CRIPP - Guide Pratique

ÉVALUER L'ADEQUATION DU MANAGEMENT DES RISQUES EN UTILISANT LA NORME ISO 31000

Décembre 2010





Sommaire

<u>Synthèse</u>	3
Introduction	5
Le management des risques dans l'organisation	7
<u>Gouvernance</u>	7
Responsabilités du management des risques	8
Surveillance et assurance	8
L'audit interne et le management des risques	11
Revue du management des risques par l'audit interne	13
Les activités d'assurance relatives au processus de management des risques	14
Les activités d'assurance relatives aux risques significatifs et aux affirmations du management	14
Le suivi du plan de traitement des risques	15
Obtenir des preuves d'audit	16
Assurance sur le processus de management des risques	19
<u>L'approche par les éléments du processus</u>	19
<u>L'approche par les principes clés</u>	20
<u>L'approche par le modèle de maturité</u>	21
Évaluer la qualité de la documentation portant sur le management des risques	23
Auteurs	24
Relecteurs et contributeurs	24
Réviseurs pour la traduction française	24



Synthèse

De nombreuses organisations s'engagent dans une approche cohérente et globale du management des risques. Celui-ci est considéré comme un processus de pilotage qui doit être pleinement intégré au management de l'organisation et être applicable à tous les niveaux : à un niveau global, au niveau des fonctions et au niveau des unités opérationnelles.

Le cadre organisationnel de management des risques doit être conçu pour s'adapter à l'organisation, c'est-à-dire à son environnement interne et externe. Pour un management des risques efficace, ce cadre devra comporter des éléments incontournables quels que soient la taille et l'objectif de l'organisation. Le présent guide détaille trois manières de donner une assurance sur le processus de management des risques : l'approche processus ; l'approche fondée sur les principes de management des risques et le modèle de maturité. Les activités qui permettent de donner une assurance devront être ajustées aux besoins de l'organisation.

Commentaire IFACI

Les activités d'assurance (« assurance ») permettent d'attester que les opérations et les processus de l'organisation sont conçus, réalisés et maîtrisés conformément aux instructions de ses organes dirigeants et de ses parties prenantes.

Comme indiqué dans la MPA 2050-2, différents prestataires internes ou externes (commissaires aux comptes, auditeurs qualité, auditeurs HSE, animateurs des auto-évaluations, services fonctionnels – DRH, DSI, directions juridiques, responsables de la conformité, risk managers, auditeurs internes, etc.) peuvent fournir une assurance sur la conformité et l'efficacité des dispositifs d'une organisation. Ces prestataires se distinguent en fonction :

- de leur positionnement et donc de leur degré d'indépendance;
- des destinataires de leurs opinions (management opérationnel, direction générale, Conseil, parties prenantes extérieures);
- de la méthode utilisée pour garantir l'objectivité de leurs opinions;
- de leur périmètre d'intervention (métier, zone géo graphique, entité juridique, groupe...).

Parmi ces prestataires, l'audit interne se distingue par son indépendance par rapport aux activités contrôlées. En effet, le positionnement au plus haut niveau de l'organisation donne à l'audit interne une vue d'ensemble des processus et des risques tout en étant un interlocuteur privilégié des instances dirigeantes. Ainsi, selon le glossaire des Normes internationales, les activités d'assurance de l'audit interne se traduisent par un examen objectif d'éléments probants, effectué en vue de fournir une évaluation indépendante des processus de gouvernement d'entreprise, de management des risques et de contrôle.

La prise de position de l'IFACI sur l'urbanisme du contrôle interne illustre les différents niveaux de prestation d'assurance. Dans leurs préconisations pour l'application de l'article 41 de la 8ème directive européenne (Directive 2006/43/CE), l'ECIIA et le Ferma propose l'adoption d'un modèle comportant 3 lignes de défense :

- En tant que première ligne de défense, le management est propriétaire des risques. Il a donc la responsabilité de les évaluer et de les gérer. Il doit rendre compte de ces activités à la direction générale.
- En tant que seconde ligne de défense, le *risk* management (ainsi que les autres fonctions

support telles que la conformité ou la qualité) facilite et surveille la mise en œuvre de la gestion des risques par le management. Il assiste ces propriétaires des risques dans la remontée d'informations adéquates sur les risques à tous les niveaux de l'organisation.

• En tant que troisième ligne de défense, l'audit interne fournit, à partir d'une approche fondée sur les risques, une assurance au Conseil et à la direction générale sur l'efficacité de l'évaluation des risques et sur leur gestion, y compris le fonctionnement de la première et de la seconde ligne de défense. Cette activité d'assurance recouvre tous les éléments du cadre organisationnel de management des risques (identification des risques, évaluation des risques et suites données à ces informations).

Les auditeurs internes devraient utiliser des méthodes d'évaluation de l'efficacité du management des risques dans l'organisation, notamment en examinant des caractéristiques du processus de management des risques. Ces règles doivent être pertinentes, fiables, compréhensibles et exhaustives. La consolidation de ces observations permettra à l'auditeur de déterminer la maturité du management des risques de l'organisation.

Les auditeurs internes doivent en particulier évaluer si le cadre en place est à même de promouvoir une approche globale et systématique du management des risques. La qualité du processus de management des risques s'améliore au fil du temps. En effet, il faut souvent plusieurs années pour instaurer un management efficace des risques et aboutir à un véritable « ERM » (Entreprise Risk Management ou management des risques de l'entreprise).

Ce guide pratique s'appuie sur la norme ISO 31000 « Management du risque, principes et lignes directrices, version 2009 », pour définir le cadre organisationnel de management du risque. D'autres cadres ou référentiels peuvent être utilisés pour l'évaluation des risques. Le présent guide n'implique pas l'adoption implicite ou explicite de la norme ISO 31000 ou de tout autre référentiel.



Introduction

Le management des risques est de plus en plus reconnu comme l'une des composantes essentielles d'une bonne gouvernance. Des pressions s'exercent sur les organisations pour identifier les risques significatifs auxquels elles sont confrontées (les risques sociaux, déontologiques et environnementaux, mais aussi les risques stratégiques, financiers et opérationnels) et expliquer comment elles les gèrent. L'utilisation de cadres de management des risques à l'échelle de toute l'entreprise (ERM) se développe au fur et à mesure que les organisations prennent conscience des avantages d'approches coordonnées.

