CRIPP

Cadre de Référence International des Pratiques Professionnelles de l'audit interne

Lignes directrices complémentaires

Guide pratique

Évaluation du processus de management des risques

The Institute of Internal Auditors | Global

A propos du CRIPP

Le Cadre de Référence International des Pratiques Professionnelles de l'audit interne® (CRIPP®) comprend les lignes directrices approuvées par l'*Institute of Internal Auditors.*

Instance internationale de normalisation, l'IIA fournit aux auditeurs internes du monde entier des orientations qui font autorité. Elles figurent dans les dispositions obligatoires ou recommandées du CRIPP.

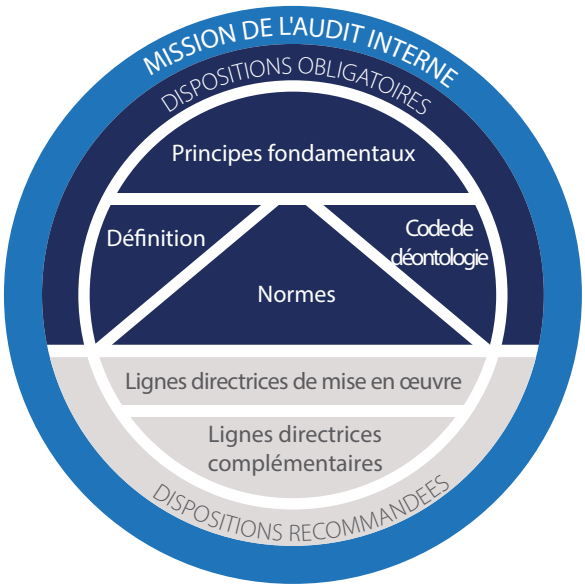
Les dispositions obligatoires sont élaborées selon un processus de diligence raisonnable qui inclut une consultation publique pour la prise en compte des avis des parties prenantes.

Elles comprennent :

- les principes fondamentaux pour la pratique professionnelle de l'audit interne
- la définition de l'audit interne
- le Code de déontologie
- les *Normes internationales pour la pratique professionnelle de l'audit interne*

CRIPP

Cadre de Référence International des Pratiques Professionnelles de l'audit interne



À propos des lignes directrices complémentaires

Les lignes directrices complémentaires font partie intégrante du Cadre de référence international des pratiques professionnelles® (CRIPP®) et proposent des recommandations supplémentaires facultatives pour la réalisation des activités d'audit interne. Tout en étayant les *Normes*, elles couvrent des domaines particuliers, ainsi que des problématiques sectorielles, et contiennent des procédures et processus détaillés. Les lignes directrices complémentaires sont homologuées par l'IIA *(the Institute of Internal Auditors)* à l'issue d'un processus formalisé de revue et d'approbation.

Guides pratiques

Les guides pratiques constituent un type de lignes directrices complémentaires qui offrent des approches séquentielles, intégrant des processus, des procédures, des outils et des programmes, ainsi que des exemples de livrables.

Ces guides pratiques sont destinés à aider les auditeurs internes. Il existe aussi des guides pratiques ciblant :

- les établissements financiers
- le secteur public
- les systèmes d'information (GTAG® pour *Global Technology Audit Guide*)

Pour de plus amples informations sur les documents de référence proposés par l'IIA, vous pouvez consulter le site web www.globaliia.org/standards-guidance

Table des matières

Synthèse 4

Introduction 5

Enjeux métier : Risques et opportunités 6

Maturité du management des risques 7

- Appétence pour le risque 9
- Structure : rôles et responsabilités 9
- Culture 10
- Gouvernance 11
- Processus 11

Rôle de l'audit interne dans le management des risques 14

Évaluer le management des risques de l'organisation 15

- Comprendre le contexte et l'objectif de la mission 15
- Collecter des informations afin de comprendre le processus de management des risques 16
- Réaliser une évaluation préliminaire des risques 17
- Définir les objectifs de la mission 18
- Etablir le périmètre d'intervention de la mission 19
- Affecter les ressources 20
- Documenter le programme de travail de la mission 21
- Réaliser la mission et communiquer les résultats 21
- Évaluer le processus de management des risques de l'audit interne 22

Annexe A. Normes et lignes directrices de l'IIA applicables 23

Annexe B. Glossaire 24

Annexe C. Scénarii potentiels de risque 25

Annexe D. Matrice des risques et des contrôles 27

Annexe E. Évaluation du processus de management des risques 29

Annexe F. Références et sources bibliographiques supplémentaires 31

Remerciements 32

Synthèse

Dans le monde entier, les activités et les initiatives de management des risques sont requises et attendues par les régulateurs, les agences de notation et par de nombreuses autres parties prenantes issues de secteurs importants tels que la finance, le secteur public, l'industrie, l'énergie et la santé, entre autres. Cependant, le management des risques n'est pas seulement impulsé par des réglementations et des facteurs externes. La mise en œuvre d'un management des risques efficace bénéficie à des organisations de tous types et de toutes tailles en les aidant à atteindre leurs objectifs opérationnels et stratégiques, à accroître leur valeur et leur durabilité et, à terme, à mieux protéger leurs parties prenantes.

Les auditeurs internes doivent évaluer l'efficacité des processus de management des risques et contribuer à leur amélioration (Norme 2120 – Management des risques). Comparer l'état actuel du management des risques de l'organisation avec un modèle de maturité dans ce domaine est un bon point de départ pour réaliser cette évaluation. Une étude comparative peut permettre à la fonction d'audit interne de communiquer avec la direction générale et le Conseil sur le niveau de maturité du management des risques de l'organisation et sur la façon d'améliorer le processus et de gagner en maturité. Ces informations permettent également aux auditeurs internes d'adapter chaque mission, en prenant en compte la maturité du domaine ou du processus audité.

Ce guide donne des exemples de modèles de maturité du management des risques ainsi qu'une méthodologie de base que les auditeurs internes peuvent utiliser pour fournir une assurance indépendante sur l'efficacité du processus de management des risques de l'organisation. Ce guide aidera les auditeurs internes à préserver et accroître la valeur de l'organisation et à répondre aux attentes de la direction générale et du Conseil.

Introduction

Les travaux d'une organisation en matière de **management des risques** sont souvent appelés « programme de management des risques ». Cependant, le terme « programme » peut sembler limité. Ce guide aborde le management des risques comme un processus plus que comme un programme, ce qui implique une notion de démarche et d'effort en continu.

Note : Les termes en gras sont définis dans le glossaire en Annexe B.

Dans de nombreux secteurs, le **Conseil** est chargé de veiller à ce qu'un processus de management des risques soit en place et réponde efficacement à l'évolution des risques. De même, le **responsable de l'audit interne** et la **fonction d'audit interne** doivent fournir une assurance indépendante sur l'efficacité du processus de management des risques de l'organisation, conformément à la Norme 2120 – Management des risques, qui détermine plusieurs critères pour réaliser l'évaluation.

Évaluer les processus de management des risques d'une organisation est un défi croissant en raison du nombre important de normes, référentiels et modèles de management des risques qui existent déjà ou voient le jour régulièrement. Le management des risques peut inclure les politiques, procédures et contrôles qui garantissent une identification, une évaluation, un traitement, un suivi et un reporting adéquats des risques de l'organisation, en continu et en temps opportun.

Ce guide ne préconise pas le recours à un programme, référentiel ou modèle de management des risques en particulier, mais traite des caractéristiques propres à un management des risques mature.

- Culture du risque : Intégration des risques à tous les niveaux du processus de décision, de rémunération et de primes, et de fixation des objectifs.
- Gouvernance des risques : Participation de toute l'organisation au processus de management des risques par l'intermédiaire de collaborateurs qualifiés et compétents en la matière.
- Processus de management des risques : Identification, priorisation, traitement, suivi et reporting des risques dans toute l'organisation.

En outre, les niveaux de maturité, les approches, les stratégies et les priorités des fonctions liées au management des risques dépendent souvent de la taille et de la complexité de l'organisation ainsi que du secteur et de la juridiction dans lesquels elle opère. Ce guide fournit des informations générales, une méthodologie et des outils pour permettre aux auditeurs internes de fournir une assurance sur l'efficacité des processus de management des risques et de contribuer à l'amélioration de ces derniers.

Ce guide aidera les auditeurs internes à :

- appliquer les principes du Code de déontologie de l'IIA et les *Normes internationales pour la pratique professionnelle de l'audit interne* pour préserver et accroître la valeur de l'organisation en fournissant une assurance, des conseils et des éclairages objectifs fondés sur les risques ;
- comprendre le besoin d'évaluer les activités de management des risques ;
- comprendre les principales composantes d'un processus de management des risques efficace ;
- développer une approche d'évaluation qui prend en compte l'activité, le contexte réglementaire et le niveau de maturité de l'organisation ;

- recueillir les informations nécessaires pour déterminer le périmètre d'intervention d'une mission dédiée à l'évaluation des activités de management des risques ;
- évaluer l'efficacité du processus de management des risques ;
- contribuer à l'amélioration du processus de management des risques.

Enjeux métier : Risques et opportunités

Le management des risques a longtemps joué un rôle essentiel dans les organisations. Il a évolué sous différentes formes et porte plusieurs noms, dont « management des risques liés au projet » ou « management des risques de l'entreprise (ERM) ». Le management des risques continue de susciter l'attention à mesure que le monde devient de plus en plus interconnecté et que les disruptions s'accélèrent dans tous les secteurs. Toutefois, l'adoption formelle d'une démarche de management des risques commune à toute l'organisation n'est pas encore reconnue comme une norme universelle.

