Audit des risques stratégiques

Points de vue concrets de responsables de l'audit interne

Etude du CBOK sur les parties prenantes

J. Michael Joyce, Jr.
CIA, CPA, CRMA

protiviti®
Face the Future with Confidence

The IIA Research Foundation

CBOK
The Global Internal Audit Common Body of Knowledge

DONNÉES – ÉTUDE SUR LES PARTIES PRENANTES

Participants à l'enquête	1 124
Participants aux entretiens	112
Pays	23
Langues	13

PARTIES PRENANTES REPRÉSENTÉES

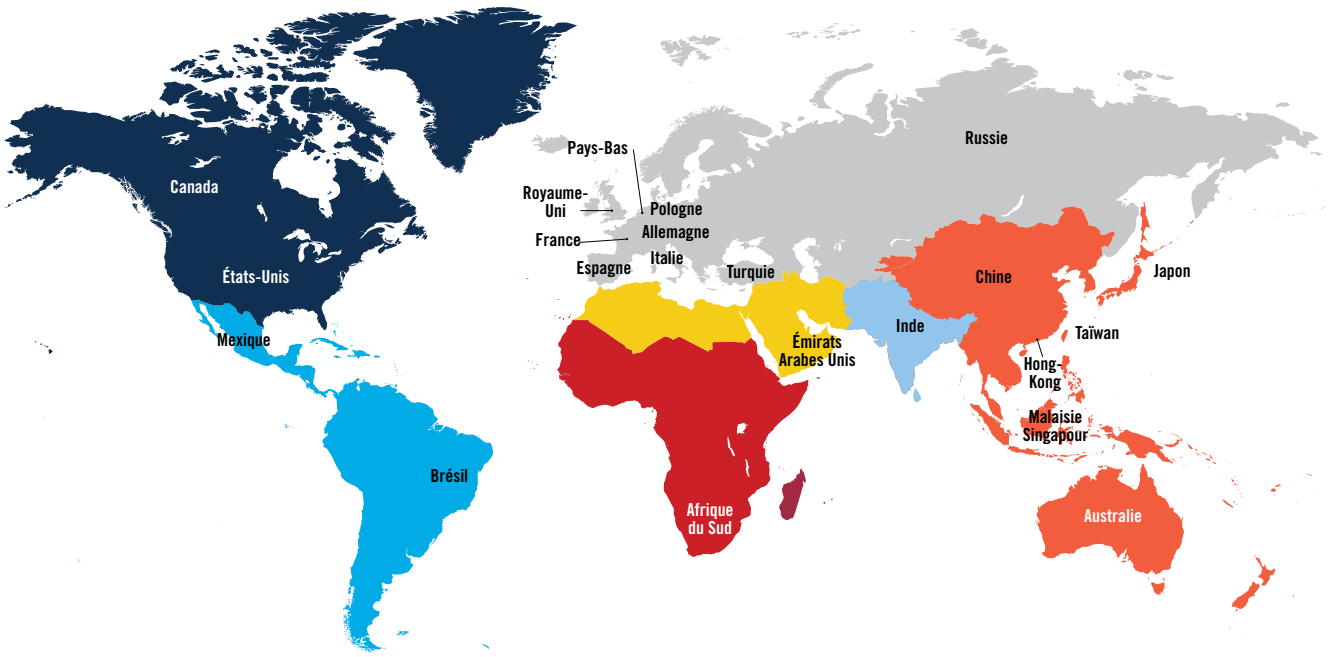
Administrateurs	34%
Directeur généraux	15%
Directeurs financiers	18%
Autres dirigeants	33%

À propos de CBOK

Le CBOK (*Common Body of Knowledge*) est la plus grande étude actuellement menée sur l'audit interne à l'échelle mondiale. Elle comprend notamment des enquêtes auprès des professionnels et de leurs parties prenantes. L'enquête mondiale sur la pratique de l'audit interne examine les activités de la profession. L'étude auprès des parties prenantes analyse leurs points de vue sur les performances de l'audit interne. Les enquêtes, les entretiens et l'analyse des données ont été effectués par Protiviti en collaboration avec les instituts de l'IIA à travers le monde. Les rapports des parties prenantes sont axés sur l'identification des meilleures pratiques qui peuvent permettre d'améliorer l'efficacité de l'audit interne.

Les rapports du CBOK sont gratuits grâce à la généreuse contribution d'individus, d'organisations, de chapitres et d'instituts de l'IIA dans le monde. Tous les rapports sont téléchargeables sur le site du CBOK Resource Exchange (www.theiia.org/goto/CBOK). Les rapports sur les parties prenantes sont également téléchargeables sur le site de Protiviti (www.protiviti.com).

