CRIPP

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

Lignes directrices complémentaires

Guide pratique

Coordination et utilisation d'autres travaux d'assurance

Élaborer une cartographie des prestations d'assurance

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.

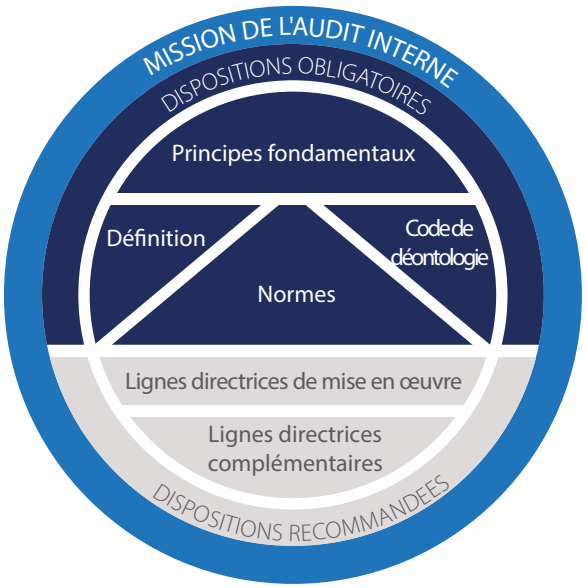
Les dispositions obligatoires sont élaborées selon un processus de diligence raisonnable qui inclut une consultation publique pour la prise en compte des avis des parties prenantes.

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
Élaborer une cartographie des prestations d'assurance 5
Identifier les sources d'information sur les risques 6
Organiser les risques par catégories de risques 8
Identifier les prestataires d'activités d'assurance 8
Consolider les informations et documenter le niveau de couverture des activités d'assurance 10
Revoir et mettre à jour régulièrement la cartographie des prestations d'assurance 12
Utilisation des cartographies des prestations d'assurance 12
Annexe A. Normes et lignes directrices de l'IIA applicables 14
Annexe B. Glossaire 15
Annexe C. Cadres de référence concernant les risques 16
Remerciements 17

Synthèse

Une des principales responsabilités du Conseil est d'obtenir l'assurance que les processus d'une organisation fonctionnent selon les paramètres fixés pour atteindre les objectifs définis. Pour ce faire, les processus de management des risques fonctionnent efficacement en traitant les risques significatifs pour les maintenir à des niveaux acceptables. Le Conseil s'appuie sur les informations provenant de multiples prestataires d'activités d'assurance, y compris les prestataires internes (par exemple, la gestion des risques, la conformité et les autres fonctions de contrôle ainsi que l'audit interne) et les prestataires externes (par exemple les auditeurs externes et les consultants).

Une cartographie des prestations d'assurance est une matrice, représentation visuelle des risques d'une organisation et de tous les prestataires internes et externes d'assurance relative à ces risques. Cette représentation révèle les lacunes et les doubles emplois. Les prestataires d'assurance peuvent utiliser cette cartographie pour coordonner le calendrier et le périmètre d'intervention de leurs activités, évitant une lassitude vis-à-vis des vérifications (« fatigue de l'audit ») dans des domaines et processus audités, sauf si la direction générale ou le Conseil ont besoin d'une seconde opinion ou d'une vérification par un autre prestataire d'assurance sur un domaine de risque élevé.

Une cartographie des prestations d'assurance pourra être utilisée par différents services de l'organisation :

- l'audit interne peut utiliser une cartographie des prestations d'assurance comme une base de discussion pour déterminer si le recours au travail d'autres prestataires d'assurance serait approprié ;
- la direction générale peut utiliser cette cartographie pour s'assurer que les fonctions de gestion des risques et de contrôle interne sont en phase et pilotées de manière efficace.

Ainsi, une cartographie des prestations d'assurance peut améliorer un processus global de management des risques à l'échelle de l'organisation, faire progresser la maturité des fonctions d'assurance et renforcer l'environnement de contrôle.

L'objectif principal de ce guide pratique est d'aider les auditeurs internes dans l'élaboration d'une cartographie des prestations d'assurance pour documenter leur niveau de couverture et permettre une utilisation efficiente des ressources liées aux activités d'assurance en minimisant la duplication des travaux.