La défaillance de la gouvernance, des systèmes et des processus de management des risques peut se traduire par un engagement de responsabilité, des amendes ou sanctions, ainsi que de nombreuses conséquences associées. Des travaux d'analyse et d'évaluation continue du management des risques contribueront, pour les organisations, à réduire la mise en péril de leurs actifs, protéger leur propriété intellectuelle, leurs parts de marché, leurs opportunités de revenus ainsi qu'à préserver la fidélité de leurs clients et leur réputation, etc. du fait de la survenance de risques qui auraient pu être prévenus, évités ou minimisés (partagés ou transférés). L'Annexe C présente des scénarii de risques liés au processus de management des risques.

Les organisations bien gérées et performantes utilisent le processus de management des risques pour coordonner le pilotage et le contrôle de l'exposition aux risques de manière à ce qu'elles puissent atteindre leurs objectifs. Il peut être difficile de mesurer les bénéfices d'un processus de management des risques mature car il est parfois compliqué, voire impossible, d'obtenir des données fiables. De ce fait, les organisations peuvent avoir du mal à analyser objectivement la maturité de leur propre processus de management des risques.

Cependant, un tel processus, lorsqu'il est mature, offre généralement des avantages en :

- permettant la prise de décisions et l'élaboration de stratégies fondées sur les risques ;
- favorisant une communication et une consultation étendue au sein de l'organisation ;
- établissant des liens et des perspectives entre les risques, les opportunités et les stratégies par le biais d'un langage du risque commun ;
- facilitant la documentation et le reporting en temps opportun des activités de management des risques, de sorte que la direction générale et le Conseil soient bien informés de l'orientation prise par le management ;
- augmentant la probabilité que l'organisation atteigne ses objectifs stratégiques ;
- créant de la valeur pour les parties prenantes et en la protégeant.

Lorsqu'ils proposent d'apporter des améliorations au processus de management des risques, les auditeurs internes peuvent rencontrer des objections, telles que :

- l'évaluation des risques prend trop de temps ;
- les informations sur les risques collectées ne sont pas pertinentes ;
- les informations sur les risques ne sont pas utilisées pour la prise de décision.

Lorsque la fonction d'audit interne conçoit une évaluation du processus de management des risques, la compréhension du niveau de maturité de ce dernier ainsi que de la culture du risque de l'organisation est essentielle pour pouvoir poser les questions appropriées. Si l'organisation n'a pas encore défini de vision ou de philosophie en matière de management des risques, la fonction d'audit interne devrait en comprendre les raisons avant de formuler ses constats et recommandations. Il est important de recueillir des avis quant à la capacité du processus de management des risques à produire des informations pertinentes. Si la direction pense que le processus de management des risques est un exercice bureaucratique qui ne mérite pas les ressources nécessaires à sa mise en œuvre, recommander des améliorations à grande échelle peut sembler précipité et susciter du scepticisme, voire un rejet total. Dans ce cas, il serait plus efficace que les auditeurs internes fassent des recommandations liées à la culture du risque de l'organisation.

Maturité du management des risques

Il existe plusieurs référentiels de management des risques. Chacun d'eux propose des principes que les organisations devraient prendre en compte lors de la conception d'un processus de management des risques global. Certains référentiels se concentrent sur les dispositifs de contrôle interne et sur leur interdépendance avec les risques de l'organisation. D'autres se focalisent seulement sur les risques SI, stratégiques ou les risques assurables par exemple. Une organisation peut conclure qu'aucun référentiel unique n'englobe l'ensemble des domaines de risques devant être couverts. Ainsi, au lieu d'adopter un seul référentiel, elle peut choisir de combiner les éléments de plusieurs référentiels pour en créer un qui sera adapté à ses caractéristiques et besoins spécifiques. Indépendamment du cadre de référence utilisé comme base pour le processus de management des risques, certains éléments peuvent aider l'organisation à mesurer sa maturité.

L'illustration n°1 montre un exemple de **modèle de maturité** du management des risques qui illustre cinq étapes de développement pouvant caractériser un processus de management des risques. Plusieurs éléments au sein de la même organisation peuvent se trouver à différents niveaux de maturité à tout moment. Par exemple, le niveau de maturité de la culture d'une organisation peut différer de celui de sa gouvernance et de son processus. Lors de la planification des missions d'audit, les auditeurs internes peuvent utiliser un modèle de maturité pour adapter chaque mission à l'élément examiné.

Illustration 1 : Exemple de modèle de maturité du management des risques

Niveau	Culture	Gouvernance	Processus
1- Initial	Les risques relèvent de l'activité de l'audit interne.	Responsable de l'audit interne/président du comité d'audit.	Audit fondé sur les risques.
2- Reproductible	Le risque est considéré en fonction des besoins.	Managers opérationnels.	Processus d'auto-évaluation des risques et des contrôles en fonction des besoins.
3- Défini	Les informations sur les risques sont partagées entre l'audit interne et les fonctions de contrôle.	Membres de la direction générale/du Conseil.	Un langage de risque commun et un processus d'évaluation des risques sont utilisés par l'audit interne et les fonctions de contrôle.
4- Maîtrisé	Les risques sont intégrés dans la planification stratégique ; l'appétence pour le risque est définie et communiquée.	Tous les niveaux du management et le Conseil.	Un langage commun du risque et un processus d'évaluation des risques cohérents sont en place dans toute l'organisation.
5- Optimisé	Les risques sont intégrés dans toutes les prises de décisions, la stratégie de rémunération et la définition des objectifs.	Participation totale.	Un langage commun du risque et un reporting des risques agrégés sont établis dans toute l'organisation.

Pour vérifier où se situe une organisation vis-à-vis du modèle de maturité du management des risques et pour évaluer l'efficacité avec laquelle ce processus sert les intérêts de l'organisation, les auditeurs internes devraient prendre en compte plusieurs éléments.

Toutes les organisations s'adonnent à une certaine forme de management des risques, même si elles n'en ont pas conscience et ne documentent pas officiellement leurs travaux. La forme la plus élémentaire de management des risques documenté consiste en l'élaboration annuelle et au plus haut niveau de l'organisation, d'un registre des risques. Il peut être assimilé à une « évaluation stratégique des risques » dans laquelle la direction générale établit et documente une liste de risques qui ne sera pas réexaminée avant l'année suivante. À l'autre extrême, les organisations bénéficiant d'un processus de management des risques plus solide ou mature prennent en compte les différents facteurs de risque, y compris ceux qui ont trait à la culture ou à la gouvernance, dans toute l'organisation de façon systématique et structurée.

Considérations relatives à la mission d'audit interne

Quel niveau de maturité une organisation devrait-elle avoir ? Sur une échelle de 1 à 5, 5 étant le niveau le plus mature. Il n'est pas nécessairement optimal ou pratique pour toutes les organisations de fonctionner à un niveau de maturité maximal. Atteindre un niveau 2 ou 3 peut être satisfaisant. Chaque organisation devrait définir le niveau de maturité optimal pour sa situation.

Appétence pour le risque

Le Cadre de référence international des pratiques professionnelles de l'IIA définit l'**appétence pour le risque** comme le niveau de risque qu'une organisation est prête à accepter. Pour bon nombre d'organisations, l'appétence pour le risque est difficile à mettre en pratique dans les échanges. Une déclaration relative au « niveau de perte acceptable » est une forme courante d'appétence pour le risque qui peut être approuvée par la direction générale et/ou le Conseil à condition que la limite des pertes ne puisse être excédée qu'avec l'accord de l'autorité compétente.

La qualification de l'appétence pour le risque comme un « niveau de perte acceptable » peut être interprétée comme un plan de l'organisation pour atteindre le niveau de perte déclaré (quantité monétaire) conditionné au niveau d'exposition aux risques, ce qui pourrait amener les managers à accepter des niveaux d'exposition supérieurs à ce qui est nécessaire ou souhaité. De plus, définir une appétence pour le risque en termes de stratégies globales peut conduire à des divergences d'interprétation sur l'application du degré de tolérance car la déclaration relative à l'appétence pour le risque s'applique à des niveaux inférieurs de l'organisation.

Les auditeurs internes devraient encourager l'organisation à adopter une méthodologie et un format d'appétence pour le risque qui permettent à la direction générale et au Conseil de donner la priorité aux stratégies et aux allocations de ressources. L'appétence pour le risque peut être dynamique et constitue souvent un équilibre entre les stratégies. L'établissement de niveaux déterminés d'exposition aux risques par les dirigeants de l'organisation peut inciter à négliger l'appétence pour le risque comme un outil pour prendre des décisions avisées de manière cohérente à tous les niveaux de l'organisation.

Structure : rôles et responsabilités

En fonction du niveau de maturité du processus de management des risques de l'organisation et des ressources disponibles auxquelles la fonction d'audit interne a accès, les rôles et les responsabilités liés au management des risques seront attribués différemment au sein de l'organisation.

Selon son niveau de développement et son accès aux ressources, une organisation peut se trouver à différents niveaux du modèle de maturité :

1 – Initial. Dans les organisations où le processus de management des risques en est aux premiers stades de développement, la fonction d'audit interne peut être plus activement impliquée qu'elle ne le serait si le processus était plus mature. À ce niveau de maturité, les activités de management des risques spécifiques peuvent ne pas être réalisées par les managers opérationnels ou par les fonctions de contrôle, de conformité, juridique, de management des risques ou d'assurance qualité interne. En revanche, ces fonctions peuvent dépendre de l'évaluation des risques ainsi que de l'assurance et des conseils fondés sur les risques fournis par l'audit interne.