Etude du CBOK 2015 sur les parties prenantes : 23 pays d'origine



Note : Les enquêtes et les questionnaires de la Fondation de l'audit interne, anciennement appelée la Fondation de la recherche de l'IIA, et de Protiviti ont été distribués aux parties prenantes dans 23 pays entre juillet 2015 et février 2016. Les questionnaires partiellement remplis ont été inclus dans l'analyse dès lors que les informations sur la population interrogée étaient complètes. Les questions sont intitulées Q1, Q2, etc. La carte met en évidence la répartition des pays ciblés par les enquêtes du CBOK en sept grandes régions (selon le modèle de la Banque mondiale).

L'étude internationale du CBOK 2015 sur les parties prenantes

Ce rapport fait partie de l'étude internationale menée auprès des parties prenantes dans le cadre du CBOK *(Common Body of Knowledge)* 2015 de la Fondation de l'audit interne (*Internal Audit Foundation*) de l'IIA. Un des principaux constats est que près de deux tiers (soit 64 %) des parties prenantes (les administrateurs, les directeurs généraux, les directeurs financiers, des systèmes d'information, de la gestion des risques et autres dirigeants) souhaitent que l'audit interne soit plus actif en matière de risques stratégiques. A travers ce rapport, des directeurs de l'audit interne de différents secteurs ont été interrogés afin d'en savoir plus sur la façon dont ils s'impliquaient dans trois principaux risques stratégiques : la cybersécurité, les projets relatifs aux systèmes d'information (SI) et les projets d'investissement. Leurs points de vue recueillis de manière anonyme ont permis d'illustrer notre propos en nous fondant sur leurs réactions et avis sincères.

Table des matières

Introduction : Des points de vue à la fois ordinaires et captivants sur l'audit des risques stratégiques

> *« Nous gardons un œil sur les hypothèses, celles qui sont à l'origine de l'initiative stratégique et celles qui continuent de soutenir l'initiative dans sa progression. Ces hypothèses sont-elles toujours pertinentes ? »*

Les pratiques exemplaires partagées par les directeurs de l'audit interne sont tour à tour ordinaires et captivantes lorsque ces responsables confient la façon dont leur fonction d'audit interne interagit avec la direction générale et le Conseil pour aborder trois types de risques stratégiques pour leur organisation : la cybersécurité, les projets liés aux systèmes d'information et les projets d'investissement.

Ces pratiques nous semblent ordinaires à cause de l'approche fondée sur les risques et des leviers que les responsables de l'audit interne indiquent pour l'efficacité d'une mission d'«audit stratégique». Notons que de plus en plus d'administrateurs, de directeurs généraux, de directeurs financiers et autres dirigeants incitent l'audit interne à se lancer dans ce type de missions. Les directeurs de l'audit interne soulignent la valeur d'une implication précoce de leur service dans les initiatives stratégiques, l'approche d'audit fondée sur les risques, la crédibilité de l'audit interne aux yeux des métiers et la capacité de la fonction à prospérer selon une méthode consultative. Ces blocs de construction cruciaux existent au sein des fonctions d'audit les plus performantes depuis un certain temps.

Deux autres constats, plus inattendus, ont également émergé de ce dialogue. Tout d'abord, les fonctions d'audit interne progressent de façon significative dans la façon dont elles vérifient et abordent les risques stratégiques à travers un large éventail de démarches (comme nous l'observons dans les paragraphes concernant la cybersécurité, les projets liés aux SI et les projets d'investissement). Ensuite, les fonctions d'audit interne à la pointe travaillent consciencieusement et avec créativité afin de conforter leur contribution dans les cercles de décision, la crédibilité de leur fonction et leur rôle de conseiller par le biais de certains effets de leviers (résumés dans la dernière partie de ce rapport).

Les entretiens avaient un double objectif : en décrivant la façon dont ils abordent les risques stratégiques, ces responsables de l'audit, qui sont à l'avant-garde, ont mis en lumière les moyens qu'ils utilisent pour promouvoir et maintenir leur rôle de partenaire stratégique des métiers sans pour autant remettre en cause la priorité qu'ils accordent à leurs responsabilités en matière de conformité et d'assurance.

