Accélération

Point de vue sur les questions clés qui dominent l'ordre du jour des comités d'audit.

Édition 2018

kpmg.ca/acceleration

Table des matières

Introduction 3

Se préparer à la révolution de la chaîne de blocs 4

Cybersécurité : un impératif pour le comité d'audit 5

Les contrôles internes après la loi Sarbanes-Oxley 6

Gestion et sécurité des données : se préparer à l'inévitable 7

L'automatisation transforme le service des finances 8

Le risque devrait toujours être à l'ordre du jour 9

Publication externe de l'information : dépasser le statu quo 10

Introduction

Par **Kristy Carscallen**
Associée directrice canadienne, Audit
KPMG au Canada

Le changement n'est pas chose nouvelle pour les comités d'audit. Les jours à venir promettent une évolution technologique constante et de nouveaux risques. L'ampleur des perturbations actuelles oblige les comités d'audit à revoir leur ordre du jour comme jamais auparavant, et cette transformation exige l'attention de tous les membres du conseil.

Dans la première édition du rapport *Accélération*, nous identifions sept tendances clés qui ont des répercussions sur les organisations d'aujourd'hui et chamboulent le mandat des comités d'audit : la chaîne de blocs, les cybermenaces, les contrôles internes, la gestion et la sécurité des données, l'automatisation du service des finances, le risque et les nouvelles formes de rapport élargi.

Qu'il s'agisse de s'adapter aux nouvelles technologies ou d'adopter de nouvelles stratégies de gestion des risques (notamment en matière de gestion de données, de cybersécurité et de contrôle interne), il n'est pas exagéré d'affirmer que les membres des comités d'audit et de la direction ont plus de pain sur la planche que jamais.

La transformation peut être déroutante, surtout lorsqu'elle a l'ampleur de celle qui s'opère en ce moment. Néanmoins, il est possible de surmonter les attentes et les responsabilités accrues en tirant parti des éléments perturbateurs, en se familiarisant avec les risques et les avantages des nouvelles technologies et en résistant à l'envie de maintenir le statu quo.

Les organisations tentent d'accélérer la croissance tout en gérant les perturbations, le risque, les cybermenaces et d'autres questions d'ordre stratégique. Les comités d'audit ont toujours prouvé leur capacité à s'adapter aux besoins de leur organisation, et ils continuent de le faire en ce moment.

Dans les pages qui suivent, des experts techniques à l'échelle de KPMG au Canada analysent les tendances actuelles et mettent en lumière les nombreuses occasions et les défis qui se dressent sur le chemin des comités d'audit. Nous espérons que les informations et les conseils contenus dans ce rapport vous aideront à faire face à ces enjeux et à avoir confiance en la capacité de votre organisation à s'adapter aux changements à venir.

Se préparer à la révolution de la chaîne de blocs

Par **Paritosh Gambhir**
Chef, Chaîne de blocs, associé et leader,
Innovation en audit, Services financiers – Audit, RGT
KPMG au Canada

Informations supplémentaires

Vous attendez toujours que la chaîne de blocs se démode? Ce n'est pas pour demain. Transformant la nature même des transactions, les grands livres numériques et les réseaux pair à pair s'imposent de plus en plus comme la nouvelle norme pour les entreprises tournées vers l'avenir.

C'est une puissante vague technologique qui entraîne tout le monde sur son passage. Les membres du comité d'audit n'y échappent pas : eux aussi doivent rester au fait des progrès technologiques de la chaîne de blocs et s'assurer que l'organisation recherche les processus qui se prêtent le mieux à l'adoption de la chaîne de blocs (connaissance de la clientèle, négociation de titres ou de produits dérivés, gestion de la chaîne d'approvisionnement, expérience clientèle, etc.). Le comité d'audit doit comprendre les risques que représente la chaîne de blocs et les contrôles internes mis en place pour vérifier que chaque maillon de la chaîne se comporte comme prévu. Dans ces étapes critiques, il peut être avisé de s'inspirer du cadre établi par le Committee of Sponsoring Organizations of the Treadway Commission (« COSO ») et de faire appel à des consultants spécialistes de la chaîne de blocs qui ont déjà parcouru le chemin de sa mise en œuvre et savent à quoi s'attendre.

