27
évaluation de l'impact 8-27
performances/rémunération, évaluation .. 8-33
plafonnement des transactions autorisées 8-34
probabilité d'occurrence des ~ 8-27, 8-28
définition 8-27
évaluation de la probabilité d'occurrence des ~ 8-27
questions et thèmes de discussion 8-56
traitement du ~ 8-29
Risques de fraude au niveau des processus .. 13-27
Risque SI (matériel ou logiciel) 7-13
Risques opérationnels 5-27, 5-28
utilisation des ~ 5-27, 5-28

S

Sarbanes-Oxley Act de 2002 3-29
obligations de l'auditeur 1-11
obligations du management 6-38
Scepticisme professionnel 8-45, 10-3
définition 8-46, 10-2
Securities Act de 1933 3-27
Securities Exchange Act de 1934 3-27
Seuils de tolérance, comprendre les ~ 13-33
Society of Corporate Compliance and Ethics (SCCE) 2-44
Stratégie, définition 3-5
Structure organisationnelle 4-8
Superviseur 9-13
Supervision directe d'une activité ou d'une fonction 4-12
Systèmes de notation 14-25
Systèmes de rémunération, évaluation 8-33
Systèmes d'information (SI)
audit des ~, sources des lignes directrices relatives 7-31
auditeur interne senior (ou chef de mission) 9-13
auditeurs internes 9-13
compétences dans les ~ 7-27
conscience professionnelle 7-27
conséquences des ~ 7-30
contrôles des ~ 6-37
contrôles physiques et environnementaux des ~, définition 7-21
contrôles relatifs à la gestion des ~ 7-21
contrôles techniques des ~ 7-23
directeur de mission 9-13
environnement interne 7-16
étude de cas 7-43
externalisation des ~ (ou infogérance) 7-28
définition 7-28
facteurs technologiques 4-9
fixation des objectifs 7-17
gouvernance des ~ 7-15
contrôles relatifs à la gouvernance des ~ 7-19
intégration de l'audit des ~ 7-29
normes relatives aux ~ 7-20
opportunités 7-14
questions et thèmes de discussion 7-41
responsabilités relatives aux ~ 7-28
risques SI 7-14
catégories de risques SI 7-14
gestion des risques SI 7-18
problématiques relatives aux SI 7-31
superviseur 9-13
Systèmes experts d'audit 10-14

Copyright © 2015 Eyrolles.

INDEX

T

Tableaux en données relatives, analyse de ~ 10-11

Taille de l'échantillon
- déterminer la ~ 11-10
- déterminer les valeurs appropriées 11-10

Taille de l'échantillon de variables classique, facteurs ayant une incidence sur la ~ 11-24

Taille d'un échantillon, facteurs ayant une incidence sur la ~ 11-8

Taux d'écarts attendu de la population 11-10

Techniques d'audit informatisées 10-6, 10-19
- définition 13-15
- utilisation 13-16

Transparence, améliorer la ~ 2-39

Travail, nature du ~ 2-29

Treadway Commission Report, Rapport de la *National Commission on Fraudulent Financial Reporting* 3-28

Trois lignes de maîtrise 3-19

U

Unité centrale (CPU) 7-5

Unité d'échantillonnage, définir l'~ 11-6

Unités monétaires, échantillonnage par ~ ... 11-23

Univers d'audit, définition 4-28, 9-9

V

Valeur ajoutée 5-3

Valeurs éthiques 4-8

Vérification des transactions *ex ante* 8-34

Y

Yellow Book 2-41