Le glossaire des Normes internationales pour la pratique professionnelle de l'audit interne (les Normes) définit le management des risques comme « un processus visant à identifier, évaluer, gérer et piloter les événements éventuels et les situations pour fournir une assurance raisonnable quant à la réalisation des objectifs de l'organisation »1. Un cadre complet de management des risques explicite l'enchaînement et les relations entre les objectifs, la stratégie et son déploiement, les risques, les contrôles et le processus d'assurance à tous les niveaux de l'organisation.

On parle couramment de management des risques de l'entreprise (ERM) ou, de façon plus appropriée, de management des risques à l'échelle de l'entreprise. Le COSO (Committee of Sponsoring Organizations of the Treadway Commission) en donne la définition suivante : « 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 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 »2.

Selon la norme ISO 31000 (section 4.1), « le succès du management du risque va dépendre de l'efficacité du cadre organisationnel de management qui fournit les bases et les dispositions permettant son intégration à tous les niveaux de l'organisme³ ». On entend par « cadre de management du risque » les composantes et l'organisation du management du risque au sein d'une entité

La Norme 2120 indique que « l'audit interne doit évaluer l'efficacité des processus de management des risques et contribuer à leur amélioration ». L'interprétation de ce principe est présentée ci-après.

« Interprétation : Afin de déterminer si les processus de management des risques sont efficaces, les auditeurs internes doivent s'assurer que :

¹ Cette définition correspond à celle que donne l'Organisation internationale de normalisation (ISO) : « activités coordonnées dans le but de diriger et piloter un organisme vis-à-vis du risque » (Guide ISO 73, 2009, définition 2.1)

² Le management des risques de l'entreprise – COSO Report II, IFACI - PriceWaterhouseCoopers, octobre 2005 (page 5)

³ © ISO. Extrait soit de la norme ISO 31000:2009, soit du Guide ISO 73:2009, reproduit avec l'aimable autorisation de l'American National Standards Institute (ANSI) pour le compte de l'Organisation internationale de normalisation (ISO). Aucune partie ne peut en être copiée ni reproduite, sous quelque forme que ce soit, avec un système d'extraction électronique, ni autrement mise à disposition sur Internet, un réseau public, par satellite, ou autre, sans l'accord préalable écrit de l'ANSI. On peut se procurer des exemplaires de cette norme auprès de l'ANSI, 25 West 43rd Street, New York, NY 10036, téléphone : (212) 642-4900, http://webstore.ansi.org

- 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. »

Afin d'améliorer le management des risques d'une organisation, il convient, dans un premier temps, de dresser un état des lieux des processus et systèmes en place et de les évaluer. Si des composantes incontournables manquent, il est très peu probable que le management des risques puisse devenir efficace. Les auditeurs internes ont un rôle important à jouer dans l'évaluation et l'amélioration du management des risques au sein de leur organisation, et l'examen des activités de management des risques constitue un pan crucial de ces efforts.

Ce guide pratique reprend la structure et une partie de la terminologie de la norme ISO 31000. Bien que cette dernière n'ait pas vocation à servir de base à une certification, on peut se fonder sur ses concepts et sur ses composantes pour évaluer un processus de management des risques. L'ISO 31000 n'est pas le seul cadre couramment utilisé pour le management des risques, et le présent guide n'implique pas que cette norme soit celle adoptée par l'organisation.



Le management des risques dans l'organisation

Gouvernance

La norme ISO 31000 donne des orientations pour structurer le management des risques (applicables aux organisations de toutes tailles). Elle définit le cadre comme un « ensemble de composantes établissant les fondements et les dispositions organisationnelles nécessaires à la conception, la mise en œuvre, la surveillance, la revue et l'amélioration continue du management du risque dans tout l'organisme⁴ ». Quel que soit son niveau de formalisation, le dispositif de management des risques est intrinsèquement intégré dans les politiques stratégiques et opérationnelles ainsi que dans les pratiques de l'organisation. Les dispositions organisationnelles incluent les projets, les interactions, les responsabilités, les ressources, les processus et les activités. Le diagramme en page 7 (figure 1) présente un modèle conceptuel qui peut être utilisé pour l'analyse de ces dispositions.

L'auditeur interne détermine si le cadre prend en compte et définit les responsabilités et la stratégie adoptée en termes de management des risques. Il s'assure également que le dispositif en place favorise le développement d'un environnement et d'une culture du risque auprès des collaborateurs, tout en permettant une prise de risque responsable et l'innovation.

⁴ Ibid.

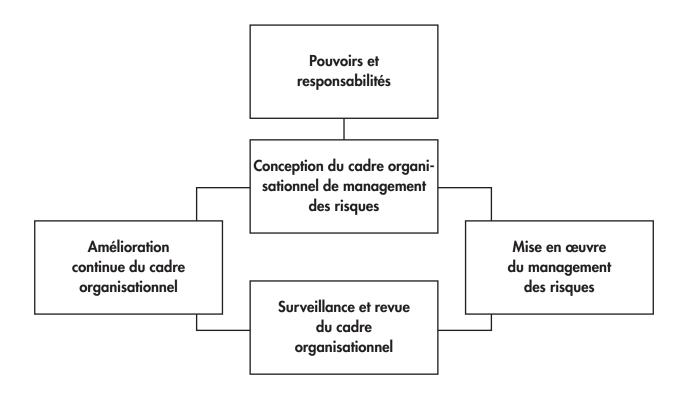


Figure 1 – Cadre organisationnel de management du risque (ISO 31000)

Responsabilités du management des risques

L'Organisation internationale de normalisation (ISO) définit l'attitude face au risque comme « l'approche d'un organisme pour apprécier un risque avant, éventuellement, de saisir ou préserver une opportunité ou de prendre ou rejeter un risque⁵ ». C'est à la direction générale qu'il appartient de définir l'attitude de l'organisation face au risque, et au Conseil de déterminer si cette attitude coïncide avec les intérêts des actionnaires

Les organes de surveillance assurent la gouvernance globale du management des risques en ayant une bonne compréhension des principaux éléments de l'ERM; ils demandent et obtiennent, de la part de la direction générale, des informations sur les risques et valident certaines décisions. Il convient de donner aux actionnaires des informations suffisantes pour qu'ils comprennent l'attitude de la direction générale et du Conseil face au risque, de manière à investir en tenant compte de leurs tolérances vis-à-vis de variations potentielles des résultats. Les organisations font état de leurs niveaux de risque dans des rapports trimestriels et annuels, des communiqués de presse, des notes aux investisseurs, etc.