De fait, la mise en œuvre de la chaîne de blocs n'est que le début de l'aventure. L'étape suivante, peut-être la plus importante de toutes, est sa gouvernance. La direction a-t-elle une ligne directrice claire pour déterminer qui peut être ajouté à la chaîne? Quels protocoles l'entreprise emploiera-t-elle? Comment l'activité sera-t-elle surveillée, et qui sera le responsable ultime de la chaîne? Étant donné la nature de la chaîne de blocs, les informations enregistrées (et leur valeur) sont pratiquement inaltérables. Il faut donc préciser clairement la façon dont les informations (et leur valeur intrinsèque) y sont ajoutées, qui en a le contrôle et qui y a accès, et quand les vérifications de conformité ont lieu (si c'est le cas).

La question de la gouvernance est un aspect incontournable que le comité doit définir adéquatement, surtout en ce qui concerne les contrôles internes. À mesure que les entreprises adopteront la chaîne de blocs, les exigences coûteuses en matière de conformité, de communication de l'information et de contrôle interne habituellement associées à la loi Sarbanes-Oxley vont probablement diminuer. Ce sera d'autant plus le cas si l'objectif est d'intégrer la chaîne de blocs à un système de gestion financière ou de gestion des risques (ou un autre processus) déjà en place. Encore une fois, il est essentiel de connaître et de comprendre la technologie et les risques et d'établir des contrôles à l'échelle de l'entreprise.

Qu'on le veuille ou non, la technologie de la chaîne de blocs est maintenant bien implantée. Tandis que l'entreprise se tourne vers les registres numériques et les réseaux décentralisés pour optimiser un nombre croissant de tâches, c'est au comité d'audit qu'il incombe de s'assurer que les risques accompagnant ces nouvelles technologies sont gérés comme il se doit.

Quelles questions les comités d'audit devraient-ils poser?

- La direction a-t-elle élaboré une stratégie à l'égard de la chaîne de blocs?
- La direction dispose-t-elle d'un environnement de contrôle et d'un cadre d'action bien définis?
- Quels contrôles internes sont mis en place pour protéger l'entreprise des risques associés aux technologies nouvelles comme la chaîne de blocs?
- Quels problèmes ou enjeux la stratégie de chaîne de blocs vise-t-elle à résoudre?

Cybersécurité : un impératif pour le comité d'audit

Par **Hartaj Nijjar**
Associé, Cybersécurité,
KPMG au Canada

Informations supplémentaires

La cybersécurité n'est plus uniquement un problème de TI : c'est devenu un important risque d'entreprise. À l'ère des perturbations et de la recrudescence des risques informatiques, la sécurité numérique est une responsabilité partagée par tous les services d'une entreprise. Le comité d'audit n'y échappe pas. Il doit se montrer plus souple dans son approche, plus dynamique dans ses activités et plus adapté au contexte actuel des cyberrisques.

Le comité d'audit n'est pas la seule ligne de défense de l'entreprise, mais il a néanmoins un rôle capital à jouer. Les professionnels des TI et de la sécurité de l'information sont en première ligne, et les membres du comité d'audit doivent soutenir leurs efforts en faisant mieux connaître les menaces qui guettent les services financiers de l'entreprise, en favorisant l'adoption de pratiques exemplaires et en s'assurant que l'entreprise prend les mesures adéquates pour consolider ses cyberdéfenses.

Pour remplir ce rôle, le comité doit poser des questions de fond. Notre stratégie d'entreprise à l'égard de la cybersécurité parvient-elle à identifier efficacement les cyberrisques et à y faire face? Se fonde-t-elle sur les bonnes informations pour surveiller et comprendre ces risques? Englobe-t-elle toutes les obligations en matière de confidentialité et de sécurité des données? S'est-elle dotée d'un plan pour gérer une cybercrise quand un incident se produira?

Le risque lié aux tierces parties doit aussi faire partie de ses préoccupations. L'entreprise élargit son empreinte numérique grâce à l'infonuagique, à la chaîne de blocs et à d'autres technologies en réseau; ce faisant, elle devient plus vulnérable au risque lié aux tiers. Encore une fois, le comité d'audit a tout intérêt à demander comment l'entreprise surveille l'usage que font ses partenaires externes de ses données sensibles et la protection dont ils les entourent, et à s'intéresser à la façon dont l'entreprise évalue l'intégrité des outils et des logiciels qu'ils emploient.