Introduction

Différents prestataires d'**activités d'assurance** contribuent au cadre global de gestion des risques et de contrôle à l'échelle de l'organisation, en donnant collectivement une assurance que les **risques** sont identifiés et traités à un niveau acceptable. Cependant, ces prestataires diffèrent selon leurs responsabilités en matière de reporting, leur niveau d'**indépendance** par rapport aux activités à propos desquelles ils donnent une assurance, et la fiabilité de l'assurance qu'ils fournissent.

Remarque : Les termes en gras sont définis dans le glossaire à la fin de ce guide pratique.

Les responsabilités en matière d'assurance étant réparties entre les trois lignes de maîtrise[1], il est important de documenter ces activités. Une compréhension précise de la couverture des risques à travers l'organisation est bénéfique à plusieurs titres, notamment en termes de réduction de la duplication des travaux d'assurance et de prévention de la « fatigue de l'audit » parmi les entités auditées. Si la couverture des activités d'assurance est insuffisante, des risques significatifs pourraient être négligés ou mal évalués. En coordonnant et en ajustant leur couverture des risques, les prestataires d'assurance peuvent bâtir un cadre de référence solide. Une cartographie des prestations d'assurance peut être élaborée à la demande de la direction générale ou du **Conseil** ; en particulier le comité d'audit ou le comité des risques, ou à l'initiative de l'audit interne.

Élaborer une cartographie des prestations d'assurance

L'élaboration d'une cartographie des prestations d'assurance devrait être un travail collaboratif, impliquant chaque prestataire d'activités d'assurance. L'audit interne peut bénéficier de la meilleure perspective pour initier la création d'une cartographie holistique des prestations d'assurance à l'échelle de l'organisation. Une fois la cartographie crée, elle peut être confiée à la fonction d'assurance la plus appropriée dans l'organisation. N'importe quelle fonction de management des risques – gestion des risques, conformité, juridique, finance ou audit interne – pourra mettre à jour cette cartographie des prestations d'assurance.

Activités d'assurance

L'objectif des activités d'assurance est de fournir un examen objectif d'éléments probants provenant d'une évaluation indépendante sur les processus de gouvernance, de management des risques et de contrôle. Parmi les exemples, on peut citer les travaux concernant la finance, la performance, la conformité, la sécurité des systèmes et les *due dilligence*.

Comme l'audit interne est la fonction la plus susceptible d'utiliser la cartographie des prestations d'assurance pour l'élaboration de son plan d'audit, c'est donc logiquement l'entité à qui la responsabilité de créer et de mettre à jour cette cartographie est confiée. Les autres prestataires d'assurance sont moins susceptibles d'utiliser cette cartographie à des fins de planification, dans la mesure où leurs activités sont en grande partie des évaluations obligatoires exigées par la réglementation ou par une autre entité externe. S'il existe une fonction de management des risques à l'échelle de l'organisation ou une fonction de planification stratégique qui réalisent une évaluation annuelle des risques, ces fonctions peuvent être d'autres attributaires naturels de la cartographie des prestations d'assurance.

[1] Prise de position de l'IIA, « Les trois lignes de maîtrise pour une gestion des risques et un contrôle efficaces », janvier 2013.

Dans sa forme la plus simple, une cartographie des prestations d'assurance peut consister en une matrice comprenant dans la première colonne les catégories de risque de l'organisation, avec des colonnes supplémentaires dont l'intitulé correspond à chaque prestataire d'assurance. Elle permet ainsi d'identifier le niveau de couverture des activités d'assurance pour chaque catégorie de risques à travers l'organisation. La cartographie des prestations d'assurance peut être aussi simple ou aussi compliquée que le souhaite l'organisation. Cependant, les principales étapes pour élaborer une cartographie des prestations d'assurance restent inchangées, quelle que soit la conception.