Le Conseil a la responsabilité globale de s'assurer que les risques sont gérés et qu'un système adéquat de management des risques est en place. Dans la pratique, le Conseil délègue la mise en œuvre du management des risques à l'équipe de direction. Il se peut qu'une fonction dédiée, qui dispose de compétences et de connaissances spécialisées, coordonne et gère ces activités. Néanmoins, chaque membre de l'organisation contribue au succès de l'ERM, et la responsabilité de l'identification et de la gestion des risques revient en premier lieu au management.

Surveillance et assurance

La mise en œuvre de l'ERM évolue au fil du temps. L'attitude face au risque peut évoluer sous l'effet de facteurs internes ou externes, certaines réactions face au risque peuvent perdre de leur pertinence, ou certaines activités de contrôle devenir moins efficaces ou cesser d'être déployées. Des changements peuvent être occasionnés par l'arrivée de nouveaux collaborateurs, des restructurations d'entités ou l'introduction de nouveaux processus. De plus, les objectifs de l'entité, ainsi que la nature des événements potentiels ou des situations susceptibles d'influer sur la réalisation de ces objectifs, évoluent également. Le management doit donc périodiquement déterminer si les composantes de l'ERM restent pertinentes et aptes à faire face aux nouveaux risques.

L'élément essentiel d'un bon système de management du risque est la surveillance, visant à s'assurer que ce système fonctionne comme prévu. La surveillance peut être permanente ou consister en des évaluations spécifiques. La combinaison de ces deux modes de surveillance permettra de vérifier que l'ERM reste efficace dans la durée.

Les processus de management des risques incluent une évaluation et une cotation périodique des risques. Plus





⁵ © ISO. Extrait soit de la norme ISO 31000:2009, soit du Guide ISO 73:2009, reproduit avec l'aimable autorisation de l'American National Standards Institute (ANSI) pour le compte de l'Organisation internationale de normalisation (ISO). Aucune partie ne peut en être copiée ni reproduite, sous quelque forme que ce soit, avec un système d'extraction électronique, ni autrement mise à disposition sur Internet, un réseau public, par satellite, ou autre, sans l'accord préalable écrit de l'ANSI. On peut se procurer des exemplaires de cette norme auprès de l'ANSI, 25 West 43rd Street, New York, NY 10036, téléphone : (212) 642-4900, http://webstore.ansi.org

la surveillance permanente est poussée et efficace, moins les évaluations spécifiques sont susceptibles d'être nécessaires. C'est au management de décider de la fréquence des évaluations spécifiques qui lui permettront d'obtenir une assurance raisonnable sur l'efficacité de l'ERM. Pour déterminer cette fréquence, le management doit prendre en considération la nature et l'ampleur des changements, la compétence et l'expérience des personnes qui mettent en œuvre les traitements du risque et les contrôles connexes, la nature des risques gérés et leur importance pour l'activité, ainsi que les résultats de la surveillance permanente.

La surveillance permanente est intégrée aux activités opérationnelles usuelles et récurrentes d'une entité. Elle peut se révéler plus efficace que les évaluations spécifigues car c'est une surveillance en temps réel, qui s'adapte et permet de réagir immédiatement à l'évolution de l'environnement, et qui est ancrée dans l'entité. C'est souvent la surveillance permanente qui permet de détecter le plus rapidement des problèmes alors que les évaluations spécifiques interviennent généralement a posteriori. Les entités dont les activités de surveillance permanente sont fiables, procèdent néanmoins à une évaluation spécifique de l'ERM ou de certains aspects. Le niveau d'objectivité perçu est plus élevé pour les évaluations indépendantes (voir précédemment dans le texte) que pour l'auto-surveillance.

Une entité qui perçoit la nécessité de procéder fréquemment à des évaluations indépendantes doit s'attacher à améliorer ses activités de surveillance permanente et, donc, à les renforcer plutôt qu'à en ajouter de nouvelles.

Ce sont les processus de gouvernance de l'organisation qui déterminent le besoin d'assurance. Il trouve son origine dans les pouvoirs et les responsabilités respectives du Conseil et des autres parties prenantes de l'organisation. Les instances de gouvernance trouvent dans leur mandat la légitimité pour mettre en place les processus pertinents de délégation et de limitation des pouvoirs. Ainsi, ils pilotent et déploient la stratégie dans une perspective de succès à long terme de l'organisation. Les processus d'assurance permettent notamment au Conseil de surveiller le bon exercice de ces délégations.

L'audit interne apporte une assurance sur l'ensemble du processus de management des risques. Cette assurance porte notamment sur la gestion du risque (tant du point de vue de sa conception que de son efficacité opérationnelle), sur le management des risques répertoriés comme risques « majeurs » (en incluant l'efficacité des contrôles et les autres traitements du risque, etc.), sur la vérification de la rigueur et de la fiabilité des évaluations des risques, ainsi que sur les remontées d'informations relatives au statut des risques et aux contrôles qui leur sont associés.

La responsabilité des activités de surveillance et d'assurance étant traditionnellement répartie entre différents intervenants, dont le management opérationnel, l'audit interne, les spécialistes du risk management et les fonctions de conformité, il importe de les coordonner de manière à ce que l'utilisation des ressources soit la plus efficiente et la plus efficace possible. Une organisation comporte souvent plusieurs groupes distincts qui exercent, indépendamment les uns des autres, différentes fonctions de conseil, de conformité ou d'assurance liées au management des risques. Une coordination et une information inefficaces peuvent générer des doublons ou empêcher la détection ou l'évaluation appropriée de risques majeurs.

D'après la Norme 2050, le responsable de l'audit interne devrait coordonner ses activités avec ceux des autres prestataires d'assurance. La cartographie des



services d'assurance peut l'aider dans cette tâche, car c'est un outil efficace pour gérer cette coordination et en rendre compte. On trouvera dans la Modalité pratique d'application 2050-2 des informations sur cette cartographie.



L'audit interne et le management des risques

La Norme 2100 dispose que « 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 ». La plupart du temps, l'audit interne a pour rôle de donner au Conseil une assurance indépendante et objective sur l'efficacité des activités de l'ERM. Cette approche permet de garantir que les risques majeurs des activités sont gérés de façon appropriée, et que le système de contrôle interne de l'organisation est efficace et efficient.

Le management des risques est un processus managérial qui favorise l'atteinte des objectifs de l'organisation au meilleur rapport coût-efficacité; les activités d'assurance apportent des informations fiables sur les résultats du management des risques. L'audit interne et le management des risques sont donc des processus complémentaires.