La vitesse des changements exige une grande capacité d'adaptation. Le comité d'audit doit aller au-delà de son approche traditionnelle et faire face aux technologies perturbatrices et aux cyberrisques en temps réel. Il se peut que l'entreprise accuse quelques manques en matière de compétences et de connaissances, mais c'est justement le temps de collaborer avec ses pairs de l'industrie et les consultants pour développer des capacités en interne. C'est la seule façon pour le comité d'audit de remplir son rôle essentiel dans la préparation de l'entreprise aux cyberrisques.

Quelles questions les comités d'audit devraient-ils poser?

- La stratégie de notre entreprise à l'égard des cyberrisques est-elle efficace? Vise-t-elle les bons aspects du problème? A-t-elle été mise à l'essai?
- Notre entreprise s'en tire-t-elle bien par rapport aux autres sociétés du secteur? Quelles sont ses lacunes?
- Lorsque se produira un cyberincident, comment réagira-t-elle? Comment s'en remettra-t-elle?

Les contrôles internes après la loi Sarbanes-Oxley

Par **Genevieve Leong**
Associée, Services-conseils – Gestion des risques
KPMG au Canada

Informations supplémentaires

Les contrôles internes sont parvenus à maturité. Les programmes d'abord conçus pour assurer la conformité aux lois encadrant la communication de l'information financière servent désormais à protéger les sociétés des risques les plus graves. Nombre d'organisations ont aussi transformé leur façon d'évaluer les contrôles internes à l'égard de l'information financière. C'est toute une évolution par rapport aux premiers jours de la loi Sarbanes-Oxley (la loi « SOX »), et ce changement modifie la donne pour les comités d'audit.

Jusqu'ici, les organisations voyaient les contrôles internes du point de vue de la conformité à la SOX. Autrement dit, elles consacraient la plus grande partie de leurs efforts aux contrôles à l'égard de l'information financière. Ce positionnement découlait de l'imposition, en 2002, d'obligations d'information financière nouvelles et élargies faisant suite aux scandales ayant ébranlé plusieurs sociétés ouvertes.

Quinze ans plus tard, les organisations cherchent à tirer davantage de valeur de leurs contrôles internes en rationalisant leurs efforts et en réalisant de nouvelles efficiences technologiques. Certaines ont élargi leurs programmes au-delà des seuls risques liés à la communication de l'information financière et réexaminent leurs contrôles internes dans une optique de gestion des risques d'entreprise et d'exploitation.

En bref, les visées évoluent; les difficultés (et les possibilités) qui en découlent exigent des comités d'audit qu'ils tiennent compte de technologies, de processus de présentation de l'information et de risques qui dépassent la sphère financière à laquelle ils s'intéressent normalement. À mesure que les progrès de l'automatisation des processus par la robotique, de l'intelligence artificielle et de l'analyse de données transforment les environnements de contrôle, les comités d'audit apprivoisent les nouveaux outils à leur disposition.

Les organisations délaissent l'organisation compartimentée pour adopter une structure centralisée et, ce faisant, elles acquièrent une plus grande sensibilité à l'égard des contrôles internes liés à tous les types de risques, de la fraude au cyberrisque et plus encore.

La nécessité de réduire les coûts influe aussi sur l'approche des comités d'audit à l'égard des contrôles internes. De plus en plus d'organisations demandent à tous leurs services de tirer davantage de valeur de leurs programmes de contrôle liés à la loi SOX. Les comités d'audit ne font pas exception et sont invités à rationaliser leur mode de fonctionnement tout en maintenant l'intégrité des activités de l'organisation – et en respectant son budget.

En fin de compte, c'est une ère nouvelle qui commence pour les contrôles internes. Tandis que les organisations renouvellent leur manière d'aborder les programmes traditionnels, les comités d'audit sont appelés à se familiariser avec ce nouveau contexte et à dépasser les bases jetées dans la foulée de la loi SOX.

Quelles questions les comités d'audit devraient-ils poser?