2 – Reproductible. À ce niveau, la fonction d'audit interne est mieux organisée et dispose de plus de ressources ; elle joue un rôle majeur dans la réalisation d'évaluations fondées sur les risques, potentiellement de plus grande ampleur. L'audit interne peut associer son expertise à celle des fonctions de contrôle, de conformité, juridique, de management des risques et d'assurance qualité interne afin d'aider les propriétaires du risque (managers opérationnels) à instaurer et suivre les contrôles opérationnels. Ce niveau est suffisant pour un grand nombre d'organisations si le processus fonctionne de façon cohérente et efficace et produit des résultats exploitables qui permettent aux organisations d'atteindre leurs objectifs.

3 – Défini. Les organisations qui se situent vers le milieu du modèle peuvent représenter un mélange de plusieurs niveaux de maturité ; certaines unités opérationnelles opérant à des niveaux de maturité plus élevés que d'autres. Avec une telle structuration, les fonctions de contrôle, de conformité, juridique, de management des risques et d'assurance qualité interne de l'organisation peuvent être en charge du processus de management des risques et assumer les responsabilités qui correspondent systématiquement aux niveaux *Maîtrisé* et *Optimisé*, par exemple. Les fonctions de contrôle et d'assurance peuvent jouer un rôle actif en aidant le management opérationnel à évaluer les risques et à réaliser d'autres activités de gestion des risques. L'audit interne peut continuer à opérer de manière fonctionnelle comme au niveau *Reproductible*.

4 – Maîtrisé. Plus en amont dans le modèle de maturité, dans les organisations ayant atteint un certain niveau de maturité, le management opérationnel possède et gère les risques de l'ensemble de l'organisation et est en charge de la mise en œuvre d'actions correctives visant les activités de processus et de contrôle. La fonction d'audit interne agit principalement comme une fonction d'assurance indépendante ; elle évalue l'efficacité du processus de management des risques au même titre que les autres fonctions de management et d'assurance.

5 – Optimisé. Pour les organisations ayant atteint ce niveau d'intégration, de sophistication et de maturité, le management opérationnel est en charge du processus de management des risques. Les fonctions de conformité et/ou de management des risques de l'organisation conduisent l'évaluation des risques pour répondre à leurs propres besoins. Elles peuvent aussi suivre l'évaluation et le reporting des risques produits par le management opérationnel et remettre en question les informations sur les risques, si nécessaire. Les risques sont suivis et gérés par plusieurs processus opérationnels.

L'audit interne, en tant que fonction d'assurance indépendante, effectue des missions pour évaluer l'efficacité des processus de management des risques dans des domaines spécifiques et dans toute l'organisation. De plus, il peut comparer son évaluation des risques avec les informations sur les risques produites par le management et corroborées par les fonctions d'assurance interne (conformité/management des risques) pour mesurer l'exactitude et l'exhaustivité de l'évaluation réalisée par le management. À l'inverse, l'audit interne peut intégrer les informations sur les risques fournies par le management à sa propre évaluation ou faire les deux, si nécessaire. Le responsable de l'audit interne devrait se coordonner avec d'autres prestataires externes d'assurance et de conseil et envisager d'utiliser leurs travaux (Norme 2050 – Coordination et utilisation d'autres travaux).

Ressource

Pour plus d'informations sur la définition des rôles et des responsabilités du management des risques, consulter le Guide pratique « Coordination et utilisation d'autres travaux : Élaborer une cartographie des prestations d'assurance ».

Culture

L'efficacité et l'exhaustivité d'un processus de management des risques dépend de la culture du risque de l'organisation. Si la culture n'est pas propice à une discussion ouverte et à la prise en compte des risques, au sens positif comme négatif du terme, alors le processus de management des risques ne pourra pas aboutir. Les auditeurs internes devraient poser la question suivante : « En l'absence de politiques, comment le management opèrerait-il ? » Une organisation peut disposer de politiques et procédures stipulant que le management des risques sera pris en considération, mais la culture peut occulter cette intention et remettre en cause toute argumentation ou action engageante.

Les organisations peuvent avoir des processus élaborés de mesure et d'évaluation des risques, sans que la culture du risque ne soit favorable au management des risques. Dans les secteurs réglementés, un processus de management des risques opérationnel peut être requis, mais si les managers se contentent simplement de cocher des cases sur une liste de contrôle, il est peu probable que celui-ci atteigne un niveau de maturité où les informations sur les risques sont bien intégrées à la prise de décision (et liées à la rémunération et aux primes), consolidées et largement diffusées dans toute l'organisation.

Si les auditeurs internes participent à la conception d'un processus de management des risques et constatent que la culture de l'organisation ne soutient pas leur démarche, ils peuvent en informer le responsable de l'audit interne qui peut discuter de la viabilité du processus avec la direction générale et le Conseil. Néanmoins, même si ces derniers y sont favorables, faire pression sur le management dans une organisation réticente à l'idée d'adopter un programme de management des risques porte rarement ses fruits. Les managers doivent comprendre la valeur de ce processus avant d'en être les promoteurs.

Gouvernance

Pour qu'un processus de management des risques soit efficace, le soutien des dirigeants doit être acquis dès le départ. Pour obtenir leur adhésion et l'allocation des ressources nécessaires, les informations sur les risques doivent être utilisées dans la prise de décision aux niveaux les plus stratégiques d'une organisation. L'intérêt des organes de gouvernance, comme le comité d'audit ou le Conseil, est essentiel pour susciter la collecte, l'évaluation et la transmission des informations sur les risques. Si le comité d'audit exige régulièrement des informations sur les risques dans le cadre de son activité de surveillance, alors le management doit trouver un moyen de les lui fournir.

En général, le processus de management des risques est conçu selon une approche descendante ; la direction générale et le Conseil sont les premiers à demander une évaluation des risques et un reporting, ce qui conduit généralement les managers opérationnels à adopter les mêmes pratiques en cascade, ces derniers devant fournir des informations sur les risques à la direction générale. Une fois que les principaux managers opérationnels, la direction générale et le Conseil sont impliqués dans le processus de management des risques, la structure peut être clarifiée et les politiques, les procédures, le reporting et les protocoles de remontée d'alertes peuvent être mis en œuvre.

Processus

Le degré d'intégration des activités de management des risques à d'autres processus opérationnels est un indicateur utile pour mesurer le niveau de maturité de l'organisation. Si des évaluations des risques sont menées régulièrement dans toute l'organisation, si l'appétence pour le risque est communiquée efficacement à tous les niveaux et si les informations sur les risques sont utilisées dans les prises de décisions importantes, l'organisation est perçue comme plus mature qu'une organisation qui réalise une évaluation des risques une fois par an ou uniquement lorsqu'elle est imposée par les réglementations. L'illustration n°2 présente les différences. Cet exemple est représentatif sans être exhaustif.

Illustration 2 : Exemple de descriptions de modèles de maturité

1 – Initial	
Appétence pour le risque	L'appétence pour le risque de l'organisation est sous-entendue mais pas clairement énoncée ni documentée. Les dirigeants peuvent avoir des idées similaires sur le niveau de risque que l'organisation est prête à accepter.
Évaluation des risques	Les auditeurs internes peuvent réaliser une évaluation des risques afin de collecter des informations en vue de leurs missions, d'une utilisation par les fonctions de contrôle, conformité, assurance interne, et/ou dans le but d'une utilisation par le management. Ce dernier n'a pas investi dans le recrutement ou la formation de collaborateurs dotés de compétences en facilitation et en évaluation des risques, et les auditeurs internes sont probablement les seuls compétents en la matière. Les risques sont évalués en fonction des besoins. Par exemple, les membres de l'équipe dirigeante peuvent évaluer une fois par an les risques liés à leurs propositions de stratégie. Les grands projets coûteux peuvent également justifier une évaluation des risques si nécessaire.
Langage commun	Le management utilise les informations sur les risques à sa disposition mais la terminologie n'est pas cohérente ou est mal interprétée au sein de l'organisation. Il peut exister plusieurs registres de risques et plusieurs critères de mesure des risques en fonction de l'objectif de l'évaluation des risques. Les critères de mesure des risques sont simples comme, par exemple, l'échelle de cotation : élevé, moyen et faible.
Utilisation des informations sur les risques	Les informations sur les risques ne sont pas agrégées ou communiquées au-delà du groupe spécifique qui a procédé à l'évaluation des risques.
2 – Reproductible	
Appétence pour le risque	L'appétence pour le risque de l'organisation a été discutée par l'équipe dirigeante et le Conseil et est documentée mais elle n'est pas partagée dans toute l'organisation. Le sujet est mis à jour de manière variable.
Évaluation des risques	Les auditeurs internes peuvent réaliser une évaluation des risques afin de collecter des informations en vue de leurs missions, d'une utilisation par les fonctions de contrôle, conformité, assurance interne, et/ou dans le but d'une utilisation par le management. Ce dernier n'a pas investi dans le recrutement ou la formation de collaborateurs dotés de compétences en facilitation et en évaluation des risques. Les risques sont évalués régulièrement mais un plan complet et stratégique fait défaut. Les grands projets coûteux peuvent donner lieu à une évaluation ponctuelle des risques.
Langage commun	Le management utilise les informations sur les risques à sa disposition mais la terminologie n'est pas cohérente ou est mal interprétée au sein de l'organisation. Il peut exister plusieurs registres de risques et plusieurs critères de mesure des risques en fonction de l'objectif de l'évaluation des risques. Les critères de mesure des risques peuvent prendre en compte la probabilité et l'impact en les catégorisant comme élevés, moyens ou faibles.
Utilisation des informations sur les risques	Les informations sur les risques sont parfois agrégées ou communiquées au-delà du groupe spécifique qui a procédé à l'évaluation des risques.