Pour soutenir le processus de management des risques, il convient que l'audit interne et les autres prestataires de services d'assurance indépendants évaluent si :

- le processus de management des risques est mis en œuvre de façon appropriée et si tous ses éléments sont adéquats et suffisants;
- le processus de management des risques est en adéquation avec les orientations et les besoins stratégiques de l'organisation. ;
- tous les risques significatifs ont été identifiés et sont traités ;
- les contrôles ont été correctement conçus et répondent aux objectifs du processus de management du risque;
- les contrôles critiques sont adéquats et efficaces ;
- la revue effectuée par la direction opérationnelle et les autres activités d'assurance hors audit interne

- permettent le maintien et l'amélioration des contrôles existants :
- les plans de traitement des risques sont exécutés ;
- le plan de management des risques prévoit un suivi approprié et documenté des avancées.

Pour soutenir le processus d'assurance, le processus de management des risques :

- définit un cadre de management des risques documenté et spécifique à l'organisation;
- fournit une analyse structurée des risques de l'organisation, en présentant :
 - le ou les objectifs organisationnels et les risques qui y sont associés,
 - les expositions potentielles et les évaluations des risques actuels,
 - les propriétaires de la gestion de chaque risque,
 - les principaux systèmes de contrôles mis en place pour gérer chaque risque.

Il est fréquent que l'audit interne travaille en étroite coopération avec la fonction de management des risques. Si cette fonction n'est pas dédiée, il arrive souvent que l'audit interne fournisse un plus large éventail de services de conseil relatifs au management des risques. L'audit interne peut apporter ce type de services sous certaines conditions :

- Les managers doivent clairement rester responsables du management des risques. Lorsque l'audit interne les consulte pour mettre en place ou améliorer des processus de management des risques, son plan de travail inclura une stratégie et un calendrier bien définis pour transférer la responsabilité de ces activités au management.
- L'audit interne ne peut pas donner une assurance objective sur toute partie du management des

- risques dont il est chargé. Cette assurance doit être apportée par d'autres intervenants qualifiés.
- Les services fournis à ce titre doivent être énoncés dans la charte d'audit interne et ne pas être en contradiction avec les autres responsabilités de l'audit interne.
- L'audit interne ne prend aucune décision relative au management des risques quels que soient les conseils ou les avis qu'il donne sur les décisions prises par le management.

La prise de position de l'IIA intitulée « Le Rôle de l'audit interne dans le management des risques de l'entreprise » comporte le diagramme en éventail ci-après (figure 2). Ce diagramme illustre différentes activités de l'ERM et montre quels rôles une fonction d'audit interne professionnelle devrait ou ne devrait pas endosser.

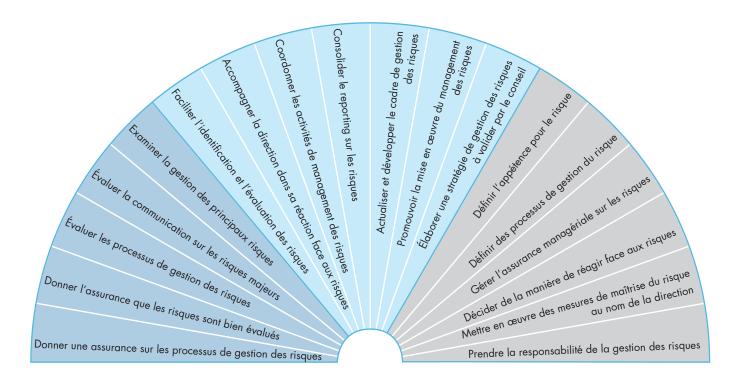


Revue du management des risques par l'audit interne

Dans les domaines à risque les plus élevés, pour lesquels le management a admis la nécessité d'améliorer les contrôles, l'audit interne peut ajouter de la valeur par des activités de conseil. La partie centrale de la figure 2 présente les activités de conseil qui peuvent être fournies au niveau d'une entité ou d'une unité opérationnelle/d'un département en préservant l'indépendance et l'objectivité de l'audit interne.

Même si ces activités de conseil peuvent constituer une composante utile du plan d'audit, le présent guide pratique est axé sur les activités d'assurance qui apparaissent dans la partie gauche de la figure 2, et que l'on peut classer en trois grandes catégories :

- Assurance sur le processus de management des risques.
- Assurance sur les risques significatifs et sur les affirmations du management.
- Suivi des progrès du plan de traitement des risques.



Principaux rôles de l'audit interne dans le processus de management des risques Rôles légitimes de l'audit interne, sous réserve de prendre les précautions nécessaires Rôles que l'audit interne ne doit pas jouer

Figure 2 - Rôle de l'audit interne dans l'ERM

Les activités d'assurance relatives au processus de management des risques

L'audit interne du processus de management des risques donne à la direction générale et au Conseil l'assurance raisonnable que le programme de management des risques est correctement conçu, documenté et mis en œuvre pour permettre la réalisation des objectifs de l'organisation. Cette assurance peut notamment permettre de répondre aux questions suivantes :

- Le programme de management des risques bénéficie-t-il d'un engagement adéquat de la part du management de l'organisation, notamment d'un statut et de ressources en rapport avec les risques, et constitue-t-il une composante appropriée des processus organisationnels et de prise de décision ?
- La conception du cadre organisationnel de management des risques et les critères d'évaluation des risques sont-ils adaptés au contexte interne et externe de l'organisation?
- Existe-t-il une définition et une communication adéquates des exigences, des critères d'évaluation des risques et des responsabilités concernant l'élaboration, la mise en œuvre et l'actualisation du cadre organisationnel de management des risques ainsi que des évaluations de domaines de risque spécifiques?
- L'attitude face au risque est-elle décidée au niveau approprié dans la structure de gouvernance de l'organisation?
- Les mécanismes de communication et d'information internes permettent-ils la diffusion appropriée des principaux résultats des activités relatives au management des risques au sein de l'organisation (en conciliant transparence et caractère sensible)?
- Les rapports aux parties prenantes reflètent-ils de façon adéquate l'attitude de l'organisation face aux risques et leur traitement?

ifaci

- Les mécanismes de communication et d'information externes permettent-ils de se conformer à la législation, à la réglementation, aux principes de gouvernement d'entreprise et aux règles relatives à l'information des actionnaires?
- Existe-t-il des mécanismes adéquats de mesure des performances et de remontée d'informations, permettant de surveiller la conception et l'efficacité du cadre organisationnel de management des risques?
- Les critères d'évaluation des risques, le niveau d'appétence pour les risques, les réponses aux risques et la remontée de l'information sont-ils appliqués uniformément dans toute l'organisation ? Des personnes, disposant des connaissances appropriées, sont-elles responsables de l'identification des risques ? La maturité en matière d'identification des risques est-il adéquate?
- Le cadre de management des risques ainsi que les processus et les contrôles associés sont-ils mis à jour lorsque les activités et les besoins organisationnels évoluent?
- Les personnes responsables de l'analyse, de l'évaluation et du traitement /des réponses aux risques disposent-elles des connaissances appropriées ? Ces activités font-elles l'objet d'une revue et d'une validation adéquates?
- Les plans de traitement des risques sont-ils suivis et communiqués de manière adéquate aux niveaux appropriés de la direction générale et du Conseil ?

