TONE at the TOP®

Fournir aux cadres supérieurs, aux conseils d'administration et aux comités d'audit des informations concises sur des sujets liés à la gouvernance.

Numéro 93 | Juin 2019

L'audit flirte avec le management des risques

Les responsables d'audit interne émettent des rapports sur toute sorte de sujets, et ce n'est pas près de changer. En revanche, le choix des destinataires de ces rapports reste une question ouverte.

D'une part, on demande aux responsables d'audit d'en faire plus. On attend d'eux qu'ils jouent le rôle de conseillers de confiance capables d'éclairer les administrateurs sur les risques. Ils doivent également adopter les nouvelles technologies qui permettent une meilleure analyse et une surveillance plus juste des risques dans toute l'entreprise.

D'autre part, les conseils d'administration sont eux aussi sous pression. Régulateurs, actionnaires, clients, partenaires et autres acteurs veulent tous qu'ils exercent une gouvernance efficace des risques et ne se contentent pas d'examiner ces derniers ou d'établir des niveaux de tolérance. Les parties prenantes veulent que les administrateurs soient plus transparents, à tout moment.

Pensez à ce que cela signifie. Si l'on demande au responsable d'audit et au conseil d'administration de s'améliorer sur les mêmes tâches (à savoir évaluer les risques et être capables d'intervenir lorsqu'un risque dépasse le niveau acceptable), cela soulève une multitude de questions concernant la gouvernance, l'assurance des risques et le rôle du responsable d'audit.

Par exemple, les conseils d'administration devraient-ils créer des comités des risques ? Si oui, quels sujets le responsable d'audit interne présenterait-il à ce comité ? Est-il judicieux qu'il aborde certaines problématiques avec le comité des risques et d'autres avec le comité d'audit ? Le rôle du responsable d'audit devrait-il être fractionné ? Ou, au contraire, les technologies modernes entraînent-elles une fusion de l'audit interne et du management des risques au sein d'une fonction plus vaste d'assurance des risques ?

« Je ne suis pas sûr que, nous, en tant que profession, ayons suffisamment fait valoir auprès de ceux qui sont moins passionnés par le sujet, qu'il existe des avantages associés à la notion de priorité du risque », déclare Tom McLeod, responsable du management des risques pour l'Australian Broadcasting Corp. et ancien membre du conseil d'administration de l'Institut d'Audit Interne australien (IIA Australia).

Par conséquent, il se peut que les responsables d'audit glissent progressivement vers un rôle que personne n'avait prévu, où fonctions d'audit et de management des risques s'entremêlent. S'ils ont toujours exercé la première responsabilité avec efficacité, les technologies modernes leur permettent de s'améliorer dans la seconde… et il faut bien que quelqu'un s'en charge.

« C'est un processus long », déclare Tom McLeod, « dans lequel vous avancez sans réaliser que vous êtes de plus en plus impliqué dans le suivi des risques avant de l'être profondément ».

Cela vaut aussi bien pour les responsables de l'audit interne que pour les conseils d'administration. Mais alors, comment ces derniers peuvent-ils utiliser cette évolution de manière productive ?

À propos de l'IIA

The Institute of Internal Audtors Inc. (IIA) est une association professionnelle qui compte plus de 190 000 membres répartis dans plus de 170 pays et territoires à travers le monde.
Porte-parole mondial de la profession d'audit interne, l'IIA intervient en tant que leader incontesté dans les domaines de la formation, de la recherche et de la formulation de normes.

The IIA

1035 Greenwood Blvd.
Suite 401
Lake Mary, FL 32746 USA

Abonnements gratuits

Consultez le site **www.theiia.org/tone** pour vous abonner gratuitement.

Avis des lecteurs

Envoyez toutes vos questions et observations à l'adresse : **tone@theiia.org**.