Les étapes d'une cartographie des prestations d'assurance comprennent :

1. l'identification des sources d'information sur les risques ;
2. l'organisation des risques en catégories de risque pour avoir une vision consolidée ;
3. l'identification des prestataires d'activités d'assurance ;
4. la consolidation d'informations et la documentation des activités d'assurance par catégorie de risques ;
5. la revue, le suivi et la mise à jour régulière de la cartographie des prestations d'assurance.

Identifier les sources d'information sur les risques

Le management des risques dans une organisation est une responsabilité partagée par chacun ; par conséquent, des informations sur les risques existeront dans pratiquement tous les domaines, qu'elles soient explicites ou non. Les risques peuvent être explicitement évalués dans des processus tels que la planification stratégique. Ils peuvent être cités dans des *business cases* (par exemple, « ce projet pourrait générer moins de chiffre d'affaires que prévu à cause des facteurs suivants... ») comme illustré dans la **figure n° 1**. Les auditeurs internes ne devraient pas se limiter à utiliser des rapports ou des évaluations explicites des risques. Les principaux documents à examiner dans une organisation pourraient comprendre :

- la (es) déclaration(s) relative(s) à l'**appétence pour le risque** ;
- les documents concernant la stratégie ;
- les évaluations des risques ;
- les politiques ;
- les rapports de contrôle ou autres rapports du management qui contiennent des informations sur la performance ;
- les comptes-rendus du Conseil ;
- les comptes-rendus du comité d'audit ;
- les *business cases* de projets d'investissement significatifs ;
- les rapports périodiques (par exemple, les rapports annuels 10-K des sociétés cotées exigés par la Security Exchange Commission).

Figure n° 1 : Exemple de *business case*

Business case

Centre d'urgence autonome
Agence hospitalière de X-ville

Nous recommandons que l'agence hospitalière de X-ville investisse dans un centre d'urgence autonome dans le quartier « Briques Rouges » pour les raisons suivantes :

1. la zone est mal desservie ;
2. la zone a un taux de criminalité élevé ;
3. la salle d'urgence la plus proche en cas de traumatisme est à une heure.

les études de marché ont montré...
les concurrents ont fait...
les coûts du projet sont estimés à...
les recettes sont estimées à :

Fourchette haute	Estimation moyenne	Fourchette basse
1 500 000 / année 1	1 000 000 / année 1	750 000 / année 1

Facteurs explicatifs de l'estimation basse :

- projet d'envergure ;
- démarrage tardif dans l'année (conditions météorologiques) ;
- manque d'expérience dans la construction et le fonctionnement d'un centre d'urgence autonome ;
- personnel non disponible ;
- incapacité à former du personnel.

Informations relatives aux risques

L'audit interne ne devrait pas s'appuyer uniquement sur sa propre expérience pour identifier les informations relatives aux risques. Alors même que l'univers des risques auditables de l'audit interne est utile, il peut ne pas représenter une image complète des risques significatifs d'une organisation. L'élaboration d'une cartographie des prestations d'assurance est censée être un processus collaboratif ; par conséquent, les auditeurs internes devraient y faire participer en amont les opérationnels et les fonctions de contrôle concernées.

Organiser les risques par catégories de risques

L'univers des risques correspond à l'ensemble des risques qui pourraient survenir dans une organisation. Il y a une multitude d'approches et de mesures des risques, dont certaines sont spécifiques à une unité opérationnelle ou une fonction donnée. Cependant, pour éviter les lacunes ou les doubles emplois dans la fourniture d'assurance au Conseil, les risques de l'organisation doivent être organisés afin d'en donner une vision holistique et cohérente. Les organisations classent généralement les risques selon les fonctions, les unités, les processus ou les programmes opérationnels et certaines peuvent utiliser un cadre de référence pour le management des risques à l'échelle de l'organisation (Voir l'annexe C pour une liste des cadres de référence qui pourraient guider ce processus si vous n'en utilisez pas déjà un dans votre organisation).

À un niveau macro, les catégories de risques devraient correspondre aux objectifs stratégiques de l'organisation. Des catégories de risques supplémentaires peuvent couvrir des domaines ou des processus opérationnels et de conformité ainsi que les risques concernant le reporting. Les domaines de risques significatifs sont ainsi pris en compte. Quelle que soit l'approche utilisée, chaque risque individuel doit être classé pour synthétiser les informations et les rendre accessibles pour une communication au Conseil et à la direction générale selon les besoins.