Illustration 2 : Exemple de descriptions de modèles de maturité (suite)

3 – Défini	
Appétence pour le risque	L'équipe dirigeante et le Conseil ont vaguement défini une appétence pour le risque qui peut être bien comprise, ou non, dans toute l'organisation.
Évaluation des risques	Les fonctions de contrôle, conformité, management des risques et assurance interne peuvent réaliser une évaluation des risques dans leurs domaines respectifs ou en vue d'une utilisation par le management. Ce dernier n'a pas investi dans le recrutement ou la formation de collaborateurs dotés de compétences en facilitation et en évaluation des risques. Une évaluation des risques peut être réalisée en fonction des besoins. Par exemple, la direction générale peut solliciter une évaluation des risques pour un grand projet d'investissement présentant une exposition importante pour l'organisation.
Langage commun	Le management utilise les informations sur les risques à sa disposition et la terminologie est majoritairement cohérente dans toute l'organisation. Les registres de risques et les critères de mesure des risques sont multiples.
Utilisation des informations sur les risques	Les risques peuvent être liés aux objectifs d'un département ou d'une équipe projet mais ne sont pas toujours ouvertement pris en compte par les échelons supérieurs de l'organisation.
4 – Maîtrisé	
Appétence pour le risque	L'équipe dirigeante et le Conseil ont défini une appétence pour le risque qui est bien comprise dans toute l'organisation.
Évaluation des risques	Les fonctions de contrôle, conformité, management des risques et assurance interne réalisent régulièrement une évaluation des risques dans leurs domaines respectifs ou en vue d'une utilisation par le management. Ce dernier a investi dans le recrutement ou la formation de collaborateurs dotés de compétences en facilitation et en évaluation des risques. L'évaluation des risques est réalisée en fonction des besoins et peut traiter des risques importants à mesure qu'ils surviennent au lieu de s'appuyer sur un plan d'audit fondé sur une approche par les risques.
Langage commun	La direction générale sollicite et utilise constamment les informations sur les risques et la terminologie est bien connue et utilisée dans toute l'organisation. Les critères de management des risques sont compris et appliqués dans toute l'organisation.
Utilisation des informations sur les risques	Les risques significatifs sont liés aux objectifs de l'organisation. Les informations sur les risques sont systématiquement communiquées aux dirigeants et le système de rémunération et de primes du management peut être associé à des indicateurs clés de performance basés sur des risques identifiés et évalués. Les informations sont utilisées pour contribuer à améliorer le processus de management des risques dans toute l'organisation.
5 – Optimisé	
Appétence pour le risque	Une fois l'appétence pour le risque approuvée par le Conseil, le management et les principaux collaborateurs l'appliquent dans toute l'organisation dans un format et un niveau de détails appropriés à leur prise de décisions.
Évaluation des risques	Le management utilise un processus commun pour réaliser une évaluation des risques, documenter les informations sur les risques et suivre sa performance au regard d'indicateurs clés de performance basés sur les risques. Le management a établi des protocoles pour garantir que les risques significatifs soient pris en compte dès leur survenance plutôt que pendant ou après la prochaine évaluation des risques prévue.
Langage commun	Tous les niveaux de l'organisation, que ce soit le Conseil, le management opérationnel ou les collaborateurs, ont la même compréhension des termes utilisés dans le processus de management des risques (p. ex. risque, facteur contributif, contrôle, impact, probabilité) et utilisent un langage commun pour échanger sur les risques.
Utilisation des informations sur les risques	Les risques sont liés aux objectifs de l'organisation à tous les niveaux. En outre, les informations sur les risques sont communiquées régulièrement dans toute de l'organisation, et la rémunération et les primes du management dépendent des indicateurs clés de performance basés sur les risques identifiés et évalués.

Rôle de l'audit interne dans le management des risques

La Norme 2120 – Management des risques stipule que « l'audit interne doit évaluer l'efficacité des processus de management des risques et contribuer à leur amélioration. » Plus spécifiquement, elle requiert des auditeurs internes qu'ils évaluent si :

- les objectifs de l'organisation sont cohérents avec sa mission ;
- les risques significatifs sont évalués par le management ;
- les modalités de traitement des risques retenues par le management sont 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, y compris au Conseil.

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 d'avoir une compréhension globale du processus de management des risques de l'organisation et de juger son efficacité. L'audit interne doit également fournir l'assurance que le management a mis en place des activités de suivi en continu des processus de management des risques.

L'audit interne peut être appelé à assumer d'autres responsabilités en matière de management des risques. S'il est sollicité pour aider au développement des processus de management des risques (p. ex. en menant et en documentant une évaluation des risques), son indépendance peut être remise en question. Pour clarifier les rôles de chacun, les auditeurs internes devraient se référer aux Normes de la série 1100 – Indépendance et objectivité, en prêtant une attention particulière à la Norme 1130 – Atteinte à l'indépendance ou à l'objectivité et à ses alinéas. Ces derniers distinguent les missions d'assurance et les missions de conseil. Par exemple, 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.A1).

La Norme 1112 – Rôles du responsable de l'audit interne en dehors de l'audit interne reconnaît que le responsable de l'audit interne peut se voir confier des rôles et des responsabilités qui ne relèvent pas de l'audit interne, telle que la responsabilité de la fonction de conformité ou de management des risques. Dans ce cas, des précautions doivent être prises pour limiter les atteintes à l'indépendance ou à l'objectivité. Celles-ci comprennent la surveillance généralement effectuée par le Conseil pour traiter les atteintes potentielles à l'indépendance et à l'objectivité. Si le responsable de l'audit interne est en charge du management des risques ou d'une fonction qui y est rattachée, alors les missions d'assurance concernant ces fonctions doivent être supervisées par une personne ne relevant pas de la fonction d'audit interne (Norme 1130.A2).

Certaines organisations peuvent assimiler le rôle de l'audit interne dans l'élaboration de processus de management des risques à des services de conseil, limitant ainsi l'impact sur son indépendance. Cependant, les Normes 1130.C1 et 1130.C2 devraient être prises en compte et les auditeurs internes devraient divulguer les atteintes potentielles si elles existent. Une autre possibilité consiste à créer des équipes d'audit indépendantes : l'une travaillant à l'élaboration des processus de management des risques tandis que l'autre évalue leur efficacité. Une autre option consiste à permettre aux auditeurs internes de développer les processus de management des risques en prévoyant d'en confier le fonctionnement et la supervision à des collaborateurs formés au sein des fonctions de conformité, management des risques, assurance interne, ou du management opérationnel.

Évaluer le management des risques de l'organisation

Selon la Norme 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 périmètre d'intervention, le calendrier de la mission, ainsi que les ressources allouées. Ce plan doit prendre en considération la stratégie, les objectifs et les risques de l'organisation pertinents au regard de la mission.

Cette section a pour but de guider les auditeurs internes à travers le processus de planification et de mise en œuvre d'une évaluation du management des risques de l'organisation. Les exemples fournis, bien que non exhaustifs, devraient les aider à définir les principaux domaines à inclure, le type de documents pouvant être demandés, et les éléments de preuve pouvant être obtenus.

Il peut être difficile d'évaluer l'ensemble du processus de management des risques. Aussi, le périmètre de la mission d'audit peut être défini selon des critères répondant à un objectif spécifique. On pourra alors le restreindre aux unités organisationnelles, sites, ou encore aux objectifs stratégiques ou à d'autres critères pertinents pour l'organisation.

Comprendre le contexte et l'objectif de la mission

Comme illustré dans le modèle de maturité du management des risques **(Illustration 1)**, des structures et des processus de gouvernance bien définis soutiennent généralement le processus de management des risques dans une organisation dotée d'une culture orientée risque. Néanmoins, il est possible qu'une organisation ne possède pas de structures ou processus semblables.

Dans une évaluation du management des risques de l'organisation, une mission d'audit se divise en deux parties : la première identifie les principes appliqués au processus de management des risques de l'organisation, l'autre évalue si ces principes sont appropriés et efficaces.

Lors de la planification de l'évaluation, les auditeurs internes devraient se référer au Guide de mise en œuvre de la Norme 2120 – Management des risques et tenir compte des éléments suivants :

- le plan stratégique et les *business plans*, les missions et les objectifs de l'organisation ;
- tout référentiel de management des risques utilisé au sein de l'organisation ;
- les méthodes utilisées actuellement et le niveau d'identification, d'évaluation, et de surveillance des risques ;
- les processus pouvant être utilisés pour suivre, évaluer et gérer les risques et les opportunités ;
- la complexité de l'organisation et ses processus de management des risques, en tenant compte de facteurs tels que sa taille, sa complexité, son cycle de vie, sa maturité, la structure de ses parties prenantes et le contexte juridique et concurrentiel ;
- la robustesse des rôles, des responsabilités et des activités en matière de management des risques dans toute l'organisation ;
- les résultats actuels des activités de surveillance des risques (identifier et discuter des risques ainsi que des actions correspondantes qui ont été choisies) ;
- les risques survenus par le passé ;

- tous les changements (réglementation, mobilité du personnel, processus, produits et services) qui auraient pu introduire de nouveaux risques ;
- l'exposition aux risques et opportunités potentielles; y compris les nouvelles évolutions, les tendances, les risques émergents, et les éventuelles perturbations liées à l'organisation (ainsi qu'à son environnement et son secteur) ;
- toutes les obligations et attentes, réglementaires ou autres, applicables à l'organisation et aux secteurs dans lesquels elle opère ;
- les attentes des parties prenantes concernant l'assurance fournie par l'audit interne sur l'efficacité du processus de management des risques de l'organisation.