Conseil consultatif en matière de contenu

Riches de plusieurs décennies d'expérience comme membres de la direction ou du conseil d'administration, les professionnels énumérés ci-après ont revu le contenu de la présente publication :

Martin M. Coyne II
Michele J. Hooper
Kenton J. Sicchitano

Commencer par soulager le conseil d'administration

Selon une étude réalisée en 2018 par le EY Center for Board Matters et publiée dans le Harvard Law School Forum on Corporate Governance and Financial Regulation, seulement 11 % environ des conseils d'administration du S&P 500 disposent d'un comité des risques. De surcroit, on constate une concentration au niveau des institutions financières, dont 74 % en sont dotées. En dehors de ce secteur, le pourcentage chute : seulement 4 % des entreprises dans les domaines de la consommation, de l'industrie, de la technologie et des services d'utilité publique en ont un.

Mais ces chiffres n'expliquent pas tout. Par exemple, la Réserve fédérale exige que les banques cotées en bourse ayant un actif de 10 milliards de dollars ou plus soient dotées d'un comité des risques. Il n'est donc pas surprenant qu'autant de banques en soient pourvues.

Par ailleurs, selon cette même étude, 14 % des organisations disposent d'un comité des politiques publiques et 38 % ont un comité de Responsabilité des Entreprises. Dans le secteur de la santé, 21 % possèdent un comité des affaires réglementaires et 18 % ont un comité technologique.

C'est logique. Les entreprises qui s'adressent au grand public ont à cœur d'être perçues comme des organisations citoyennes, ce qui explique qu'elles soient si nombreuses à posséder un comité de Responsabilité des Entreprises. Les acteurs de la santé sont très réglementés, surtout en ce qui concerne les informations médicales personnelles. Ils sont donc plus susceptibles d'avoir un comité de conformité et un comité technologique. Tant que l'organisation dispose, au niveau de ses administrateurs, d'un comité qui surveille les risques importants pour son activité, qui se soucie de son nom ?

James Lam, président du comité des risques d'E*TRADE et consultant expérimenté spécialisé en management des risques, affirme que toute entreprise dont le chiffre d'affaires annuel dépasse le milliard de dollars devrait envisager de créer son propre comité des risques.

Selon lui, ce comité devrait se pencher sur les « risques techniques et granulaires », qui peuvent autant relever de la conformité et du développement durable, que de la cybersécurité et de la lutte contre le blanchiment d'argent, ou de tout autre sujet nécessitant une attention particulière. L'objectif est de faire en sorte que le conseil d'administration, déjà débordé, soit déchargé de ces enjeux pour pouvoir se concentrer sur les risques stratégiques.

« Si le conseil d'administration au complet peut s'en charger, tant mieux, déclare James Lam, mais cela constitue un programme très chargé ».

Tom McLeod cite l'exemple de Rio Tinto, où il a exercé en tant que responsable de l'audit interne au début des années 2010. Le conseil disposait d'un comité du développement durable qui s'intéressait aux droits fonciers, à la gestion des ressources hydriques ainsi qu'à d'autres problématiques environnementales, « des enjeux fondamentaux rarement abordés ou pris en compte », selon lui.

Tom McLeod rendait compte au comité d'audit ainsi qu'au comité des risques de Rio Tinto, mais il savait quels points aborder avec chacun d'eux. Lorsque les deux entités sont regroupées, « la délimitation n'est pas claire », explique-t-il.

Tout cela pourrait être le signe d'une mauvaise compréhension de la gouvernance des risques plus qu'autre chose. Les comités d'audit existent depuis des décennies et leurs obligations en matière de reporting financier sont clairement définies depuis la loi Sarbanes-Oxley en 2002. Leurs attributions sont donc bien comprises.

La notion de gouvernance des risques est vague. En dehors du secteur bancaire, il est rare de trouver des règlementations spécifiques concernant les missions du comité des risques. Réfléchir sur les risques demande créativité et imagination. Exigences qui ne sont peut-être pas toujours expressément attendues des membres du comité d'audit.