Comme décrit ci-dessus, la première colonne d'une cartographie des prestations d'assurance énumère généralement les catégories de risques qui ont été identifiées dans les évaluations des risques à travers l'organisation (cf. figure n° 2). S'il n'existe ni évaluation formalisée des risques et reporting, ni une vision partagée sur les risques, alors les prestataires d'assurance devraient se réunir pour élaborer une vision commune et agréer une catégorisation des risques.

Figure n°2 : Exemple de catégories de risques

Stratégiques	
	Gestion de crise
	Environnement concurrentiel
	Affectation des ressources
	...
Opérationnels	
	Qualité des produits
	Capacité de production
	Fournisseurs et principaux partenaires
	...
Ressources humaines	
	Plan de succession
	Formation
	Mobilité
	...
Financiers	
	Reporting financier
	Comptes créditeurs
	Comptes débiteurs
	...
Conformité réglementaire & reporting	
	Communication externe
	Reporting environnemental
	Données personnelles
	...
Systèmes d'information	
	Sécurité des données
	Disponibilité et efficacité du matériel informatique
	Facilité d'utilisation et efficience des logiciels
	...

Identifier les prestataires d'activités d'assurance

Un concept qui pourrait aider l'audit interne à identifier les prestataires d'assurance au sein de l'organisation est le modèle des trois lignes de maîtrise qui distingue, selon des rôles et responsabilités clés, les acteurs

internes du management des risques en trois principaux groupes (ou lignes de maîtrise). Les deux premières lignes de maîtrise comprennent les propriétaires des risques qui sont rattachés à la direction générale. La troisième ligne de maîtrise – la fonction d'audit interne – a un double rattachement à la direction générale et au Conseil. Des activités d'assurance supplémentaires peuvent être fournies par des acteurs externes tels que des consultants.

Première ligne de maîtrise – le management opérationnel

Le management opérationnel, ou ligne hiérarchique, est responsable du maintien d'un contrôle interne efficace dans les systèmes et les processus. En tant que « propriétaire de risques », ce groupe s'assure que les risques opérationnels sont traités et que les objectifs opérationnels sont atteints.

Cette ligne de maîtrise peut manquer d'indépendance et d'**objectivité**, mais elle apporte une contribution précieuse, car elle donne le point de vue des collaborateurs en prise avec les activités et les problèmes quotidiens. Ces propriétaires de risques devraient aider à compléter la cartographie des prestations d'assurance en fonction de leurs rôles et responsabilités. L'audit interne devrait communiquer avec la direction générale si des propriétaires de risques ne peuvent pas être identifiés pour des risques clés.

La direction générale peut avoir l'assurance que la première ligne s'acquitte de ses responsabilités en matière de gestion des risques grâce à l'élaboration et la mise en œuvre de politiques et de bonnes pratiques, d'indicateurs de performance et/ou de tableaux de bord, qui peuvent être mis à jour et suivis selon l'appétence pour le risque de l'organisation. Ce dispositif, complété par les opinions des deuxième et troisième lignes de maîtrise, constitue le fondement d'un programme complet de management des risques. Il est aussi utile de préciser les outils de management qui donnent des informations utiles aux propriétaires de risques dans les cartographies des prestations d'assurance.

Deuxième ligne de maîtrise – les fonctions de gestion des risques et de conformité

Les fonctions de gestion des risques et de conformité assurent la supervision des activités réalisées par la première ligne de maîtrise. Ces fonctions donnent également l'assurance que les exigences réglementaires, environnementales, déontologiques et d'assurance qualité, ou concernant éventuellement d'autres domaines, sont respectées. Les fonctions de conformité assurent le suivi des obligations réglementaires liées à la santé et à la sécurité, à l'environnement, aux chaînes d'approvisionnement, etc. Les activités de la deuxième ligne pourraient aussi consister à évaluer la précision et l'exhaustivité des rapports fournis par la première ligne de maîtrise et à examiner des processus automatisés de suivi et des bases de données de l'organisation.