Il est primordial que l'audit interne analyse si le management a fixé des objectifs en matière de management des risques. Les auditeurs internes devraient chercher des preuves que le management œuvre à la réalisation de ces objectifs mais aussi obtenir des précisions sur la vision de ce dernier concernant le processus de management des risques, ses projets, et ses méthodes d'évaluation.

Lors de l'élaboration du plan de mission, les auditeurs internes collectent des informations en prenant connaissance des évaluations précédentes (ex : évaluations des risques, rapports de prestataires de services d'assurance et de conseil), en identifiant et en cartographiant les flux et contrôles relatifs au processus de management des risques, et en organisant des entretiens avec les parties prenantes concernées. Les informations acquises au cours de la phase de planification devraient être bien documentées, rapidement mises à jour et prises en compte tout au long de la mission. Ces informations peuvent également être utiles au responsable de l'audit interne dans sa planification à long terme des futures missions.

Collecter des informations afin de comprendre le processus de management des risques

Après avoir identifié les départements, les fonctions et les rôles pertinents pour la mission au sein de l'organisation, les auditeurs internes doivent recueillir des informations pour étayer une évaluation préliminaire des risques et planifier le déroulé de la mission, comme indiqué dans la Norme 2201 – Considérations relatives à la planification.

Les éléments suivants peuvent aider les auditeurs internes à identifier les risques de l'organisation et les stratégies mises en œuvre pour les gérer :

- les chartes, politiques et autres informations sur le mandat des instances de gouvernance responsables de l'établissement de la stratégie de management des risques ;
- la documentation sur les processus de management des risques y compris les politiques, les lignes directrices et les normes ;
- la (es) déclaration(s) relative(s) à l'appétence pour le risque ;
- les documents relatifs à la stratégie ;
- les rapports de contrôle ou autres rapports du management contenant des informations sur la performance ;
- les comptes-rendus ou procès-verbaux des réunions du Conseil/comité d'audit et d'autres comités compétents (p. ex. le comité des risques) ;
- les *business cases* de projets d'investissement significatifs ;

- les rapports externes périodiques (par exemple, aux Etats-Unis, les rapports annuels 10-K des sociétés cotées exigés par la Security Exchange Commission) ;
- l'évaluation des risques de la part du management ;
- l'inventaire des risques de l'organisation comprenant les risques stratégiques, opérationnels, humains, financiers, liés à la conformité réglementaire et les risques SI ;
- la documentation relative à toutes les phases du processus de management des risques, y compris l'identification, l'évaluation, le traitement et le suivi des risques ;
- les résultats des activités de suivi des risques.

Comme mentionné dans le Guide pratique de l'IIA « Coordination et utilisation d'autres travaux : élaborer une cartographie des prestations d'assurance, » le management des risques dans une organisation est une responsabilité partagée par tous ; par conséquent, les informations sur les risques devraient être disponibles dans tous les domaines, même s'il est possible qu'elles ne soient pas officiellement documentées ou clairement visibles. Les risques peuvent parfois être explicitement évalués dans des processus tels que la planification stratégique. Toutefois, ils peuvent aussi être identifiés de manière moins évidente dans des *business cases* (par exemple, « ce projet pourrait générer moins de chiffre d'affaires que prévu à cause des facteurs suivants... »). Pour identifier autant de risques que possible, les auditeurs internes ne devraient pas se limiter aux rapports de missions précédentes ou à l'évaluation unique des risques les plus évidents.

Considérations relatives à la mission d'audit interne

Les auditeurs internes peuvent choisir d'évaluer les processus de management des risques soit dans le contexte de missions spécifiques figurant dans le plan d'audit interne, soit dans le cadre d'une évaluation dédiée des processus identifiés comme porteurs de risques.
Le Guide pratique de l'IIA « Coordination et utilisation d'autres travaux : élaborer une cartographie des prestations d'assurance » peut aider les auditeurs internes à identifier les processus comportant des risques.

Réaliser une évaluation préliminaire des risques

La Norme 2210.A1 stipule que « les auditeurs internes doivent procéder à une évaluation préliminaire des risques liés à l'activité soumise à l'audit ». Souvent, l'évaluation des risques associés au processus de management des risques en lui-même ne requiert pas la même approche d'évaluation préliminaire des risques que les autres types de missions.

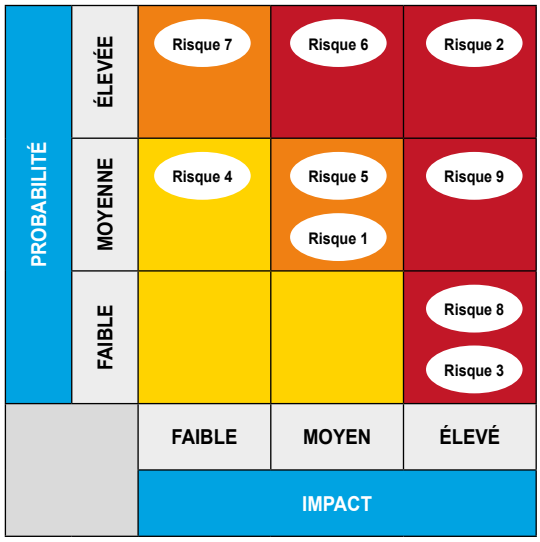
Une manière efficace d'élaborer et de documenter une mission d'évaluation des risques consiste à créer une matrice des risques présentant les risques pertinents, puis de l'élargir pour y inclure des indicateurs du caractère significatif de ces derniers. Le format de la matrice peut varier, mais celle-ci comprend généralement une ligne pour chaque risque et une colonne pour chaque critère d'évaluation, comme l'impact et la probabilité.

Dans les organisations disposant d'un processus de management des risques élaboré et mature, l'audit interne peut être en mesure d'examiner et d'utiliser l'évaluation des risques effectuée par le management plutôt que d'en réaliser une nouvelle. En rapprochant l'évaluation du processus de management des risques du modèle de maturité, les auditeurs internes mettent clairement en évidence que l'évaluation des risques est un élément clé pour déterminer le niveau de maturité du management des risques. Si le management ne l'a pas encore fait, les auditeurs internes peuvent ajouter au processus de management des risques une liste de

risques qui s'inscrivent dans les catégories culture, gouvernance et processus du modèle de maturité (voir Annexe D pour un exemple de matrice des risques et des contrôles incluant ces catégories). Ces risques peuvent ensuite être classés en termes d'impact et de probabilité. Une cartographie des risques, comme celle de **l'illustration n°3**, est un outil utilisé pour représenter visuellement le caractère significatif du risque sur une échelle simple comportant trois niveaux : élevé, moyen et faible.

En outre, la cartographie des risques peut être retenue comme document pour appuyer le plan et le programme de travail de la mission, conformément à la Norme 2240 – Programme de travail de la mission.

Illustration 3 : Cartographie des risques



Définir les objectifs de la mission

La Norme 2210 – Objectifs de la mission énonce que « les objectifs doivent être précisés pour chaque mission ». Les Normes 2210.A1 et 2210.A2 ajoutent que les objectifs d'une mission d'assurance doivent être déterminés en fonction des résultats de l'évaluation préliminaire des risques et doivent tenir compte de la probabilité qu'il existe des erreurs significatives, des cas de fraudes ou de non-conformités et d'autres risques importants.

En général, l'objectif global d'une évaluation du processus de management des risques est de fournir à la direction générale et au Conseil des éclairages sur le degré de maturité du management des risques de l'organisation et de leur indiquer si celle-ci est conforme à leurs attentes. Ce type d'évaluation peut également inclure un benchmark des meilleures pratiques sélectionnées ou encouragées par la direction générale et le Conseil.

Selon la Norme 2210.A3, pour une mission d'assurance, des critères adéquats sont nécessaires pour évaluer le management des risques, et si les auditeurs internes déterminent que la direction générale et/ou le Conseil ont déjà défini des critères pertinents (c.-à-d. un référentiel de management des risques est en place), alors ils devraient s'en servir dans leur évaluation. Dans le cas contraire, les auditeurs internes doivent collaborer avec le management et/ou le Conseil pour en élaborer. Les critères peuvent être :

- internes (par exemple, les règles et procédures de l'organisation) ;
- externes (par exemple, les lois, les règlements ainsi que les dispositions fixées par les régulateurs) ;
- issus de pratiques de référence (par exemple, des lignes directrices sectorielles ou professionnelles).

Les auditeurs internes peuvent adapter le modèle de maturité préalablement mis en place pour y intégrer ces critères de la manière la plus appropriée pour leur organisation. Les exigences externes peuvent être combinées avec les meilleures pratiques du secteur, intégrées dans le modèle de maturité et comparées avec les procédures et politiques internes de l'organisation.

Pour les organisations moins matures, il peut être préférable d'opter pour une mission de conseil en convenant des objectifs avec la direction générale et/ou le Conseil. Dans les missions de conseil, les objectifs peuvent être de nature consultative ; par exemple, sensibiliser sur l'importance de la mise en œuvre de processus de management des risques plus formalisés.