« Le comité d'audit est «payé pour penser de manière traditionnelle», dans un monde de communication d'entreprise, de règles de reporting financier et de tests SOX », explique James Lam. « Il existe des règles, des exigences en matière de contrôle interne et des tests très spécifiques ».

Le comité des risques, lui, est «payé pour penser en dehors du cadre ». Sa vision des activités de l'organisation diffère de celle du comité d'audit. Le comité des risques a besoin de différents types d'informations, en l'occurrence de plus d'informations variées, pour guider ses travaux.

La difficulté de trouver un compromis

Réfléchissons un instant. Le responsable d'audit interne transmet des informations au conseil d'administration. Par conséquent, si ce dernier crée des comités d'audit et des risques séparés, le responsable d'audit peut-il rendre compte aux deux ?

Tom McLeod pense que oui. C'est d'ailleurs ce qu'il faisait chez Rio Tinto. Toutefois, des voix discordantes se font entendre, comme celle de Richard Anderson, président du comité des risques de Pay.UK, à Londres, et membre du comité d'audit de cette même entreprise. Selon lui, le management des risques est « aux prises avec les multiples perspectives d'avenir qui s'ouvrent à l'organisation », ce qui le distingue nettement de la fonction d'audit.

L'avènement de la technologie moderne rend cette question particulièrement épineuse. En effet, l'intelligence artificielle, l'automatisation des processus et la visualisation des données aident ensemble, le responsable d'audit interne à identifier les risques et à tester les dispositifs de contrôle interne comme jamais auparavant. C'est la bonne nouvelle.

Mais dès que l'équipe d'audit interne développe ces nouveaux outils d'analyse des risques, ces derniers se transforment immédiatement en outils de management des risques que les fonctions opérationnelles peuvent utiliser pour guider leurs activités.

Par exemple, il serait relativement simple pour les auditeurs internes de développer des algorithmes permettant de repérer les données personnelles recueillies avant qu'un consentement n'ait été donné ou les contrats de sous-traitance signés avant qu'un examen de diligence raisonnable du tiers n'ait été effectué. Par la suite, les équipes de marketing ou de vente pourraient utiliser ces algorithmes pour gérer leurs propres risques. Dans les organisations internationales qui se préoccupent de la protection des données personnelles ou de la corruption, un comité des risques pourrait se pencher sur ces problématiques.

Plans d'action

Examiner les chartes des comités. Le comité d'audit traite les problèmes un par un, des risques de non-conformité à la cybersécurité en passant par la culture d'entreprise et bien d'autres, en plus de ses tâches habituelles de supervision du reporting financier et des dispositifs de contrôle interne. Réexaminez les chartes du comité pour déterminer si un comité des risques capable d'accorder à ces questions toute l'attention qu'elles méritent ne serait pas mieux placé pour traiter ces risques extra financiers.

Évaluer les fonctions d'assurance des risques. De la même manière, examinez toutes les fonctions d'assurance des risques de l'organisation afin de déterminer si la création d'un poste de responsable du management des risques est justifiée. Il y a fort à parier que la plupart des fonctions de première et de deuxième ligne de maîtrise assurent déjà une certaine forme de gestion des risques, même si leur approche manque d'uniformité et de discipline. Si tel est le cas, un responsable du management des risques permettrait-il d'instaurer cette discipline ? Ou une petite organisation peut-elle se contenter d'adopter une méthodologie standard pour parvenir au même résultat ?

Prendre en compte la contribution des technologies au management des risques. L'analyse des données, les outils de visualisation et l'intelligence artificielle pourraient facilement constituer des technologies « à double usage », capables d'aider l'audit interne à évaluer les dispositifs de contrôle et d'autres fonctions à gérer les risques. Votre organisation dispose-t-elle d'une stratégie en matière de technologie pour la guider, pour aider la direction générale et le conseil à prendre de meilleures décisions ?