La cybersécurité n'existe pas hors de tout cadre

> *« La cybersécurité doit fonctionner comme l'ensemble des systèmes et des organes d'un corps humain qui interagissent pour le défendre face aux menaces et le rendre plus efficace. Ce n'est pas une procédure isolée. Il n' y a pas un aspect de notre entreprise qui n'impacte pas la cybersécurité ».*

A la comparaison entre un projet d'investissement majeur en cours dans une région en guerre et une mission d'audit de la cybersécurité, un directeur de l'audit interne a immédiatement répondu : « Ce projet d'investissement n'est ni aussi complexe ni aussi impressionnant ».

Les comités d'audit réclament des informations actualisées sur la capacité de l'entreprise à aborder le risque stratégique colossal que constitue la cybersécurité. Les directeurs de l'audit interne y répondent de différentes façons. Par exemple, en aiguisant leur vision de la cybersécurité au sein de l'organisation grâce à des évaluations formelles des risques et une implication directe dans les comités et exercices de pilotage de la cybersécurité, en augmentant et en étendant les points liés à la cybersécurité dans les programmes d'audit et en ajustant leurs activités de gestion du risque avec les DSI, les fonctions sécurité de l'information et management des risques à l'échelle de l'entreprise (ERM - *Entreprise risk management).*

Les directeurs de l'audit interne interrogés ont surtout cité les activités et les bonnes pratiques suivantes pour décrire leurs facteurs d'efficacité en matière d'audit de cybersécurité :

- **Collaborer avec ceux qui définissent et façonnent la stratégie de cybersécurité :** Tout en soulignant que leurs fonctions ont toujours mené de nombreuses missions sur la gestion des identités, la gestion des *patchs* et d'autres formes d'audit de la cybersécurité bien avant que le terme de « cybersécurité » n'acquière sa signification actuelle, les responsables de l'audit interne indiquent qu'ils cherchent désormais à jouer le rôle de conseillers au sein de comités chargés de définir et de renforcer les stratégies et les compétences de cybersécurité de l'organisation. Par ailleurs, comme le souligne l'un des directeurs de l'audit interne, une autre option est de : « travailler avec le comité d'audit pour créer un sous-comité dédié à la cybersécurité qui lui soit rattaché et soit composé d'experts externes qui peuvent apporter des avis pertinents sur les questions de cybersécurité cruciales et d'actualité ».
- **Clarifier les responsabilités de maîtrise des risques de cybersécurité et être coordonné avec les autres acteurs :** Les directeurs de l'audit interne travaillent étroitement avec leurs partenaires de la DSI, des équipes de sécurité de l'information et de gestion des risques (ERM) pour identifier leurs activités en matière de cybersécurité. Cette coordination aide à synchroniser l'ensemble des efforts au sein d'une entreprise tout en renforçant le rôle de l'audit interne dans la fourniture d'une assurance objective et indépendante en ce qui concerne le risque de cybersécurité. Par exemple, un directeur de l'audit interne et son responsable de l'information, effectuent des présentations conjointes sur les risques de cybersécurité au comité d'audit afin de montrer que « nous travaillons de façon coordonnée sur la base d'une approche commune d'évaluation des risques ».
- **Effectuer une évaluation formelle des risques :** Les évaluations formelles des risques, qu'elles soient réalisées par l'audit interne ou un expert tiers, constituent une partie essentielle de la démarche de cybersécurité. Ces analyses permettent d'identifier les lacunes, clarifient les progrès et les priorités

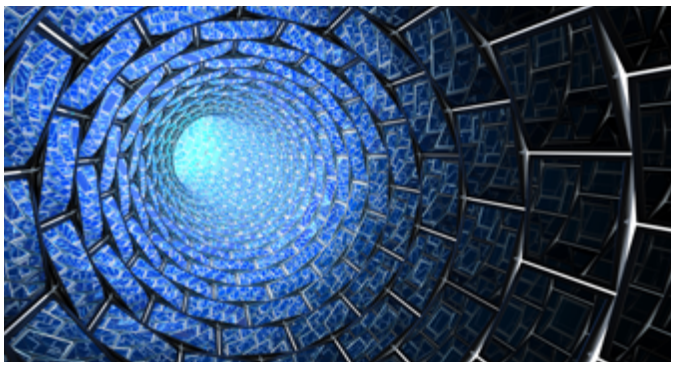
Bonnes pratiques d'audit du risque stratégique :

CYBERSECURITE

- *Collaborer avec ceux qui définissent et façonnent la stratégie de cybersécurité.*
- *Clarifier les responsabilités de maîtrise des risques de cybersécurité et être coordonné avec les autres acteurs.*
- *Effectuer une évaluation formelle des risques.*
- *Donner des conseils sur les cadres de référence, normes et guides de cybersécurité.*
- *Evaluer la cyber résilience.*
- *Apprendre sans discontinuer.*
- *Surmonter le défi des compétences et des connaissances en matière de cybersécurité.*

de remédiation (par exemple faire face à une forte augmentation des mèls de *phishing*), aident à déterminer les différentes facettes de la cybersécurité dans le plan d'audit, influencent les conseils en matière de cybersécurité et aident l'entreprise à ajuster ses risques de cybersécurité et ses objectifs d'amélioration.