Etablir le périmètre d'intervention de la mission

Le responsable de l'audit interne ou les auditeurs internes assignés à la mission devraient être impliqués dans les réunions concernant les risques et le management des risques qui ont lieu au sein de l'organisation afin de mieux cadrer le périmètre d'évaluation de l'audit interne. Comme requis par la Norme 2220 – Périmètre d'intervention de la mission, le périmètre d'intervention doit être suffisant pour atteindre les objectifs de la mission.

A minima, le périmètre d'une évaluation en matière de management des risques devrait déterminer si des processus identifiés comme porteurs de risques sont en place et en adéquation avec les critères externes (p. ex. les lois, réglementations, exigences du secteur). Lors de la définition du périmètre d'une mission, les auditeurs internes peuvent prendre en compte :

1. la juste adéquation et l'efficacité opérationnelle des politiques, procédures et activités sur lesquelles s'appuie le processus de management des risques, y compris leur adéquation avec l'appétence pour le risque de l'organisation, les attentes des parties prenantes et les normes du secteur ;
2. l'efficacité des structures de gouvernance qui sous-tendent les politiques, procédures et activités liées au processus de management des risques ;
3. le caractère adéquat des ressources dédiées au processus de management des risques ;
4. l'intégration des éléments suivants dans le processus de management des risques :
   - les rôles et responsabilités en matière de management des risques et d'assurance clairement définis dans toute l'organisation ;
   - la prise en compte explicite du risque dans la stratégie de l'organisation ;
   - les registres/répertoires de risques, critères de cotation des risques, et processus d'évaluation des risques ;
   - les attentes en matière de traitement des risques ;
   - les rapports d'exposition aux risques requis ;
   - les processus de classification, de remontée et suivi des constats liés aux activités de pilotage des risques.

Alors que tous ces éléments devraient être présents sous une forme ou une autre dans le cadre du processus de management des risques, les auditeurs internes peuvent adapter leur périmètre d'intervention aux caractéristiques et aux besoins spécifiques de l'organisation ou de la mission concernée.

Affecter les ressources

Une fois que les objectifs et le périmètre de la mission ont été établis, le responsable de l'audit interne ou les auditeurs internes assignés à la mission doivent prendre en compte la nature et la complexité de la mission, les contraintes de temps et les ressources disponibles avant de déterminer si la quantité de ressources et l'éventail des compétences disponibles sont appropriés pour exécuter la mission avec conscience professionnelle (Norme 2230 – Ressources affectées à la mission).

Pour évaluer l'efficacité d'un processus de management des risques, les auditeurs internes devraient avoir connaissance des exigences du secteur en la matière ainsi que d'une variété de référentiels de risques et de contrôles. Ils devraient aussi comprendre la culture de l'organisation et connaître les autres « soft controls » de l'environnement de contrôle de l'organisation.

L'évaluation du processus complet de management des risques d'une organisation étant un exercice laborieux et chronophage, le responsable de l'audit interne devrait proposer une approche raisonnable en termes d'allocation des ressources. Pour garantir leur adéquation, ces missions peuvent être abordées de plusieurs manières, comme le montre **l'illustration n°4**, en fonction de la structure de l'organisation. Ces exemples ne sont pas exhaustifs.

Illustration 4 : Exemple d'approches de la mission d'audit

Approche descendante	
Méthode la plus efficace pour collecter des informations	■ Entretiens. ■ Analyse documentaire.
Participants	■ Administrateurs (p. ex. membres du comité d'audit et/ou président du comité des risques). ■ Equipe dirigeante. ■ Équipe managériale Groupe et Filiales/Divisions.
Limites	■ Le niveau de détail obtenu est faible. ■ L'évaluation peut se focaliser sur la gouvernance en fonction du groupe de participants. ■ Les points de vue du Conseil et de la direction générale peuvent ne pas être représentatifs du reste de l'organisation, notamment en matière de culture.
Approche ascendante	
Méthode la plus efficace pour collecter des informations	■ Entretiens. ■ Études. ■ Analyse documentaire. ■ Tests de cheminement.
Participants	■ Managers intermédiaires ■ Responsables de service.
Limites	■ Les enquêtes peuvent générer une certaine confusion si un langage du risque ou un processus communs ne sont pas établis. ■ Les retours aux participants peuvent être réalisés de manière aléatoire. ■ De nombreux managers et responsables peuvent être dans l'incapacité de participer en raison de contraintes de ressources ou de temps (ce qui peut être révélateur de la priorité donnée au processus de management des risques).

Illustration 4 : Exemple d'approches de la mission d'audit (suite)

Approche combinée	
Méthode la plus efficace pour collecter des informations	■ Entretiens (cadres supérieurs). ■ Enquêtes (managers intermédiaires). ■ Analyse documentaire.
Participants	■ Administrateurs (p. ex. membres du comité d'audit et/ou président du comité des risques). ■ Équipe dirigeante. ■ Équipe managériale Groupe et Filiales/Divisions. ■ Managers intermédiaires.
Limites	■ Même si cette approche devrait fournir une vision plus exhaustive, toutes les limitations mentionnées précédemment s'appliquent.

Documenter le programme de travail de la mission

Pendant la phase de planification, les auditeurs internes répertorient les informations recueillies dans les documents de travail de la mission. Ces informations deviennent partie intégrante du programme de travail permettant d'atteindre les objectifs de la mission, conformément à la Norme 2240 – Programme de travail de la mission).

Le processus de définition des objectifs et du périmètre d'intervention de la mission peut déboucher sur la production d'un ou plusieurs des documents de travail suivants :

- Cartographies de processus.
- Registres de risques.
- Synthèse des entretiens et études.
- Argumentaire des décisions concernant le niveau de maturité du management des risques de l'organisation.
- Critères qui seront utilisés pour évaluer le processus de management des risques.

Réaliser la mission et communiquer les résultats

L'Annexe E présente, d'une manière générale, les activités que les auditeurs internes peuvent réaliser dans le cadre de l'évaluation du processus de management des risques d'une organisation. Les normes de la série 2300 (Réalisation de la mission) décrivent les exigences requises pour identifier, analyser, évaluer et documenter les informations nécessaires pour atteindre les objectifs de la mission.

La mission devrait aboutir à des recommandations adaptées au statut actuel et souhaité du management en fonction du modèle de maturité. Les auditeurs internes devraient suivre les procédures de communication des résultats établies par la fonction d'audit interne, détaillées dans les normes de la série 2400 (Communication des résultats) et les guides de mise en œuvre correspondants. Les auditeurs internes devraient noter que, pour se conformer à la Norme 2410 - Contenu de la communication et à la Norme 2410.A1, la communication finale des résultats de la mission doit inclure les objectifs, le périmètre d'intervention, les résultats, les conclusions ainsi que les recommandations et/ou les plans d'actions appropriés.

Pour être conforme à la Norme 2440 – Diffusion des résultats, le responsable de l'audit interne doit s'assurer que les résultats sont communiqués aux destinataires appropriés. Les évaluations des processus de management des risques peuvent impliquer l'envoi d'un rapport à la direction générale, au Conseil et à d'autres tiers jugés appropriés. Les communications doivent être adaptées au public visé.

Évaluer le processus de management des risques de l'audit interne

Pour évaluer l'efficacité de l'audit interne et pour identifier les axes d'amélioration, conformément à la Norme 1300 – Programme d'assurance et d'amélioration qualité, le responsable de l'audit interne peut appliquer les enseignements tirés des évaluations du management des risques menées par l'audit interne dans toute l'organisation. L'utilisation d'un modèle de maturité du management des risques (Illustration 1) peut aider le responsable de l'audit interne à améliorer le processus de management des risques de l'audit interne et à atteindre des niveaux de maturité plus élevés. Une plus grande maturité renforce la capacité de l'audit interne à fournir des services d'assurance et de conseil, lui permettant de mieux préserver et accroître la valeur de l'organisation.

Annexe A. Normes et lignes directrices de l'IIA applicables

Les ressources IIA suivantes sont mentionnées dans ce guide pratique. Pour en savoir plus sur l'application des *Normes internationales pour la pratique professionnelle de l'audit interne*, veuillez vous référer aux guides de mise en œuvre.

Code de déontologie
Principe 1 : Intégrité
Principe 2 : Objectivité
Principe 3 : Confidentialité
Principe 4 : Compétence
Normes
Norme 1100 – Indépendance et objectivité
Norme 1112 – Rôles du responsable de l'audit interne en dehors de l'audit interne
Norme 1130 – Atteinte à l'indépendance ou à l'objectivité
Norme 2050 – Coordination et utilisation d'autres travaux
Norme 2120 – Management des risques
Norme 2200 – Planification de la mission
Norme 2201 – Considérations relatives à la planification
Norme 2210 – Objectifs de la mission
Norme 2220 – Périmètre d'intervention de la mission
Norme 2230 – Ressources affectées à la mission
Norme 2240 – Programme de travail de la mission
Norme 2300 – Réalisation de la mission
Norme 2400 – Communication des résultats
Norme 2410 – Contenu de la communication
Norme 2440 – Diffusion des résultats
Lignes directrices
Guide pratique « Rapports d'audit : Communiquer les résultats d'une mission d'assurance », 2016.
Guide pratique « Coordination et utilisation d'autres travaux d'assurance : élaborer une cartographie des prestations d'assurance », 2018.
Guide pratique « Planification de la mission : définir les objectifs et le périmètre d'intervention », 2017.