Les activités d'assurance relatives aux risques significatifs et aux affirmations du management

Pour tous les autres travaux d'assurance dont le périmètre concerne les risques de niveaux d'exposition importants (identifiés dans le cadre d'un processus de



management des risques de l'organisation), les procédures et les communications de l'audit interne devraient être conçues pour évaluer les affirmations du management concernant l'efficacité des contrôles et leur capacité à réduire le risque à un niveau tolérable pour l'organisation.

Les rapports à la direction générale (et au Conseil) peuvent décrire l'exposition potentielle, et l'évaluation du management (y compris la qualité des contrôles en place) des risques actuels ainsi que l'évaluation des risques par l'audit interne. Chaque écart est pris en compte dans le processus de management des risques.

L'effet cumulatif des activités portant sur des domaines de risque spécifiques et réalisées dans le cadre d'un plan d'audit fondé sur les risques permettra de fournir une assurance non seulement sur ces domaines de risque spécifiques mais également sur l'efficacité du processus global de management des risques.

Le suivi du plan de traitement des risques

Dans le cas d'une exposition potentielle plus importante, il peut être approprié d'assurer le suivi de l'efficacité de la mise en œuvre des plans de traitement et de contrôle des risques, surtout si ces plans sont à long terme. Cette surveillance est, a minima, conçue pour communiquer au management une évaluation des avancées par rapport aux jalons définis et pour valider l'état d'avancement des plans de traitement des risques présentés au Conseil.

De plus, cette surveillance peut consister à évaluer la structure des plans, les ressources, les responsabilités, la gestion de projets, etc... Elle donne lieu à des recommandations et à des remarques visant à améliorer la probabilité de succès des plans.



Obtenir des preuves d'audit

Concernant les audits du processus de management des risques d'une organisation, la Modalité pratique d'application 2120-1, Évaluer la pertinence des processus de management des risques, paragraphe 8, indique :

- « Afin de se forger une opinion sur l'adéquation des processus de management des risques, les auditeurs internes devront disposer d'éléments suffisamment probants et appropriés pour avoir l'assurance que les principaux objectifs de ces processus sont bien remplis. Pour recueillir ces éléments, l'auditeur interne peut recourir aux procédures d'audit décrites ci-après :
- rechercher et analyser des informations sur le secteur d'activité de l'organisation, l'évolution récente et les tendances, ainsi que toute autre source d'information appropriée, afin de déterminer les risques susceptibles d'affecter l'organisation et les procédures de contrôle utilisées pour gérer, suivre et réévaluer ces risques;
- examiner les règles de l'entreprise ainsi que les procès-verbaux des délibérations du Conseil et du comité d'audit afin de déterminer les stratégies de l'organisation, son approche du management des risques, son appétence pour le risque et son acceptation des risques;
- examiner les rapports d'évaluation des risques précédemment établis par le management, les auditeurs internes ou externes et par tout autre intervenant :
- organiser des entretiens avec l'encadrement opérationnel et leur direction afin de déterminer les objectifs de chaque branche d'activité, les risques correspondants, et les mesures de suivi, de contrôle et d'atténuation des risques prises par le management;
- recueillir des informations afin d'évaluer, en toute indépendance, l'efficacité du processus de suivi, de

- communication et d'atténuation des risques, et des activités de contrôle correspondantes ;
- déterminer si les informations ou rapports relatifs au suivi des risques sont adressés au niveau hiérarchique approprié;
- vérifier si les rapports concernant les résultats du management des risques sont diffusés selon des modalités et dans des délais appropriés;
- s'assurer du caractère exhaustif de l'analyse des risques effectuée par le management et des mesures prises pour résoudre les points soulevés dans le cadre du processus de management des risques, et proposer des améliorations;
- apprécier l'efficacité du processus d'auto-évaluation mis en œuvre par le management, au moyen d'observations et de tests sur les procédures de suivi et de contrôle testant l'exactitude des informations utilisées dans le cadre des opérations de suivi, et par d'autres techniques appropriées;
- examiner les signes de faiblesse éventuels du dispositif de management des risques et, le cas échéant, les analyser avec la direction générale et le Conseil.
 S'il estime que le management a accepté un niveau de risques non compatible avec la stratégie et les procédures de l'organisation en matière de management des risques, ou jugé inacceptable pour l'organisation, l'auditeur se réfèrera à la Norme 2600 relative à l'acceptation des risques par le management et aux lignes directives correspondantes pour des orientations complémentaires.

Différentes techniques permettent d'obtenir des preuves d'audit, notamment :

 les observations, par exemple en étant présent lorsque des activités relatives au management des risques sont conduites aux différents échelons de l'organisation; au niveau des organes dirigeants et



jusqu'aux différents départements, programmes, projets et collaborateurs;

- les entretiens ;
- l'examen de documents, par exemple des ordres du jour, des documents de travail et des procèsverbaux, émanant notamment du conseil, de la direction générale et d'autres comités de la direction générale, des plans stratégiques ou des documents d'aide aux décisions relatives aux ressources:
- les résultats des audits antérieurs ;
- les travaux réalisés par des tiers ;
- les techniques analytiques, par exemple l'analyse causale (root cause analysis) des défaillances détectées ;
- la cartographie des processus;
- l'analyse statistique, par exemple, l'analyse des types d'incidents ou de quasi-incidents (near-misses).
- l'analyse et l'évaluation des modèles de risques ;
- les enquêtes;
- l'analyse des auto-évaluations du contrôle interne.