- En matière de contrôles internes, comment l'organisation a-t-elle fait évoluer son programme de contrôle interne, sur le plan de l'évaluation des risques, de la façon d'évaluer l'efficacité des contrôles internes et de la communication de l'information financière?
- À quelles technologies fait-elle appel pour atteindre cet objectif?
- Quelle influence ces changements ont-ils sur le rôle, les responsabilités et les processus du comité d'audit?

Gestion et sécurité des données : se préparer à l'inévitable

Par **Corey Fotheringham**
Associé-leader national, Stratégie et exploitation,
Enquêtes technologiques et cybercriminalité
KPMG au Canada

Informations supplémentaires

On le dit souvent, et non sans raison : la question n'est pas de savoir si un cyberincident se produira, mais bien *quand* il se produira. Nombre d'entreprises prennent ce nouveau dicton très au sérieux et font de la sécurité des données une priorité dans tous leurs services – y compris leur comité d'audit.

L'ère des dossiers papier et des classeurs fermés à clé tire à sa fin. De nos jours, les comités d'audit manipulent des données financières sensibles qui doivent être stockées, archivées et transmises par des réseaux de serveurs, des réseaux internes et des services infonuagiques. Bien que les avantages de l'ère numérique soient innombrables, les risques de vol, de perte ou de fuite de données sont suffisamment importants pour faire perdre le sommeil aux membres des comités d'audit.

Après tout, le fait d'omettre de protéger des données financières peut causer des pertes financières et des atteintes à la réputation. Il existe des règlements sur la protection des données, des lois sur la dénonciation obligatoire et des obligations internationales en matière de confidentialité (comme le *Règlement général sur la protection des données en vigueur* dans l'UE) qui, s'ils ne sont pas respectés, peuvent entraîner des pénalités considérables. Qui plus est, même la marque la mieux réputée risque de subir des dommages irréversibles si le public apprend qu'elle est victime d'une cyberattaque.

Les comités d'audit ne mesurent pas nécessairement la gravité de ces risques. Ils jouent néanmoins un rôle crucial dans le respect des politiques de gestion et de sécurité des données et doivent veiller à ce que la cybersécurité demeure une priorité pour les dirigeants de l'entreprise.

En tant que gardiens de données vitales sur l'entreprise et sa clientèle, ils doivent soulever d'importantes questions : quelles données possédons-nous? Quelle en est la valeur? Où ces données sont-elles stockées? S'il y avait une fuite, quelles seraient les conséquences pour l'entreprise et comment y ferions-nous face?

Comme pour toute autre composante d'une organisation, les comités d'audit partagent la responsabilité de comprendre la mesure dans laquelle l'entreprise est exposée, d'attirer l'attention sur les risques liés à la cybersécurité et de collaborer avec leurs collègues pour améliorer les stratégies de gestion et de sécurité des données. Ce n'est que lorsque toutes ces composantes s'engagent à fond pour mieux la prémunir contre les cyberattaques qu'une société peut véritablement se dire préparée à la cybercrise qui ne manquera pas de se produire.

Quelles questions les comités d'audit devraient-ils poser?

- Quelles données possédons-nous? Quelle en est la valeur?
- Si nos données étaient volées, à quoi l'entreprise serait-elle exposée et comment réagirait-elle?
- De quels moyens dispose le comité d'audit pour améliorer la position de l'entreprise devant les cybermenaces?

L'automatisation transforme le service des finances

Par **Stephanie Terrill**
Associée et leader mondiale,
Gestion financière
KPMG au Canada

Informations supplémentaires

L'automatisation extrême modifie à toute vitesse le fonctionnement même des entreprises et de leur service des finances. Tandis que les entreprises se tournent vers les services infonuagiques et les systèmes reposant sur l'analyse des données, il est important que toutes les parties en cause s'engagent à fond dans l'automatisation des processus et contrôles financiers au moyen de technologies perturbatrices telles que les progiciels de gestion intégrés (ERP) infonuagiques, l'intelligence artificielle, l'informatique cognitive, l'automatisation des processus par la robotique et la chaîne de blocs.

L'automatisation extrême supprime le risque que comportent les processus routiniers et procure à l'utilisateur des résultats plus garantis à un coût moins élevé. La plupart du temps, elle est appliquée aux processus transactionnels répétitifs; pour en maintenir l'intégrité, elle utilise des contrôles d'application intégrés, des rapports sur les exceptions et la mise à l'essai des contrôles de cybersécurité.