Les fonctions d'assurance de la deuxième ligne sont généralement plus objectives que le management opérationnel, mais elles font toujours partie du management, et par conséquent, elles ne sont pas indépendantes au sein de l'organisation. Les informations provenant des domaines de risques couverts par les fonctions de la deuxième ligne, y compris les résultats de leurs évaluations et l'étendue et la qualité de leurs travaux, sont une contribution précieuse à la cartographie des prestations d'assurance et aident les auditeurs internes à évaluer si les activités d'assurance sont bien gérées.

Troisième ligne de maîtrise – la fonction d'audit interne

En tant que troisième ligne de maîtrise, la fonction d'audit interne fournit à la direction générale et au Conseil une évaluation indépendante et objective des processus de gouvernance, de management des risques et de contrôle de l'organisation et contribue à l'amélioration de ces processus (Norme 2100 – Nature du travail). En conformité avec la Norme 1000 – Mission, pouvoirs et responsabilités et les Normes de mise en œuvre 1000.A1 et 1000.C1, la nature des **activités de conseil** et d'assurance sont définies dans la charte d'audit interne, qui est approuvée par la direction générale et par le Conseil. Lors de l'établissement de la charte d'audit interne, le responsable de l'audit interne interagit avec la direction générale et le Conseil pour déterminer leurs besoins en matière d'assurance.

Prestataires externes d'activités d'assurance

Une organisation peut avoir recours à divers consultants et spécialistes externes pour obtenir une assurance dans les domaines prévus par la réglementation ou parce qu'une tierce opinion est souhaitée. Ces consultants peuvent avoir des informations cruciales sur les risques et/ou nécessiter d'être inclus dans la cartographie des prestations d'assurance. L'audit interne devrait examiner les recours de l'organisation à des prestataires externes d'assurance et déterminer dans quelle mesure leurs activités devraient être incluses dans la cartographie des prestations d'assurance.

Consultants externes et spécialistes :

- Consultants en gestion des risques
- Cabinets d'avocats
- Cabinets de commissaires aux comptes et/ou d'experts comptables agréés
- Spécialistes en finance ou fraude liée aux états financiers
- Consultants en environnement, santé et sécurité
- Consultants en systèmes d'information (études comparatives, fournisseurs de logiciels, protection antivirus, maintenance)
- Analystes de marché
- Partenaires dans le cadre d'une coentreprise (joint venture)
- Sociétés privées de sécurité

Consolider les informations et documenter le niveau de couverture des activités d'assurance

Une fois les catégories de risques énumérées dans la première colonne de la cartographie des prestations d'assurance, des colonnes supplémentaires sont créées pour documenter le niveau de couverture par chaque prestataire d'assurance. L'audit interne peut juger utile d'organiser les colonnes en distinguant les prestataires internes des prestataires externes et de les regrouper en utilisant le modèle des trois lignes de maîtrise, comme illustré dans la **figure n° 3**. Visuellement, ces regroupements donnent une indication générale du niveau d'indépendance de chaque prestataire. Ces informations peuvent ultérieurement aider le responsable de l'audit interne pour la planification des missions.

Le responsable de l'élaboration de la cartographie devrait rencontrer les propriétaires de risques et les prestataires d'assurance afin de valider les risques qu'ils couvrent et pour combler d'éventuelles lacunes dans les informations recueillies. Idéalement, chaque prestataire d'assurance complète la colonne qui le concerne dans la cartographie, en décrivant ses activités pour chaque catégorie de risques. L'audit interne devrait éviter d'émettre des hypothèses sur le périmètre de responsabilité et le niveau de couverture des risques d'autres prestataires d'assurance.