Souvent, on utilisera une combinaison de plusieurs techniques d'audit afin de rassembler des informations et preuves d'audit suffisantes pour aboutir à une conclusion. L'auditeur choisit la procédure la mieux appropriée compte tenu de l'objectif de sa mission. Il détermine également si les ressources et les compétences requises sont disponibles pour effectuer tous les travaux nécessaires à l'obtention d'une opinion suffisamment étayée. Si tel n'est pas le cas, l'auditeur doit se demander s'il ne serait pas prudent soit de refuser d'exprimer une opinion, soit d'assortir cette opinion de réserves en excluant certains domaines ou risques de l'univers sur lequel porte l'opinion.

Les preuves d'audit nécessaires diffèrent suivant le type d'avis que l'auditeur souhaite rendre. C'est l'assurance affirmative qui apporte le niveau d'assurance le plus élevé et qui requiert également le plus de preuves d'audit pour étayer l'opinion. A titre d'exemple, une telle opinion indique non seulement si les contrôles/processus d'atténuation des risques sont adéquats et efficaces, mais donne également une assurance raisonnable que, si des preuves du contraire existaient, elles auraient été identifiées.

L'assurance négative n'apporte pas un niveau d'assurance aussi important et ne nécessite donc pas autant de preuves d'audit. Lorsque l'auditeur rend une assurance négative, il affirme, par exemple, que, sur la base des travaux effectués, aucun point n'a attiré son attention. En rendant ce type d'opinion, l'auditeur n'endosse aucune responsabilité quant au caractère suffisant du champ et des procédures d'audit pour déceler tous les problèmes significatifs. Une telle opinion a généralement moins de valeur qu'une assurance positive.

On trouvera des recommandations plus complètes sur les opinions dans le Guide pratique « Formuler et exprimer une opinion d'audit ».

Les conclusions d'audit doivent être factuelles, objectives et reposer sur des preuves d'audit suffisantes. Les preuves d'audit sont suffisantes lorsqu'elles sont documentées, adéquates et concluantes, de sorte qu'une personne prudente et informée pourrait parvenir aux mêmes conclusions que l'auditeur. Les preuves d'audit doivent être correctement documentées et organisées.

Le service d'audit ne doit pas donner, sans le savoir, de fausse assurance (cf. MPA 2120-2 : Évaluer la perti-

nence des processus de management des risques, paragraphe 8). La « fausse assurance » est un niveau de confiance ou d'assurance qui se fonde sur des perceptions ou des hypothèses plutôt que sur des faits. Dans de nombreux cas, la simple intervention de l'audit interne dans un domaine peut aboutir à donner une fausse assurance. Le champ de la participation de l'audit interne peut être mal interprété et il peut s'en suivre une fausse assurance.



Assurance sur le processus de management des risques

Un organe de direction doit être à même de déterminer dans quelle mesure le processus de management des risques en place dans son organisation répond aux besoins de cette dernière et respecte les bonnes pratiques généralement acceptées. La gestion des risques étant une composante cruciale du dispositif de contrôle interne, une lacune dans les processus de management des risques indiquerait que le système de contrôle interne de l'organisation est déficient.

Il est important pour une organisation d'obtenir une assurance sur son processus de management des risques. Il faut que cette assurance tienne compte du fait que l'auditeur interne n'est peut-être pas indépendant de la fonction *risk management*. Dans ce cas, on pourra faire appel à une tierce partie pour obtenir une telle assurance.

Pour évaluer un processus de management du risque, on peut recourir aux trois formes d'assurance suivantes⁶:

- Approche par les éléments du processus.
- Approche par les principes clés.
- Approche par le modèle de maturité.

Chaque approche se suffit à elle-même, mais chacune apporte une perspective différente sur l'efficacité d'un processus de management des risques dans une organisation. Souvent, c'est en retenant non pas une mais plusieurs approches que l'on obtient les résultats les plus riches d'enseignements et les plus utiles. Le proces-

⁶ Ces approches sont extraites de HB158: 2010 Delivering assurance based on ISO 31000:2009 Risk management – Principles and guidelines, une publication conjointe de Standards Australia, IIA-Australia et de l'IIA Research Foundation. HB158 propose une analyse plus approfondie sur ces questions, entre autres.

sus de management des risques doit être défini en fonction de l'organisation, de sa taille, de sa culture, de ses objectifs et de son profil de risque. Par conséquent, le processus d'assurance doit lui aussi être défini en fonction des besoins de l'organisation.

Il convient de valider les résultats de toute analyse théorique en examinant si, en pratique, le cadre de management du risque fonctionne efficacement. Autrement dit, ce type d'activité d'assurance ne doit pas être mené isolément et doit toujours accompagner ou associer les activités classiques d'assurance fondée sur le contrôle :

- si les risques sont efficacement identifiés et correctement analysés ;
- si un traitement des risques et un contrôle adéquats et appropriés sont en place ;
- si la direction procède à une surveillance et à un examen efficaces pour détecter les changements dans les risques et les contrôles.

Approche par les éléments du processus

Cette approche permet de vérifier que chaque élément du processus de management des risques est en place. Il est crucial de valider les intentions de la direction générale au moyen de preuves d'audit suffisantes pour confirmer que l'élément concerné est satisfaisant en pratique. Rares sont les cas où les seules affirmations du management pourraient être considérées comme suffisantes. La norme ISO 31000 identifie sept composantes du processus de management du risque :

• Élément 1 – Communication et concertation : Un management du risque sain nécessite une communication et une consultation structurées et régulières avec ceux qui sont concernés par les opérations de l'organisation et au sein du secteur d'activité.



- <u>Élément 2 Établissement du contexte :</u> Il faut comprendre l'environnement externe (politique, social, etc.) et interne (objectifs, stratégies, structures, déontologie, discipline, etc.) de l'organisation ou de l'activité avant de pouvoir identifier toute la gamme des risques.
- <u>Élément 3 Identification du risque :</u> L'identification des risques doit être un processus formel et structuré qui tient compte des sources de risque, des domaines d'impact, des événements ainsi que de leurs causes et conséquences potentielles.
- Élément 4 Analyse du risque : L'organisation doit recourir à une technique formalisée pour prendre en compte les conséquences de chaque risque et leur probabilité de survenance.
- <u>Élément 5 Évaluation du risque :</u> L'organisation dispose d'un mécanisme permettant de classer les risques en fonction de leur importance relative, de façon à déterminer l'ordre de priorité dans la mise en œuvre des traitements.
- Élément 6 Traitement du risque : Un bon management du risque requiert des décisions rationnelles concernant le traitement des risques. Classiquement, ce traitement consiste à éviter l'activité qui induit le risque, à partager le risque, à maîtriser le risque au

- moyen de contrôles ou à accepter le risque et ne pas prendre de mesure supplémentaire.
- Élément 7 Surveillance et revue : La surveillance consiste à vérifier l'avancement de la mise en œuvre des plans de traitement des risques, à surveiller les contrôles et leur efficacité, à s'assurer que les activités proscrites sont évitées et à vérifier que le contexte n'a pas évolué d'une façon qui a une incidence sur les risques.