Annexe B. Glossaire

Les termes marqués d'un astérisque (*) sont issus du glossaire du *Cadre de référence international des pratiques professionnelles* ® (CRIPP) de l'IIA, édition 2017.

Audit interne* – Fonction 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. L'audit interne aide cette organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de gouvernance, de management des risques et de contrôle, en faisant des propositions pour renforcer leur efficacité.

Appétence pour le risque* – Niveau de risque qu'une organisation est prête à accepter.

Conseil* – Le niveau le plus élevé des organes de gouvernance (par exemple, un conseil d'administration, un conseil de surveillance ou un organe délibérant) responsable du pilotage, et/ou de la surveillance des activités de l'organisation et, envers lequel la direction générale a un devoir de rendre compte.
Bien que les mécanismes de gouvernance varient selon les juridictions et les secteurs, le Conseil comprend généralement des membres qui ne font pas partie du management. Si un tel Conseil n'existe pas, le mot « Conseil » dans les *Normes* correspond à un groupe ou à une personne en charge de la gouvernance de l'organisation. En outre, « Conseil » dans les *Normes* peut renvoyer à un comité ou une autre instance auquel l'organe de gouvernance a délégué certaines fonctions (par exemple, un comité d'audit).

Environnement de contrôle* – L'attitude et les 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 des collaborateurs.

Management des risques* – Processus visant à identifier, évaluer, gérer et contrôler les événements ou les situations potentiels pour fournir une assurance raisonnable quant à la réalisation des objectifs de l'organisation.

Modèle de maturité – Indicateurs servant à mesurer le niveau de maîtrise actuel d'un domaine donné par une organisation ainsi que les progrès réalisés.

Responsable de l'audit interne* – désigne une personne, occupant un poste hiérarchique de haut niveau, qui a la responsabilité de diriger efficacement la fonction d'audit interne conformément à la charte d'audit interne et aux dispositions obligatoires du *Cadre de référence international des pratiques professionnelles de l'audit interne*. Le responsable de l'audit interne ou des personnes qui lui sont rattachées de l'audit interne devront disposer des certifications et des qualifications professionnelles appropriées. L'intitulé exact du poste et/ou de la fonction du responsable de l'audit interne varie selon les organisations.

Annexe C. Scénarii potentiels de risque

Pour assurer le succès de l'organisation et créer de la valeur, tous les risques organisationnels significatifs, y compris les risques d'opportunités manquées, doivent être clairement compris, priorisés et traités. Évaluer de manière appropriée le processus de management des risques et fournir une assurance aide les organisations à mettre en œuvre des actions appropriées pour prévenir ou gérer les scénarii de risques susceptibles de compromettre leur capacité à atteindre leurs buts et objectifs, tels que ceux listés ci-dessous :

- L'assurance indépendante fournie au Conseil et à la direction générale est inadaptée et les amène à croire, à tort, que les risques sont gérés en accord avec le niveau d'appétence pour le risque de l'organisation, et qu'ils soutiennent sa capacité à réaliser ses objectifs et stratégies.
- La gouvernance du management des risques, ses systèmes et processus sont défaillants, donnant lieu à une mauvaise gouvernance d'entreprise ainsi qu'à des notes tout aussi faibles de la part des agences de notation, qui sont ensuite communiquées aux parties prenantes et au marché.
- Des risques pouvant être évités se réalisent et entraînent un engagement de responsabilité, des amendes ou sanctions et de nombreuses conséquences associées ainsi que la mise en péril des actifs, de la propriété intellectuelle, des parts de marché, des opportunités de revenus, de la fidélité des clients, et de la réputation de la marque.
- L'allocation de ressources et l'attribution des rôles ne sont pas optimisées ; par conséquent, un management des risques durable sur le plan opérationnel ne peut être mis en place.
- La culture de l'organisation freine les progrès pour atteindre un niveau de maturité de management des risques plus élevé.
- Les risques sont soit ignorés, soit mal priorisés ou maîtrisés de façon inefficace, ce qui conduit à l'émergence de risques qui empêchent l'atteinte des objectifs opérationnels et organisationnels et la réalisation de la stratégie.
- Les contraintes de temps ne sont pas respectées et les opportunités ne se concrétisent pas en raison d'une mauvaise gestion des risques.
- Les priorités et stratégies de l'organisation ne sont pas définies en tenant compte des risques ou des facteurs de risques à l'origine des initiatives.
- Les risques liés aux SI, aux ressources humaines et au financement ne sont pas pris en compte et génèrent des pertes financières et opérationnelles ou des défaillances stratégiques.

Annexe D. Matrice des risques et des contrôles

Le tableau suivant énumère certains des principaux domaines de risque et contrôles que les auditeurs internes devraient prendre en considération quand ils évaluent le processus de management des risques d'une organisation. Cette liste n'est ni exhaustive, ni destinée à être utilisée comme un programme de travail ou une liste de contrôles.

Risques liés à la culture	
Risques	**Dispositifs de contrôle**
■ Aucune ressource n'a été allouée au développement du management des risques. ■ Le risque est perçu comme « la propriété » des auditeurs internes et des fonctions de contrôle. ■ Il est difficile de planifier des entretiens et de recevoir les résultats d'enquêtes en temps utile. ■ Les mauvaises nouvelles ne remontent pas dans l'organisation. ■ Impliquer toute l'organisation présente des difficultés inattendues ou plus importantes que prévu. ■ L'organisation ne prend pas en compte les résistances internes au changement. ■ L'organisation perçoit le processus de management des risques comme une obligation. ■ L'audit interne n'a pas rapporté ni expliqué les constats et les cotations de risque de manière efficace. ■ Le management craint une exposition aux risques. ■ Les traditions culturelles sont opposées aux objectifs de management des risques.	■ L'audit interne conduit des ateliers ou des entretiens pour guider les collaborateurs dans le processus de management des risques. ■ Le Conseil représente l'exemplarité au plus haut niveau. ■ Les forums confidentiels permettent aux collaborateurs de s'exprimer sur des questions culturelles ou sur des obstacles à la communication d'informations sur les risques. ■ La direction générale encourage les réunions et les discussions régulières ainsi que l'échange d'informations à tous les niveaux de la chaîne managériale. ■ La direction veille à ce que la remontée d'informations sur les risques dans l'organisation n'entraîne pas de représailles.

Risques liés à la gouvernance	
Risques	**Dispositifs de contrôle**
■ Les entités (Conseil, direction, régulateurs) ont des exigences différentes en matière de management des risques. ■ Il n'existe pas de système de reporting standard pour les problèmes de management des risques (p. ex. rapidité, format). ■ La direction n'aborde pas régulièrement les risques dans les réunions. ■ Le Conseil ne remplit pas son rôle de surveillance de manière adéquate.	■ Les critères internes et externes de management des risques sont connus et intégrés au processus. ■ L'organisation investit dans un logiciel de reporting des risques. ■ Le Conseil et l'équipe dirigeante instaurent une exigence d'informations sur les risques diffusée au sein de l'organisation.

Annexe D. (suite)

Risques liés au processus	
Risques	**Dispositifs de contrôle**
■ Le processus d'évaluation des risques n'est pas cohérent dans toute l'organisation. ■ Un trop grand nombre de risques sont identifiés. ■ Les conséquences des risques ne sont pas suivies. ■ Les critères d'impact et de probabilité diffèrent, même pour des lignes métier similaires. ■ Le reporting concernant le traitement des risques s'arrête au niveau du superviseur. ■ L'audit interne est la seule entité qui effectue une évaluation des risques à l'échelle de l'organisation. ■ Le processus de management des risques implique un langage et une terminologie que les collaborateurs ne comprennent pas. ■ Le niveau attendu pour la mesure quantitative de l'exposition aux risques (en valeur réelle) n'est pas fixé. ■ L'attention portée aux risques émergents n'est pas suffisante.	■ L'organisation s'accorde sur le(s) référentiel(s) de management des risques à utiliser. ■ L'organisation investit des ressources dans le regroupement d'informations sur les risques et le reporting à intervalles réguliers. ■ Les fonctions de contrôle (p. ex. conformité/ juridique/ environnement santé et sécurité) sont bien formées au processus d'évaluation des risques et au référentiel de management des risques adopté par le management. ■ Un glossaire des termes liés au management des risques et une description du processus d'évaluation des risques sont fournis avant de procéder aux évaluations des risques. ■ Les matrices d'impact et de probabilité sont mises en œuvre de manière cohérente dans toute l'organisation.

Annexe E. Évaluation du processus de management des risques

D'une manière générale, ces tableaux décrivent les activités effectuées par les auditeurs internes dans le cadre de l'évaluation du processus de management des risques d'une organisation. Ces activités ne constituent pas le programme de travail exhaustif de l'évaluation en question. En effet, les auditeurs internes peuvent être amenés à créer des analyses plus détaillées et des étapes de test adaptées aux politiques et procédures propres à l'organisation. Pour mener une évaluation complète du processus de management des risques, les auditeurs internes peuvent également avoir besoin de concevoir des programmes de travail spécifiques à certains domaines (par ex. risque juridique, risque de conformité, planification stratégique), en particulier si l'évaluation est divisée en missions de moindre ampleur comme mentionné dans ce guide.