Les entreprises sont de plus en plus forcées d'adopter de nouvelles technologies et d'abaisser les coûts de leur service des finances, ce qui tend à accélérer la course à l'automatisation extrême. Il en va de même de la nécessité de mieux comprendre le fonctionnement des technologies d'automatisation, leur relation avec les autres fonctions et leur incidence sur l'environnement de contrôle. Pour le comité d'audit, la diligence raisonnable comprend le fait de poser à la direction les bonnes questions sur la séparation des tâches au sein des principales applications et d'une application à l'autre, et de vérifier que le chef de l'information et celui de l'audit interne collaborent pour assurer la sécurité et la séparation des tâches. Ce dernier aspect était déjà important bien avant l'avènement des technologies perturbatrices et de l'automatisation extrême, mais il s'agit maintenant d'appliquer les principes fondamentaux d'un cadre de contrôle à un environnement qui englobe les locaux de l'entreprise et l'infonuagique.

Le risque lié aux tiers doit également être pris en compte. Les entreprises se tournent massivement vers les logiciels-services, de sorte que davantage de parties externes se trouvent intégrées à leur réseau numérique. Ces parties externes comprennent les intervenants ayant conçu et mis en application leur service infonuagique, de même que ceux qui y accèdent de manière continue. Ici aussi, la gestion des accès et la séparation des tâches revêtent une importance capitale, tant pour déterminer qui peut détenir l'autorisation d'accéder au système que pour surveiller les activités de ces personnes. Il est avantageux de bien comprendre les politiques et les rôles des tiers et d'intégrer à chaque contrat des dispositions sur les risques liés aux tiers.

En fin de compte, la préparation en vue de l'automatisation relève du devoir de diligence de chacun. Pour le comité d'audit, elle suppose aussi d'aller de l'avant avec une certaine curiosité à l'égard des nouvelles technologies, de se montrer ouvert à l'automatisation extrême et de se réconcilier avec les perturbations.

Quelles questions les comités d'audit devraient-ils poser?

- La direction a-t-elle institué une séparation des tâches appropriée pour les systèmes automatisés?
- Quelles sont les politiques qui encadrent les logiciels-services et comment ceux-ci sont-ils surveillés?
- Comment la direction adapte-t-elle son mode de gestion des risques et des contrôles pour assurer la sécurité de ses systèmes à mesure qu'interviennent de nouvelles technologies d'automatisation et de nouveaux fournisseurs de logiciels?
- Comment le risque lié aux tiers est-il géré? Avec qui faisons-nous affaire et quels contrôles diligents avons-nous mis en œuvre à l'égard de nos partenariats et de nos fournisseurs?

Le risque devrait toujours être à l'ordre du jour

Par **Heather Cheeseman**
Associée, Énergie et ressources naturelles
KPMG au Canada

Informations supplémentaires

Le risque est de nature subjective. Les menaces et les vulnérabilités sont différentes d'une organisation à l'autre et, par conséquent, les stratégies de gestion des risques et les responsabilités diffèrent aussi. Le rôle du comité d'audit n'est donc pas le même d'une société à l'autre. Cependant, le comité le plus efficace est toujours celui qui peut compter sur une approche bien définie par le conseil d'administration.

À quels signes reconnaît-on une approche bien définie venant du conseil d'administration? Tous les membres du conseil d'administration savent que la responsabilité de surveiller la gestion du risque leur revient. Les rôles et les mandats des comités sont clairement définis de façon que l'expertise des administrateurs et des comités soit mise à profit et qu'ensemble, tous s'assurent que l'entreprise a identifié, mesuré et priorisé ses principaux risques. Le conseil d'administration tient compte des risques lorsqu'il s'engage à soutenir les plans stratégiques de l'entreprise, il approuve les mesures prises pour faire face aux risques et il surveille leur mise en application.

Il faut garder en tête qu'un risque n'est pas nécessairement une menace. Un risque peut aussi être l'indice d'une occasion de croissance ou d'innovation que l'entreprise peut décider d'exploiter. Les réponses stratégiques (visant à réduire les répercussions négatives ou à tirer profit des possibilités positives) doivent reposer sur des informations fiables au sujet des risques et respecter la tolérance au risque de l'entreprise.