Figure n° 3 : exemple de cartographie des prestations d'assurance

Catégories de risques	Management 1ère ligne											Surveillance fonctionnelle 2ème ligne							Independante 3ème ligne				
	Finance	Ressources humaines	Trésorerie	Opérations	SI	Achats	Marketing	Juridique	Budget et planification	Communication	…	Processus de management des risques	Comité de pilotage de la performance	Instance de revue de la sécurité	Equipe de gestion de l'environnement	Comité de développement des réseaux	Comité de pilotage des SI	…	Fonction d'audit interne	Auditeurs qualité externes	Consultants en matière d'environnement, de santé et de sécurité	Consultants en gestion des risques	…
Stratégiques																							
Gestion de crise																							
Environnement concurrentiel																							
Affectation des ressources																							
…																							
Opérationnels																							
Qualité des produits																							
Capacité de production																							
Fournisseurs et principaux partenaires																							
…																							
Ressources humaines																							
Plan de succession																							
Formation																							
Mobilité																							
…																							
Financiers																							
Reporting financier																							
Comptes créditeurs																							
Comptes débiteurs																							
…																							
Conformité réglementaire et reporting																							
Communication externe																							
Reporting environmental																							
Données personnelles																							
…																							
Systèmes d'information																							
Sécurité des données																							
Disponibilité et efficacité du matériel informatique																							
Facilité d'utilisation et efficience des logiciels																							
…																							

- Couverture totale des risques
- Couverture partielle des risques
- Couverture des risques limitée ou inexistante
- Domaine de risques hors du périmètre de responsabilité

Revoir et mettre à jour régulièrement la cartographie des prestations d'assurance

Les processus relatifs aux risques, au management des risques et aux activités d'assurance sont continus et dynamiques, et la cartographie des prestations d'assurance devrait être à cette image. L'organisation devrait adopter un processus de revue et de mise à jour régulière de la cartographie des prestations d'assurance avec la contribution de tous les prestataires d'assurance internes et externes. Des évènements peuvent modifier la cartographie des prestations d'assurance, parmi ceux-ci :

- les fusions-acquisitions ;
- le lancement d'une nouvelle gamme de produits ;
- des changements économiques ;
- des changements dans la réglementation ;
- des changements dans le comportement des clients.

Si l'audit interne a en charge la cartographie des prestations d'assurance, il devrait s'assurer qu'elle est mise à jour au moins une fois par an. L'audit interne peut également envisager de demander ou d'entreprendre une révision de la cartographie si des changements significatifs sont identifiés. La cartographie des prestations d'assurance restera ainsi utile à l'organisation.

Utilisation des cartographies des prestations d'assurance

Les cartographies des prestations d'assurance sont utiles pour de nombreux services d'une organisation, y compris l'audit interne. Une cartographie des prestations d'assurance complète et mise à jour permet :

- une compréhension partagée des risques auxquels une organisation doit faire face selon des catégories de risques ;
- l'identification des rôles et des fonctions de management des risques et de fourniture d'assurance dans l'organisation ;
- l'élaboration d'un cadre de référence exhaustif et holistique des activités d'assurance, qui peut être utile lors de périodes de transition, comme lors de fusions-acquisitions, d'une restructuration ou de l'évaluation et du changement de la stratégie de l'organisation ;
- la collaboration entre les prestataires d'assurance pour faciliter une utilisation des ressources efficiente et efficace.

Au sein de sa fonction, le responsable de l'audit interne peut utiliser la cartographie des prestations d'assurance comme outil de communication des hypothèses sous-jacentes au plan d'audit auprès de la direction générale et du Conseil.

En conformité avec la Norme 2050 – Coordination et utilisation d'autres travaux, le responsable de l'audit interne peut aussi définir un processus et des critères pour déterminer si la fonction d'audit interne peut utiliser les travaux d'un autre prestataire d'assurance, au lieu de dupliquer cette activité. Le responsable de l'audit interne peut décider d'utiliser les travaux d'autres prestataires d'assurance, internes ou externes, pour diverses raisons, notamment pour :

- prendre en compte les domaines pour lesquels la fonction d'audit interne ne détient pas collectivement les compétences nécessaires ;

- approfondir les connaissances auprès d'autres prestataires d'assurance ;
- améliorer effectivement la couverture des risques au-delà du plan d'audit interne.