Dans un monde où l'analyse de données prédomine (monde auquel, selon l'avis général, la fonction d'audit interne devrait s'ouvrir, rappelons-le), où s'arrête l'audit et où commence le management opérationnel des risques ?

Richard Anderson ne mâche pas ses mots quant à la perspective que l'audit interne développe des algorithmes que l'organisation pourrait utiliser pour le management des risques : « Ils ne devraient ni les développer ni les exécuter ». Les organisations devraient élaborer leurs propres modèles, dont l'efficacité sera ensuite testée par la fonction d'audit.

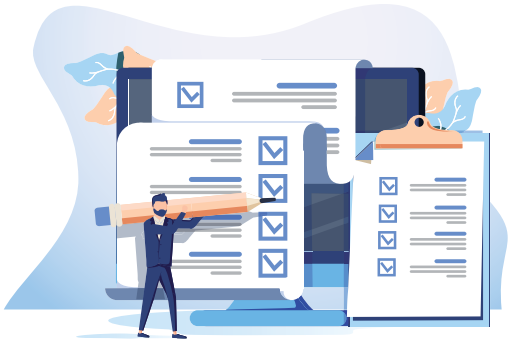
Toutefois, à raison ou à tort, de nombreuses entreprises ne s'y prennent pas de cette manière. Elles préfèrent se lancer dans un management des risques basé sur l'analyse de données et attendent de l'audit interne qu'il leur montre la voie. La raison étant que ce dernier affine ses compétences dans ce domaine depuis des années, notamment en étudiant les transactions financières ou les justificatifs de dépense.

Considérez l'idée dans son ensemble : Tout commence par un besoin urgent du conseil d'améliorer le management des risques sans pour autant définir la manière dont le comité devrait y répondre. Au lieu de cela, le Conseil dit, en substance : « Vous, les auditeurs internes, aidez-nous avec ça ».

Cette dynamique pourrait éventuellement pousser les fonctions d'audit interne et de management des risques à s'unir pour former ce que Tom McLeod appelle la fonction de « Responsable de l'Assurance globale »... le rôle du futur, une fusion de deux entités qui n'ont jamais été bien délimitées ».

Mais il ajoute : « ce qui passe à la trappe de ce fait, c'est l'indépendance ».

Au bout du compte, les conseils d'administration doivent comprendre le caractère unique de la fonction d'audit interne et reconnaître la valeur de son indépendance.



Sondage rapide

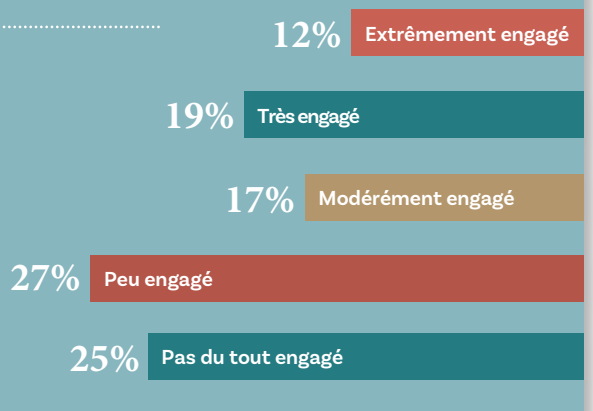
À quelle fréquence la fonction d'audit interne transmet-elle des rapports au comité des risques ?

- ❑ De manière régulière
- ❑ Ponctuellement sur des risques spécifiques
- ❑ Uniquement sur demande
- ❑ Il n'existe pas de comité des risques distinct

Rendez-vous sur **www.theiia.org/tone** pour répondre à cette question et connaître les réponses des autres.

RÉSULTAT DU SONDAGE PRÉCÉDENT

Dans quelle mesure l'audit interne s'engage-t-il à garantir que des informations exactes et complètes sont transmises au Conseil ?



Source : Tone at the Top avril 2019