- **Donner des conseils sur les cadres de référence, normes et guides de cybersécurité :** Chaque directeur de l'audit interne a cité une ou plusieurs normes que leur entreprise utilise et adapte, pour aider à structurer l'ensemble du programme de cybersécurité et les activités d'assurance afférentes. Ces normes comprennent entre autres le cadre de référence de cybersécurité NIST, COSO ERM, HITRUST, COBIT, ISO, le guide d'audit (GTAG - *Global Technologies Audit Guide)* de l'IIA : « Évaluer le risque de cybersécurité : Les rôles des trois lignes de maîtrise », CSC20, FFIEC. Un directeur de l'audit interne qui apprécie le cadre de référence COSO ERM parce qu'il permet notamment une cohérence, une transparence et une sensibilisation du conseil d'administration vis-à-vis du risque de cybersécurité, souligne également que ce cadre de référence « peut, par exemple, ne pas suffire en Inde, en Australie ou dans d'autres pays où d'autres modèles de gestion des risques de cybersécurité sont utilisés. Nous avons pris ce que nous estimons être le meilleur dans chaque modèle et l'avons appliqué pour répondre à nos besoins au niveau mondial ». L'implication directe des directeurs de l'audit interne dans la discussion et l'évaluation de chacun des cadres de référence potentiels, de leurs avantages et inconvénients, place l'audit interne en position d'aider leurs organisations à tirer le meilleur bénéfice des cadres de référence.
- **Evaluer la cyber résilience :** En partant du constat que, dans le contexte actuel, une intrusion est inévitable, les directeurs de l'audit interne devront évaluer la capacité de l'organisation à réagir, communiquer et se restaurer lorsqu'une intrusion se produit. Les domaines à prendre en compte incluent non seulement les procédures de continuité mais également les plans de gestion de crise.
- **Apprendre sans discontinuer :** La connaissance des menaces extérieures, des nouvelles normes, des nouvelles obligations de conformité et même le profilage psychologique, sont des facteurs essentiels du succès d'une mission d'audit de cybersécurité. « Je suis un *Certified Information Systems Security Professional* (CISSP) », a fait remarquer un directeur de l'audit interne « et j'ai passé beaucoup de temps à étudier et à faire des recherches sur la cybersécurité ... [par exemple], je veux savoir exactement comment Equifax a été attaqué ». Ce même responsable exhorte aussi son équipe à comprendre l'état d'esprit de nombreuses parties prenantes qui pourraient exposer, en connaissance de cause ou à leur insu, l'entreprise à une menace de cybersécurité. « L'audit interne nécessite de comprendre le raisonnement et la méthodologie d'un hacker », a-t-il déclaré. « Un responsable d'audit interne doit être capable de penser comme un comptable, un investisseur, un avocat, un expert de la conformité, un commercial, un directeur des ressources humaines, quiconque qui pourrait être à l'origine d'un risque qui exposerait l'entreprise à une défaillance de cybersécurité ». Par ailleurs, l'examen de l'efficacité de la formation et de la sensibilisation à la cybersécurité réalisée dans l'ensemble de l'organisation constitue un des volets des missions d'assurance menées par l'audit interne.
- **Surmonter le défi des compétences et des connaissances en matière de cybersécurité :** La plupart des directeurs de l'audit interne confirment que le recrutement et la fidélisation d'auditeurs internes possédant des connaissances en informatique et cybersécurité est un défi. Ils gèrent cet obstacle par des stratégies et des tactiques de gestion des talents, tels que des programmes de formation et de développement professionnel, le recours à des experts externes et une étroite collaboration avec les collègues des ressources humaines afin de concevoir des mesures d'incitation pour le recrutement, la performance et la fidélisation.



Projets relatifs aux systèmes d'information : Examiner rigoureusement les données, le développement et les comportements

« Si les gens pensent que la cybersécurité et les projets SI sont séparés, ils se trompent ».