Les risques ne sont jamais statiques, et il est impossible de les confiner dans des espaces clos. Les risques évoluent, prennent de l'ampleur et se rattachent à d'autres risques par des liens complexes et inattendus. Sans boule de cristal, on ne peut prédire avec précision les conséquences de ces risques interconnectés ayant un effet multiplicateur. Mais le conseil d'administration doit remettre en cause les décisions de la direction afin d'évaluer l'ensemble des interactions entre les risques. Étant donné la vitesse des changements et la complexité des affaires dans un monde sans cesse plus connecté, il est pratiquement impossible de vouloir comprendre et gérer tous les risques à l'horizon (virtuel). Le conseil d'administration doit garder dans sa ligne de mire les entraves possibles à la réalisation des objectifs stratégiques de l'entreprise. Les organisations doivent prioriser les risques en fonction de leur gravité et de leur probabilité de matérialisation en s'appuyant sur un cadre ou une échelle d'évaluation établis.

La bonne nouvelle, c'est que le conseil n'est pas laissé à lui-même. Il existe une multitude de ressources et de conseillers externes prêts à collaborer avec le conseil pour pallier les éventuelles lacunes en matière de compétences et à fournir les outils et l'aide nécessaires à l'exécution d'une approche de gestion du risque véritablement dynamique.

Quelles questions les comités d'audit devraient-ils poser?

- Les rôles et les responsabilités de surveillance des risques sont-ils clairement définis au niveau du conseil d'administration?
- Comment l'entreprise fait-elle pour identifier, évaluer et atténuer ses risques critiques?
- Comment avons-nous pris en compte l'évaluation du risque au moment d'établir le plan stratégique de l'entreprise?
- Quel degré de risque l'entreprise consent-elle à prendre pour atteindre ses objectifs?
- Comment avons-nous évalué l'incidence des risques les uns par rapport aux autres? Quelle est la dépendance d'un risque par rapport à un autre et comment les répercussions de l'un multiplieront-elles la gravité de l'autre?

Publication externe de l'information : dépasser le statu quo

Par **Bill Murphy**
Leader national, groupe Changement climatique et développement durable
KPMG au Canada

Informations supplémentaires

Il est temps d'élargir votre surveillance de l'information publiée en externe. Les tendances et les directives en matière de communication de l'information ont évolué, et les comités d'audit doivent répondre à de nouvelles attentes. Avant de communiquer des rapports aux parties prenantes hors du cercle de l'entreprise, il convient d'examiner ces nouveautés.

Les organismes de réglementation des valeurs mobilières s'intéressent de très près au recours à des mesures non conformes aux PCGR dans le rapport de gestion du rapport annuel et dans les communiqués de presse qui s'y rapportent. À leur tour, les comités d'audit sont appelés à examiner plus à fond ces mesures et à s'assurer qu'ils en comprennent la définition et l'utilisation ainsi que les rapprochements présentés à leur sujet.

Les comités d'audit doivent aussi se pencher sur les nouveaux thèmes abordés dans le rapport annuel. De nouvelles rubriques sont ajoutées sous l'effet de diverses tendances, la première étant la formulation de recommandations telles que celles du Groupe de travail sur l'information financière relative aux changements climatiques (« GIFCC »). Ces recommandations réclament la communication d'informations accrues sur les risques financiers importants que représentent les changements climatiques pour le modèle économique, les services, la chaîne d'approvisionnement et la clientèle des sociétés. Ces risques pourraient avoir des répercussions négatives sur l'accès aux capitaux et la rentabilité des sociétés. À l'heure actuelle, l'adhésion aux recommandations du GIFCC est volontaire, mais divers organismes de réglementation les étudient, comme c'est le cas des Autorités canadiennes en valeurs mobilières. De nouveaux thèmes s'invitent aussi dans le rapport annuel en raison des obligations d'information sur la diversité.