L'approche par les principes clés

Cette approche repose sur l'idée que, pour être pleinement efficace, tout processus de management du risque doit respecter un minimum de principes ou de caractéristiques. La norme ISO 31000 y consacre un chapitre. Un audit reposant sur cette approche évalue dans quelle mesure ces principes se vérifient pour le processus de management du risque de l'organisation:

- Le management du risque crée de la valeur et la préserve⁷. Il s'ensuit que plus la valeur en jeu est élevée, plus la gestion des risques doit être rigoureuse. Il s'ensuit également que l'organisation dispose de différentes techniques, correspondant à différents niveaux d'exposition.
- Le management du risque est intégré aux processus organisationnels⁸. Le management du risque ne doit pas être perçu comme une tâche supplé-
- Le management du risque est intégré au processus de prise de décision⁹. Plus la décision est importante, plus ce lien doit être explicite.
- Le management du risque traite explicitement de **l'incertitude**¹⁰. On attend des évaluations des risques qu'elles documentent les zones d'incertitude



⁷ © ISO. Extrait soit de la norme ISO 31000:2009 soit du Guide ISO 73:2009, reproduit avec l'aimable autorisation de l'American National Standards Institute (ANSI) pour le compte de l'Organisation internationale de normalisation (ISO). Aucune partie ISO ne peut en être copiée ou reproduite sous quelque forme que ce soit, avec un système d'extraction électronique ni autrement mise à disposition sur Internet, un réseau public, par satellite, ou autre, sans l'accord préalable écrit de l'ANSI. On peut se procurer des copies de cette norme auprès de l'ANSI, 25 West 43rd Street, New York, NY 10036, téléphone : (212) 642-4900, http://webstore.ansi.org

⁸ Ibid. 9 Ibid. 10 Ibid.

et déterminent comment remédier au mieux à l'incertitude identifiée.

- Le management du risque est systématique, structuré et utilisé en temps utile11.
- Le management du risque s'appuie sur la meilleure information disponible¹². L'obtention d'informations peut se révéler onéreuse et le processus doit donner des indications sur ce qui peut être considéré comme des informations suffisantes.
- Le management du risque est adapté¹³. Il ne s'agit pas d'un processus prêt à l'emploi : il doit être adapté en fonction des activités de l'organisation.
- Le management du risque prend en compte les facteurs humains et culturels¹⁴. Les processus doivent être adaptés à la compétence et à la culture des utilisateurs.
- Le management du risque est transparent et participatif¹⁵. La participation adéquate et en temps opportun des parties prenantes est nécessaire.
- Le management du risque est dynamique, itératif et réactif au changement¹⁶. Le processus doit être régulièrement examiné et adapté aux changements dans l'organisation et dans son environnement, de sorte qu'il reste pertinent.
- Le management du risque facilite l'amélioration **continue de l'organisme**¹⁷. Le management du risque doit gagner en maturité parallèlement aux processus de l'organisation.

L'approche par le modèle de maturité

L'approche par le modèle de maturité part du postulat de l'amélioration continue de la qualité du management des risques d'une organisation. Les systèmes de management des risques immatures ont un rendement très faible par rapport à l'investissement qui y a été consacré et sont souvent considérés comme des coûts de mise en conformité ou comme un poste obligatoire, qui vise davantage à rendre compte des risques qu'à y remédier efficacement. Les processus de management des risques efficaces sont construits progressivement, chaque étape du processus de maturité apportant une valeur additionnelle. L'approche par le modèle de maturité permet d'évaluer le processus de management des risques de l'organisation sur la courbe de maturité, de sorte que le Conseil et la direction générale peuvent juger s'il répond aux besoins de l'organisation et s'il se développe comme prévu.

Un aspect crucial de l'approche par le modèle de maturité est la mise en relation de la performance et des progrès du management des risques concernant l'avancement dans l'exécution du plan de management du risque, et d'un système de mesure et de management des performances. Les résultats ainsi obtenus peuvent être présentés à la direction générale et au Conseil comme des preuves de l'amélioration du management des risques. Un tel système se compose généralement des éléments suivants :

- Des règles de fonctionnement, tenant compte des approches du management des risques en vigueur et anticipant les besoins stratégiques à venir. Les règles de fonctionnement s'appuient généralement sur une liste de d'exigences détaillées à l'aune desquelles tout progrès dans la mise en œuvre pourra être mesuré.
- Un guide sur la manière concrète de respecter les règles et les exigences associées.
- Un moyen de mesurer les performances effectives au regard de chaque règle et de chaque exigence.





¹¹ Ibid. ¹² Ibid. ¹³ Ibid. ¹⁴ Ibid. ¹⁵ Ibid.

¹⁶ Ibid. 17 Ibid.

- Un moyen d'enregistrer les performances et les progrès et d'en rendre compte.
- La vérification périodique indépendante de l'autoévaluation effectuée par le management.

Les « principes » pratiques et essentiels détaillés dans l'ISO 31000 doivent constituer le point de départ de toute évaluation de la maturité. Ces principes s'intéressent non seulement à la question « cet élément du processus ou du système existe-t-il ? » mais ils permettent également de savoir si l'élément concerné est « efficace et pertinent pour l'organisation ? » et si l'élément concerné « est créateur de valeur ? ». En réalité, le principe fondamental est que le management des risques doit créer de la valeur.

L'évaluation des performances effectives est réalisée au regard de chaque règle de fonctionnement au moyen d'un système de mesure de la maturité en fonction des intentions, mais n'accorde la meilleure note que dans le cas d'une mise en œuvre complète et d'une application effective de la règle. Le tableau ci-dessous présente un modèle envisageable pour mesurer la maturité (d'après le concept original du Capability Maturity Model développé par la Carnegie Mellon University).