Alors que de plus en plus d'entreprises misent tout sur la transformation numérique et que de plus en plus de systèmes d'information et d'applications migrent vers le cloud, de plus en plus de projets relatifs aux systèmes d'information de toutes tailles et de différents champs d'application présentent des risques stratégiques. Par conséquent, une plus grande variété de projets SI et d'activités de développement d'applications nécessitent un examen rigoureux de la part de l'audit interne.

Cette rigueur peut également être profitable à l'audit interne. Un directeur de l'audit interne se souvient de la mise en place d'un logiciel majeur qui a mobilisé ses auditeurs SI car le prestataire externe chargé de tester le système n'a pas fourni des résultats assez précis. « Nous avons pris les devants pour indiquer que nous n'étions pas prêts à approuver les travaux menés, d'autant plus que nous pouvions étayer de manière factuelle notre position par le fait que les résultats des tests n'étaient pas satisfaisants », explique-t-il. La documentation complète de son équipe a convaincu que d'autres tests étaient nécessaires avant de lancer le système. « Cela nous a conforté dans le positionnement de la fonction », poursuit-il. « Depuis, le cycle de test du logiciel a continué à s'améliorer ».

Une rigueur minutieuse et une audace factuelle similaires sont mises en avant par les responsables d'audit parmi les facteurs d'efficacité des missions d'audit des projets SI :

- **Développer une procédure structurée d'évaluation à plusieurs phases :** Les directeurs de l'audit interne insistent sur la valeur du développement et de l'amélioration des évaluations structurées pour chaque phase d'un projet SI. Etant donné que le volume, la valeur et l'importance des données concernant les nouvelles implémentations et les conversions de systèmes augmentent, la sécurité apparaît souvent comme le point de départ de l'évaluation d'un projet SI. Un directeur de l'audit interne a expliqué comment son équipe d'audit SI s'était organisée en deux pôles pour les missions concernant les projets SI : l'un se focalise sur l'évolution des systèmes liés aux contrôles financiers qui nécessitent la contribution d'auditeurs SI et d'auditeurs au profil financier ; l'autre se focalise sur des thèmes plus classiques de gestion des projets SI, de gouvernance et d'efficience.
- **Dépasser les barrières psychologiques :** Un directeur de l'audit interne a précisé comment les auditeurs SI ont constaté à plusieurs reprises que des équipes en charge de projets SI ont ignoré ou manifestement caché des problèmes. L'audit interne a par conséquent revu sa communication avec ces équipes de projet. « Une fois que nous avons constaté qu'elles ne voulaient pas parler des problèmes importants, nous avons fait en sorte qu'elles se sentent plus à l'aise de le faire », a expliqué le responsable de l'audit. « A propos du système d'évaluation par les couleurs rouge, jaune et vert, nous avons lancé un nouveau slogan *« red is not dead »,* autrement dit : « rouge ne veut pas dire mort ». L'équipe d'audit SI a également formulé un *business case* explicitant les bénéfices de la remontée et de la résolution des problèmes le plus en amont possible du cycle de vie du projet plutôt que lorsque les conséquences et les coûts de problèmes mineurs auront pris de l'ampleur.

Bonnes pratiques d'audit du risque stratégique :

PROJETS SI

- *Développer une procédure structurée d'évaluation à plusieurs phases.*
- *Dépasser les barrières psychologiques.*
- *Proposer des prestations de conseil en complément des missions d'assurance.*
- *Admettre la nécessité de traiter les développements en mode agile.*

- **Proposer des prestations de conseil en complément des missions d'assurance :** Une équipe d'audit SI a développé une offre de conseils à partir de critères d'évaluation que les auditeurs SI utilisent lors d'une mission d'audit d'un projet SI (par exemple : Avons-nous une stratégie d'implémentation ? Qui est le sponsor ? Le financement est-il approuvé ? Quels sont les risques connus du projet ? Quel est le plan d'urgence requis ?) Au fil de la revue de ces questions avec les équipes en charge des projets SI, les auditeurs SI donnent des conseils sous forme de recommandations qui ne donnent pas lieu à un plan d'action formel. Selon le directeur de l'audit interne, « les équipes de projet ont tellement bien intégré cette prestation qu'elles n'ont plus besoin de la demander. Elles le font d'elles-mêmes en suivant les éléments que nous avons formalisés et partagés ».