L'analyse approfondie des stratégies et de la création de valeur à long terme des sociétés est la seconde tendance observée. Notons par exemple l'obligation de publier un rapport stratégique et les directives qui entourent ce rapport, lesquelles sont publiées par le Financial Reporting Council au Royaume-Uni. Bien que les sociétés nord-américaines ne soient pas assujetties à une obligation semblable, les grands investisseurs institutionnels exigent de plus en plus souvent des informations accrues sur la façon dont les émetteurs de titres se positionnent pour créer de la valeur à long terme et la faire durer.

Par ailleurs, les communications externes ne se limitent plus au seul rapport annuel. S'y sont ajoutés progressivement les rapports sur le développement durable et les changements climatiques, les rapports sur les émissions de carbone et les réponses à une multitude de sondages et de questionnaires menés après des investisseurs. En parallèle, divers organismes dont on ne démêle plus les sigles y sont allés de leurs directives pour encadrer toutes ces publications, qu'il est loin d'être simple d'adopter et de surveiller. C'est à cette fin qu'un projet de dialogue entre les normalisateurs a été mis sur pied, dans le but de travailler à une harmonisation des directives sur la communication de l'information.

Pour s'y retrouver parmi ces nouvelles formes de rapport, les sociétés doivent se doter de processus et de contrôles qui transcendent le domaine habituel des finances et demander à leur personnel de direction et à leur comité d'audit d'exercer une supervision plus serrée. Les comités d'audit sont invités à réexaminer l'état actuel des choses et à se renseigner sur la façon dont les informations accrues sont rassemblées, compilées et publiées. Ils doivent aussi vérifier si les contrôles et procédures de communication de l'information actuels sont restés adéquats.

Quelles questions les comités d'audit devraient-ils poser?

- Les contrôles et procédures de communication de l'information de la société et le mandat de son comité d'audit sont-ils suffisamment larges pour englober ces formes de rapport élargi?
- Comment les informations accrues sont-elles rassemblées, compilées et publiées?
- Comment le comité d'audit peut-il se tenir au fait de ces nouvelles formes de rapport externe, compte tenu de leur expansion rapide?

Réalisons-le.

En tant que membre de comité d'audit, vous avez la responsabilité d'aider votre organisation à s'orienter parmi les nombreux enjeux et défis plus complexes que jamais auxquels elle fait face. Vous devez mettre l'accent sur la croissance, le risque et les perturbations, tout en vous acquittant de votre mandat traditionnel de gouvernance et de présentation de l'information. Voilà la nouvelle norme au sein des comités d'audit.

Bien que le défi n'ait jamais été aussi grand, KPMG peut vous aider à acquérir la confiance dont vous avez besoin pour vous orienter dans le domaine en évolution de l'audit et de la certification et vous donner les outils nécessaires pour accélérer la croissance de votre entreprise. **Réalisons-le.**

Allez au kpmg.ca/acceleration pour visionner les vidéos des entrevues avec chacun des experts techniques nommés dans ce rapport.

Collaborateurs

Kristy Carscallen
Associée directrice canadienne, Audit
KPMG au Canada
416-777-8677
kcarscallen@kpmg.ca
LinkedIn

Heather Cheeseman
Associée, Énergie et ressources naturelles
KPMG au Canada
416-777-3314
hcheeseman@kpmg.ca
LinkedIn

Corey Fotheringham
Associé et leader national, Stratégie et opérations
Enquêtes technologiques et cybercriminalité
KPMG au Canada
416-218-7974
coreyfotheringham@kpmg.ca
LinkedIn

Paritosh Gambhir
Chef, Chaîne de blocs, leader du groupe Innovation
en audit, RGT, Associé, Audit, Services financiers
KPMG au Canada
416-777-3335
pgambhir@kpmg.ca
LinkedIn

Genevieve Leong
Associée, Services-conseils –
Gestion des risques
KPMG au Canada
416-777-3226
genevieveleong@kpmg.ca
LinkedIn

Bill Murphy
Leader national, Changement climatique
et développement durable
KPMG au Canada
416-777-3040
billmurphy@kpmg.ca
LinkedIn

Hartaj Nijjar
Associé, Cybersécurité
KPMG au Canada
416-228-7007
hnijjar@kpmg.ca
LinkedIn

Stephanie Terrill
Associée et leader mondiale, Gestion financière
KPMG au Canada
403-691-8374
sterrill@kpmg.ca
LinkedIn

kpmg.ca/acceleration