Culture du management des risques

Reporting des risques

- Réunir les documents suivants :
  - Chartes, politiques et autres informations nécessaires aux organes de gouvernance en charge de l'établissement et de la supervision du processus de management des risques.
  - Documentation de toutes les phases du processus de reporting des risques.
- Avoir une idée précise des principaux risques identifiés comme liés aux objectifs de l'organisation.
- Déterminer si le reporting rend réellement compte du degré d'exposition aux risques au sein de l'organisation (p. ex : est-il trop compliqué ou trop simple ?).
- Noter les risques selon la méthodologie d'évaluation des risques établie par l'organisation.
- Examiner les informations recueillies lors de l'évaluation préliminaire des risques afin d'apprécier l'impact et la probabilité de ceux liés à la culture du risque.

Communication

- Suivre le reporting des risques dans plusieurs activités pour vérifier si les informations relatives aux risques sont communiquées de manière fluide à tous les niveaux de l'organisation.
- Prendre connaissance des investigations en matière d'éthique et de conformité pour déterminer si la communication d'informations sur les risques entraîne des représailles.
- Utiliser les sondages, les entretiens ou d'autres méthodes pour s'assurer de la participation des collaborateurs aux programmes de communication et de leur niveau de compréhension de l'appétence pour le risque de l'organisation.

Devoir de rendre compte

- Confirmer que les propriétaires des risques sont effectivement tenus responsables des expositions aux risques dans leur périmètre de responsabilités.
- Confirmer que le Conseil et la direction générale sont tenus responsables de l'exigence d'informations sur les risques et de l'utilisation de ces dernières dans la prise de décision.

Annexe E. (suite)

Gouvernance du management des risques

Reporting des risques

- Utiliser les informations communiquées sur les risques pour évaluer la culture et examiner la pertinence en termes de diffusion, suivi et conservation des données.
- Examiner les informations recueillies lors de l'évaluation préliminaire des risques afin d'apprécier l'impact et la probabilité de ceux liés à la culture du risque.

Reporting au Conseil

- Examiner les rapports sur les risques préparés pour le Conseil. Veiller à ce qu'ils contiennent toutes les informations pertinentes dont le Conseil a besoin pour prendre des décisions éclairées.
- Examiner les rapports de la direction générale sur le niveau d'exposition aux risques par rapport aux stratégies et à l'appétence pour le risque.

Appétence pour le risque

- Examiner le profil d'appétence pour le risque de l'organisation pour s'assurer qu'il est exhaustif et approprié et qu'il contient les éléments suivants :
  - Capacité à supporter le risque : Le niveau maximal de risque que l'organisation peut assumer étant donné le niveau actuel de ses ressources, contraintes et obligations.
  - Limites de risque : L'allocation des limites agrégées de l'appétence pour le risque à des lignes métier, des entités juridiques, des catégories de risques spécifiques et d'autres niveaux plus fins pertinents.
  - Tolérance au risque : L'écart que l'organisation acceptera en matière de recettes et de dépenses, etc., compte tenu des paramètres définis en termes de capacité à supporter le risque et de leurs limites associées.
- Revoir les plans et les processus pour communiquer l'appétence pour le risque à tous les collaborateurs.
- S'assurer que le plan couvre toute l'organisation et qu'il est régulièrement réalisé.
- Utiliser des enquêtes, des entretiens ou toute autre méthode pour vérifier à la fois la participation des collaborateurs aux programmes de communication et leur niveau de compréhension de l'appétence pour le risque de l'organisation.

Processus de management des risques

Politiques et procédures

- Vérifier que les politiques et procédures sont actualisées et mises à jour en temps opportun suite à un changement significatif des pratiques.
- Confirmer que toutes les mises à jour demandées par le Conseil au cours de la revue annuelle ont été effectuées correctement.
- S'assurer que les politiques et procédures couvrent en détail l'ensemble du processus de management des risques. Des domaines spécifiques particulièrement importants sont :
  - Les liens avec les stratégies et l'appétence pour le risque ;
  - la présentation générale de la gouvernance ;
  - Les limites de risque, et degrés de tolérance, les éléments déclencheurs et protocoles d'escalade qui leur sont associés (suivre pas à pas le processus de l'identification d'une faille jusqu'à sa résolution) ;
  - Les rôles et responsabilités ;
  - Les éléments à prendre en considération sur les données.
- Les obligations réglementaires.

Processus d'évaluation des risques

- Déterminer où et à quelle fréquence les évaluations des risques sont effectuées à l'échelle de l'organisation.
- Examiner la cohérence des processus d'identification, d'évaluation, de traitement, de suivi et de reporting des risques.
- Examiner les informations recueillies lors de l'évaluation préliminaire des risques afin d'apprécier l'impact et la probabilité des risques liés aux processus de management des risques en place dans toute l'organisation.

Annexe F. Références et sources bibliographiques supplémentaires

Références

Cadre de référence International des pratiques professionnelles de l'audit interne (CRIPP), édition 2017. Lake Mary, Floride : The Institute of Internal Auditors, 2017.

Autres sources bibliographiques

Anderson, Richard J. and Mark L. Frigo. *Assessing and Managing Strategic Risks: What, Why, How for Internal Auditors.* Lake Mary : Fondation d'audit interne, 2017. https://bookstore.theiia.org/assessing-and-managing-strategic-risks.

Anderson, Urton and Andrew J. Dahle. *Applying the International Professional Practices Framework, 4th Edition.* Lake Mary : Fondation d'audit interne, 2018. https://bookstore.theiia.org/applying-the-international-professional-practices-framework-4th-edition-2.

Baker, Larry L. *Practical Enterprise Risk Management: Getting to the Truth*. Lake Mary : Fondation d'audit interne, 2018. https://bookstore.theiia.org/practical-enterprise-risk-management-getting-to-the-truth.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). *Le management des risques de l'entreprise – Une démarche intégrée à la stratégie et à la performance.* COSO, 2017. https://bookstore.theiia.org/enterprise-risk-management-integrating-with-strategy-and-performance.

Committee of Sponsoring Organizations of the Treadway Commission. *Le management des risques de l'entreprise – Une démarche intégrée à la stratégie et à la performance : Compendium of Examples.* PwC, 2018. https://bookstore.theiia.org/coso-enterprise-risk-management-integrating-with-strategy-and-performance-compendium-of-examples.

International Organization for Standardization (ISO). ISO 31000:2018, *Risk management – Guidelines*. ISO, 2018. https://www.iso.org/standard/65694.html.

Sobel, Paul J. *Auditor's Risk Management Guide: Integrating Auditing and ERM, 2015 Edition*. Wolters Kluwer, 2015.

Sobel, Paul J. *Managing Risk in Uncertain Times: Leveraging COSO's New ERM Framework*. Lake Mary, Fondation d'audit interne, 2018. https://bookstore.theiia.org/managing-risk-in-uncertain-times-2.

Remerciements

Équipe de projet

Glenn Ho, CIA, CRMA, Afrique du Sud (Chairman)
Hans-Peter Lerchner, CIA, Autriche (Project Lead)
Susan Haseley, CIA, Etats-Unis
Rune Johannessen, CIA, CCSA, CRMA, Norvège
Ian Lyall, CIA, CCSA, CGAP, CRMA, Australie
Michael Lynn, CRMA, Etats-Unis
Denis Neukomm, CIA, CRMA, Suisse

Contributeurs

Mohamed Ahmed Abdulla, Egypte
Lance Johnson, CIA, CRMA, Etats-Unis
Cornelis Klumper, CIA, Etats-Unis
Steven Nyakatuura, CFSA, Afrique du Sud
Tejinder Bob Shahi, CIA, Canada
Rita Thakkar, CIA, Etats-Unis

Collaborateurs de l'IIA Global en charge des Normes et des lignes directrices

Anne Mercer, CIA, CFSA, Director (Project Lead)
Jim Pelletier, CIA, CGAP, Vice President
Cassian Jae, Managing Director
Jeanette York, CCSA, FS Director
Shelli Browning, Technical Editor
Lauressa Nelson, Technical Editor

Réviseurs de la traduction française

Marie-Elisabeth Albert, CIA
Jerôme Cantiant
Jean-François Charbonnier
Julien Cornuché, CIA, CISA
Vianney Dumont, CIA
Charlotte Gabet
Béatrice Vedrenne Robson

L'IIA souhaite remercier les instances suivantes pour leur soutien : Financial Services Guidance Committee, Guidance Development Committee, Information Technology Guidance Committee, Public Sector Guidance Committee, Professional Guidance Advisory Council, International Internal Audit Standards Board, Professional Responsibility and Ethics Committee, et International Professional Practices Framework Oversight Council.

À propos de l'IIA

Porte-parole mondial de la profession d'audit interne, l'*Institute of Internal Auditors* (IIA) est une autorité reconnue et un leader incontesté dans la formation et la formulation de normes, lignes directrices et certifications. Fondé en 1941, l'IIA, dont le siège mondial se situe à Lake Mary (Floride, États-Unis), compte actuellement quelque 190 000 membres dans plus de 170 pays et territoires. Plus d'informations sont disponibles sur le site www.globaliia.org / www.theiia.org.

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 est seulement destinée à servir de guide. L'*Institute of Internal Auditors* vous recommande de toujours solliciter un expert indépendant pour avoir un avis dans chaque situation. L'IIA dégage sa responsabilité pour les cas où des lecteurs se fieraient exclusivement à ce guide.

Copyright

Copyright© 2019 *The Institute of Internal Auditors, Inc.* Tous droits réservés. Pour l'autorisation de reproduction, prière de contacter l'*Institute of Internal Auditors* à l'adresse guidance@theiia.org.

Juillet 2019 – ISBN: 978-2-915042-98-6

The Institute of Internal Auditors | *Global*

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101
www.theiia.org