- **Admettre la nécessité de traiter les développements en mode agile :** De nombreux directeurs de l'audit interne avec lesquels nous avons discuté cherchent à aborder les risques associés aux développements en mode agile qui sont de plus en plus adoptés par les DSI. Bien que cette approche très collaborative, itérative et allégée des développements logiciels réduise énormément la durée nécessaire pour créer de nouvelles applications et améliore indirectement l'agilité de l'organisation et sa vitesse d'accès au marché, elle n'est pas sans risque. « Du point de vue de l'audit, nous devons résoudre des questions comme les exigences de traçabilité, l'obtention des approbations appropriées de la conception par les équipes de développement, etc. », explique un responsable de l'audit interne. « Cela peut être un avantage pour les organisations mais présente également de nouveaux risques ».

Projets d'investissement : Le processus avant tout

« Nous évaluons le processus et non la personne ».

Les directeurs de l'audit interne dont les fonctions réalisent des missions d'audit et des évaluations de gros projets d'investissement ont tendance à mettre l'accent sur l'importance de deux sujets. Tout d'abord, il est fondamental de distinguer le suivi de l'équilibre et de l'évolution de chaque projet d'investissement qui relève de la direction générale, et l'assurance qu'apporte l'audit interne. Deuxièmement, les responsables de l'audit interne font la distinction entre leur travaux relatifs à des projets d'investissement donnés et la nécessité d'évaluer la capacité générale de l'organisation à gérer des projets d'investissement. Ce dernier point peut être très utile dans le premier cas.

Les directeurs de l'audit interne ont cité les activités et les bonnes pratiques suivantes pour augmenter l'efficacité de leurs missions d'assurance et de conseil relatives aux projets d'investissement :

- **Etre impliqué en amont et dès la planification :** L'implication de l'audit interne au premier stade de toute initiative stratégique est un atout pour l'organisation. C'est particulièrement vrai dans le cas, par exemple, d'un projet de construction de 500 millions de dollars sur plusieurs années à l'autre bout du monde. Cette implication se manifeste souvent par des évaluations des risques en phase préliminaire fortement axées sur la structure de gouvernance des projets. Un directeur de l'audit interne explique qu'une de ces évaluations des risques a eu pour conséquences des modifications fondamentales, y compris au niveau de l'équipe d'ingénierie, au niveau des achats et de l'entreprise de construction prestataire, qui ont influencé l'évolution des travaux.
- **Etre attentif à la logique sous-jacente à l'investissement :** De nombreux projets d'investissement s'étalent sur plusieurs années et les hypothèses sous-jacentes à la décision d'investissement peuvent changer dans le temps. Dans le cadre des audits de projets d'investissement, un directeur de l'audit interne et son équipe identifient quelles sont les sources de données qu'il faut utiliser pour valider les hypothèses de la prise de décision. « Nous testons ces hypothèses de façon sélective lorsque cela a du sens et est pratique », poursuit-il. « Sur quels faits pouvons-nous nous baser ? Si vous avez effectué une modélisation, comment savez-vous que les modèles sont exacts ? Comment savez-vous que les formules sont intègres ? Le retour sur investissement prévu est-il confirmé/validé ? »
- **Déployer l'expertise nécessaire :** Un directeur de l'audit interne a récemment engagé en externe un auditeur spécialiste de la construction afin de réaliser une étude détaillée des factures du principal prestataire d'un type de chantier que nous n'avions jamais réalisé. Ainsi, « nous avons pu poser des questions techniques auxquelles seule une personne expérimentée dans ce type de projet de construction pouvait penser. » D'autres directeurs d'audit recrutent et fidélisent des auditeurs internes ayant une expérience approfondie des projets d'investissement et de construction, qui savent quels problèmes rechercher et auxquels ils devront éventuellement s'attaquer au fur et à mesure des visites sur site, des réunions de suivi et des états d'avancement du projet.
- **Effectuer des évaluations de projets rigoureuses et centrées sur les processus :** Dans la plupart des cas, les missions d'audit de projets d'investissement concernent l'ensemble du projet et sont peu automatisées. L'évaluation de la gouvernance

Bonnes pratiques d'audit du risque stratégique :

PROJETS D'INVESTISSEMENT

- *Etre impliqué en amont et dès la planification.*
- *Etre attentif à la logique sous-jacente à l'investissement.*
- *Déployer l'expertise nécessaire.*
- *Effectuer des évaluations de projets rigoureuses et centrées sur les processus.*
- *Donner des conseils pour améliorer la gestion des projets d'investissement.*
- *Effectuer des missions d'audit et des évaluations a posteriori.*

détermine si l'équipe de pilotage du projet s'est focalisée sur les risques pertinents et si elle reçoit des informations correctes, complètes et en temps voulu. L'évaluation de l'état d'avancement et du budget nécessite l'analyse de gros volumes de données et les pièces justificatives accompagnant les factures du principal prestataire ont tendance à être particulièrement épaisses. Alors qu'une approche rigoureuse est absolument nécessaire, les directeurs de l'audit interne soulignent constamment le besoin de clarifier auprès des chefs de projet que l'audit interne s'intéresse aux processus et ne vise pas les personnes. Atteindre cet équilibre nécessite que les responsables d'audit traduisent les risques, les dispositifs de contrôle interne et les autres jargons et perspectives en des termes qui interpellent les chefs de projet pressés par le temps.