NIVEAU DE MATURITÉ	NUL	TRÈS FAIBLE	FAIBLE	BON	COMPLET
Signification	Très peu voire pas de confor- mité avec les exigences.	Une conformité limitée avec les exigences. Le management soutient le prin- cipe d'un mana- gement des risques, mais en pratique, l'appli- cation des règles est médiocre.	Conformité limitée à l'énoncé des éléments. Adhésion au principe mais conformité limitée en pratique.	Le manage- ment souscrit totalement au principe, mais, en pratique, la conformité n'est que partielle.	Conformité totale à l'énoncé des éléments- en principe et en pratique, à tout moment et partout.

Figure 3 – Modèle de maturité – source : HB158





Évaluer la qualité de la documentation portant sur le management des risques

L'ampleur de la documentation du management des risques de l'entreprise (ERM) variera en fonction de la taille et de la complexité de l'entité. Les grandes organisations disposent généralement de manuels de procédures, de diagrammes formels, de descriptifs de postes, d'instructions opérationnelles, de diagrammes de flux des systèmes d'information, etc. Les organisations plus petites, moins complexes, disposent habituellement d'une documentation beaucoup plus restreinte.

De nombreux aspects de l'ERM peuvent être informels et ne pas être documentés, mais être néanmoins mis en œuvre régulièrement et être très efficaces. Ils peuvent être testés de la même manière que les activités documentées. Le fait que des éléments de l'ERM ne soient pas documentés ne signifie pas nécessairement qu'ils ne sont pas efficaces ou ne peuvent être évalués. Toutefois, un niveau adéquat de documentation rend la surveillance plus efficace, et présente aussi d'autres avantages : il permet aux collaborateurs de comprendre plus facilement le fonctionnement du processus et leurs rôles spécifiques, et simplifie la réalisation de modifications, si besoin est.

Pour décider de documenter le processus d'évaluation lui-même, l'auditeur interne s'appuiera généralement sur la documentation existante des processus de management des risques. Le plus souvent, la documentation existante sera complétée par des documents additionnels préparés par l'auditeur, notamment des preuves des tests et des analyses réalisés au cours du processus d'évaluation. La nature et l'ampleur de la documentation sont normalement plus importantes lorsque les affirmations concernant l'ERM sont destinées à d'autres parties.

Lorsque la direction générale se prononce, vis-à-vis de tiers, sur l'efficacité de l'ERM, elle devrait envisager de produire et de conserver une documentation étayant cette déclaration. L'auditeur interne devrait alors se demander:

- si une stratégie de gestion des informations sur les risques concerne toutes les sources d'informations possibles. et si cette stratégie est en place ;
- si les infrastructures nécessaires à la communication des informations sur les risques sont en place;
- s'il existe des définitions communes ;
- s'il existe des recommandations concernant la création, la suppression et le partage des informations sur les risques ;
- si des ressources adéquates sont allouées ;
- si la technologie est rentable et utilisée à propos;
- si la surveillance est proactive;
- si les informations sur les risques sont intégrées dans le processus de planification ;
- si les informations sur les risques sont intégrées aux informations sur les performances.

Il convient de documenter ces éléments et toute décision visant à mettre en œuvre des activités/processus. Cette documentation pourra se révéler utile si la déclaration concernée est, par la suite, remise en cause.

Auteurs

Andrew MacLeod, CIA Patricia A. MacDonald Benito Ybarra, CIA Trygve Sorlie, CIA, CCSA Brian Foster, CIA Teis Stokka, CIA

Relecteurs et contributeurs

Douglas J. Anderson, CIA Steven E. Jameson, CIA, CCSA, CFSA James A. Rose, III, CIA

Réviseurs pour la traduction française

Marie-Elisabeth Albert, CIA, Groupe La Poste José Bouaniche, CIA, Caisse des dépôts Christophe Butikofer, CIA, SFR Pierre Drouard, CIA, Renault Benoît Harel, CIA, IFACI Certification Béatrice Ki-Zerbo, CIA, IFACI Jacques Renard, Consultant



À PROPOS DE L'IIA

Fondé en 1941, *The Institute of Internal Auditors* (IIA) est une organisation professionnelle internationale dont le siège mondial se situe à Altamonte Springs, en Floride, aux États-Unis. L'*Institute of Internal Auditors* est la voix mondiale, une autorite reconnue, un leader inconteste et le principal defenseur de la profession d'auditeur interne. C'est egalement un acteur de premier plan pour la formation des auditeurs internes. Il est represente en France par l'IFACI.

À PROPOS DES GUIDES PRATIQUES

Les guides pratiques détaillent la réalisation des activités d'audit interne. Ils contiennent des processus et des procédures, tels que les outils et techniques, les programmes et les approches pas-à-pas, et donnent des exemples de livrables. Les guides pratiques s'inscrivent dans le Cadre de référence international des pratiques professionnelles de l'audit interne de l'Institute of Internal Auditors. Ces guides pratiques relèvent de la catégorie des dispositions fortement recommandées. La conformité à ces guides pratiques n'est donc pas obligatoire, mais fortement recommandée. Ces guides ont été officiellement révisés et approuvés par l'IIA.

Pour de plus amples informations sur les documents de référence proposés par l'Institute, vous pouvez consulter notre site Web, www.theiia.org/guidance ou www.ifaci.com.

AVERTISSEMENT

L'Institute of Internal Auditors publie ce document à titre informatif et pédagogique. Cette ligne directrice n'a pas vocation à apporter de réponses définitives à des cas précis, et doit uniquement servir de guide. L'Institute of Internal Auditors vous recommande de toujours solliciter un expert indépendant pour avoir un avis dans chaque situation. L'Institute dégage sa responsabilité pour les cas où des lecteurs se fieraient exclusivement à ce guide.

COPYRIGHT

Le copyright de ce guide pratique est détenu par l'Institute of Internal Auditors et par l'IFACI pour sa version française. Pour l'autorisation de reproduction, prière de contacter l'Institute of Internal Auditors à l'adresse <u>quidance@theiia.org</u> ou l'IFACI à l'adresse <u>recherche@ifaci.com</u>

SIÈGE MONDIAL

247 Maitland Ave,

Altamonte Springs, Florida 32701, États-Unis

Téléphone : +1 407 937 1100 Télécopie : +1 407 937 1101

Site Web: www.theiia.org

Courrier électronique : <u>guidance@theiia.org</u>

IFACI

98bis, Boulevard Haussman 75008 PARIS. France

Téléphone : 01 40 08 48 00

Fax: 01 40 08 48 20 Site Web: www.ifaci.com

Courrier électronique : recherche@ifaci.com