Cependant, comme mentionné dans la Norme 2050 – Coordination et utilisation d'autres travaux, le responsable de l'audit interne devrait soigneusement prendre en considération les compétences, l'objectivité et la conscience professionnelle des autres prestataires et avoir une compréhension précise de leur périmètre d'intervention, objectifs et résultats. En effet, le responsable de l'audit interne a toujours le devoir d'étayer de manière adéquate les conclusions et opinions de fonction d'audit interne. Une cartographie des prestations d'assurance peut être la première étape dans l'élaboration d'un plan d'utilisation d'autres travaux.

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.

Normes
Norme 1000 – Mission, pouvoirs et responsabilités
Norme 2050 – Coordination et utilisation d'autres travaux
Norme 2100 – Nature du travail
Lignes directrices
Guide pratique, « Reliance by Internal Audit on Other Assurance Providers », décembre 2011.
Guide pratique, « L'audit interne et les activités de la 2ème ligne de maîtrise », janvier 2016.
Autres ressources IIA
Prise de position de l'IIA, « Les trois lignes de maîtrise pour une gestion des risques et un contrôle efficaces », janvier 2013.

Annexe B. Glossaire

Les termes sont issus du glossaire du *Cadre de référence internationale des pratiques professionnelles de l'IIA*, édition 2017.

Activités d'assurance – Il s'agit d'un examen objectif d'éléments probants, effectué en vue de fournir à l'organisation une évaluation indépendante des processus de gouvernance, de management des risques et de contrôle. Par exemple, des travaux concernant la finance, la performance, la conformité, la sécurité des systèmes ou les *due diligence*.

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

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).

Indépendance – L'indépendance c'est la capacité de l'audit interne à exercer, sans biais, ses responsabilités.

Objectivité – L'objectivité est un état d'esprit non biaisé qui permet aux auditeurs internes d'accomplir leurs missions de telle sorte qu'ils soient confiants en la qualité de leurs travaux menés sans compromis. L'objectivité nécessite que les auditeurs internes ne subordonnent pas leur jugement professionnel à celui d'autres personnes.

Risque – Possibilité que se produise un événement qui aura un impact sur la réalisation des objectifs. Le risque se mesure en termes de conséquences et de probabilité.

Annexe C. Cadres de référence concernant les risques

Lors de l'élaboration d'une cartographie des prestations d'assurance, les auditeurs internes peuvent avoir besoin de se référer à un cadre de référence concernant les risques afin de les aider à identifier et classer les informations en la matière. Parmi les organisations qui produisent des cadres de référence notons :

- le COSO *(Committee of Sponsoring Organizations of the Treadway Commission)*, Management des risques de l'entreprise – cadre de référence intégré ;
- le NIST *(National Institute of Standards and Technology)* ;
- l'ISO (Organisation internationale de normalisation) / l'IEC (Commission électrotechnique internationale) ;
- l'ISACA *(Information Systems Audit and Control Association)*.

Remerciements

Équipe de projet

Glenn Ho, CIA, CRMA, Afrique du Sud (Chairman)
Alp Buluc, CIA, CCSA, CRMA, Turquie (Project Lead)

Contributeurs

Rune Johannessen, CIA, CCSA, CRMA, Norvège
Hans Lofgren, Suède
Sally Anne Pitt, CIA, CGAP, Australie
Bruce Turner, CGAP, CRMA, Australie
Benito Ybarra, CIA, Etats-Unis

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

Anne Mercer, CIA, CFSA, Director (Project Lead)
Lisa Hirtzinger, CIA, QIAL, CCSA, CRMA, Vice President
Eva Sweet, CISA, CISM, IT and PS Director
Jeanette York, CCSA, FS Director
Debi Roth, CIA, Managing Director
Shelli Browning, Technical Editor
Lauressa Nelson, Technical Editor

Réviseurs de la traduction française

Béatrice Ki-Zerbo, CIA
Sébastien Lepers, CIA, CFE, CGAP, CRMA
Béatrice Vedrenne Robson

L'IIA aimerait remercier les organes de surveillance suivants pour leur soutien : Guidance Development Committee, Professional Guidance Advisory Council, International Internal Audit Standards Board, Professional Responsibility and Ethics Committee, and 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© 2018 *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 ou l'IFACI à l'adresse recherche@ifaci.com

Janvier 2018 – ISBN: 978-2-915042-89-4

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