- **Donner des conseils pour améliorer la gestion des projets d'investissement :** Une fonction d'audit interne a développé une offre de conseils que les équipes en charge de projets d'investissement peuvent utiliser au début d'une nouvelle initiative. L'audit interne donne des lignes directrices sur les principaux contrôles opérationnels, financiers et risques liés aux projets dont l'équipe doit tenir compte ainsi qu'une formation de sensibilisation et de prévention des fraudes liées aux factures de prestataires. « Nous avons alors un rôle de conseiller en matière de risques et de partenaire stratégique sans pour autant perturber les premières échéances et une implémentation réussie », déclare le directeur de l'audit interne. Une autre équipe d'audit interne participe à une initiative stratégique centrée sur l'amélioration de la capacité de gestion de projets d'investissement de l'entreprise et, plus particulièrement, sur les modalités de mesure et de suivi des investissements. Dans cette organisation, le rôle de la fonction d'audit interne consiste à s'assurer que des contrôles appropriés sont intégrés dans les nouveaux processus que l'équipe développe.
- **Effectuer des missions d'audit et des évaluations a posteriori (post mortem) :** Les résultats de ces activités peuvent constituer un retour d'information utile sur la validité des hypothèses initiales utilisées pour justifier le projet d'investissement et améliorer les approches pour les projets futurs, y compris la possibilité d'une mission d'audit interne aux stades préliminaires du projet.

Les quatre leviers des fonctions d'audit interne à la pointe

En plus des éléments spécifiques identifiés ci-dessus, les commentaires et les points de vue des directeurs de l'audit interne révèlent plusieurs leviers essentiels dans le succès des missions d'audit stratégique. Les directeurs de l'audit interne interrogés indiquent que ces attributs existent dans chacune de leur fonction.

Quatre principaux leviers :

1. *Démonstration permanente de la valeur ajoutée*
2. *Accès*
3. *Langage commun*
4. *Participation*

1. **Démonstration permanente de la valeur ajoutée :** La plupart des directeurs de l'audit interne évoquent les moments à l'origine de l'acceptation de la fonction d'audit interne comme un partenaire stratégique donnant de l'assurance et des conseils. Comme des *flashbacks* dans un film qui nous permettent de découvrir comment les super-héros ont acquis leurs super pouvoirs, ces descriptions soulignent les circonstances dans lesquelles les actions de l'audit interne ont modifié la façon dont la direction générale, les membres du Conseil et les propriétaires de processus considèrent leur fonction d'audit interne. En particulier, les responsables de l'audit interne soulignent que la réputation bien méritée de leur fonction doit être entretenue et confortée par une démonstration permanente de sa valeur ajoutée. De nouveaux dirigeants et propriétaires de processus rejoignent en permanence l'organisation et, tôt ou tard, ils cherchent la preuve de la crédibilité de l'audit interne.
2. **Accès :** La démonstration de la valeur ajoutée de la fonction d'audit interne et l'engagement du directeur de l'audit interne à développer des relations durables lui offrent un important laissez-passer vers les membres du Conseil, la direction générale et les propriétaires de processus dans toute l'entreprise. Cet accès se traduit par une connaissance

appréciable de ce qui se passe dans toute l'organisation et des changements et initiatives stratégiques qui peuvent se présenter.

3. **Langage commun :** Il est surprenant de constater combien de directeurs de l'audit interne ont cité l'importance de traduire le terme « contrôle interne » de manière plus intelligible dans le contexte des fonctions SI, du *Chief Information Security Officer* (CISO), des gestionnaires de projets d'investissement et des autres propriétaires de processus. Un responsable de l'audit interne indique qu'au lieu de « contrôle interne », ils préfèrent parler, « des processus qui, où que vous soyez (usine, fonction, site), vous font avancer vers vos objectifs ». Les directeurs de l'audit interne insistent sur la nécessité de traduire l'ensemble des travaux de la fonction en des termes pratiques et compréhensibles qui ont une signification pour les parties prenantes dans leurs contextes.
4. **Participation :** Les fonctions d'audit à l'avant-garde ont tendance à être très actives et participatives. Elles participent à des exercices de simulation d'incidents conçus pour être confrontées à des défaillances de la cybersécurité. Elles passent un temps non négligeable dans les ateliers de fabrication et les chantiers. « Nous effectuons des tests d'intrusion sur le réseau dans le cadre de notre plan d'audit », a déclaré un directeur de l'audit interne. « Cela nous permet de mieux saisir les points faibles et la façon dont le management les aborde ». Les informations que le responsable de l'audit interne partage avec le Conseil lui permettent une communication actualisée et tangible sur la cybersécurité au comité d'audit.

En guise de conclusion : L'assurance vient avant le conseil

Bien que les directeurs de l'audit interne décrivent une intéressante série de prestations de conseil que leurs fonctions offrent afin d'aider l'organisation à aborder les risques stratégiques, ils insistent également, sans ambiguïté, sur le fait que les missions d'assurance sont toujours prioritaires.

L'anecdote suivante en est un bon exemple : Quelques semaines après son recrutement, un auditeur sénior a demandé à son directeur de l'audit interne pourquoi la fonction ne faisait pas plus la promotion de sa gamme de services de conseil qui ne cessait de s'étoffer. Sa réponse a clarifié les priorités de la fonction : « Plutôt que de foncer bille en tête avec les services de conseil, je préfère que les personnes avec lesquelles nous interagissons pour les missions d'assurance, qui comprennent notre valeur, nous demandent des conseils. Je pense que c'est de cette façon que l'on attire des clients ».

À propos des auteurs

J. Michael Joyce Jr., CIA, CPA, CRMA, FAHM, est Vice-président, Responsable de l'audit et de la conformité pour la Blue Cross Blue Shield Association (BCBSA), une fédération nationale rassemblant 36 entreprises Blue Cross et Blue Shield indépendantes et exerçant localement. Blue System est l'assureur le plus important du pays en matière de santé, couvrant plus de 107 millions d'adhérents, soit un américain sur trois. Joyce a la responsabilité de l'audit interne, de la lutte contre la fraude et de la conformité de cette association. Il possède une expérience professionnelle de 35 ans et travaille pour BCBSA depuis juin 1999. Il est un contributeur actif de l'IIA depuis 1989.

À propos de la Fondation de l'audit interne

Le CBOK est géré par la Fondation de l'audit interne, qui réalise depuis 40 ans des études novatrices sur la profession d'audit interne. À travers différents projets d'exploration des problématiques actuelles, des nouvelles tendances et des besoins futurs, la Fondation n'a cessé de jouer un rôle moteur pour l'évolution et le développement de la profession. La Fondation peut être contactée au : 1035 Greenwood Blvd., Suite 401, Lake Mary, Floride 32746, États-Unis.

À propos de Protiviti Inc.

Protiviti est un cabinet de conseil international qui offre une expertise approfondie, des idées objectives, une approche sur mesure et une collaboration inégalée en vue d'aider les leaders à affronter l'avenir avec confiance. Protiviti et nos entreprises membres indépendantes fournissent des solutions de conseil en finance, technologie, opérations, données, analyses, gouvernance, risques et audit interne à nos clients grâce à notre réseau de plus de 70 bureaux établis dans plus de 20 pays.

Plus de 60 % des entreprises du classement *Fortune* 1000® et 35 % de celles figurant au classement Fortune Global 500® ont fait appel à Protiviti. La société travaille également avec des entreprises de plus petite envergure, des entreprises en croissance, des entreprises souhaitant s'introduire en bourse, ainsi que des organismes publics. Protiviti est une filiale détenue à 100 % par Robert Half (coté au NYSE : RHI). Fondée en 1948, la société Robert Half est membre de l'indice S&P 500.

Protiviti n'est ni agréé ni enregistré comme cabinet d'experts comptables, et ne délivre pas d'opinions sur les états financiers ni ne propose de service de certification.

Limite de responsabilité

La Fondation de l'audit interne publie ce document à titre informatif et pédagogique uniquement. Elle ne fournit aucun service juridique ou de conseil, et ne garantit, par la publication de ce document, aucun résultat juridique ou comptable. En cas de problèmes juridiques ou comptables, il convient de recourir à l'assistance de professionnels.

ID #2018-0722

Vos dons ont un impact

Les rapports du CBOK sont disponibles gratuitement en libre accès grâce à la généreuse contribution d'individus et d'organisations, mais également de branches et d'instituts de l'IIA du monde entier.

Faire un don

www.theiia.org/goto/CBOK