L'échange CCRC

Mars 2016

La surveillance des risques liés aux TI par le comité d'audit

L'enjeu

Les technologies et les systèmes d'information sont des composantes essentielles de la stratégie et des activités d'une organisation, rendant possibles les innovations et les gains d'efficience pour tous ses processus d'affaires.

Toutefois, la dépendance de plus en plus marquée à l'égard des technologies et le rythme des changements technologiques se traduisent également par une élévation des niveaux de risque et de vulnérabilité dans des domaines tels que la sécurité, la confidentialité, la reprise après sinistre et la gouvernance.

Le Conseil canadien sur la reddition de comptes (CCRC) a été informé par des comités d'audit que, pour eux et pour les conseils d'administration, les risques liés aux TI comportent un degré de priorité de plus en plus élevé, bien qu'ils se sentent souvent mal équipés pour s'acquitter de leur rôle de surveillance à cet égard. En se familiarisant avec les risques d'entreprise et en posant les bonnes questions aux auditeurs externes, aux auditeurs internes et à la direction, les comités d'audit peuvent en arriver à gérer plus facilement les risques liés aux TI de leur organisation et à protéger plus efficacement les actifs informationnels de celle-ci.

Les plus grands défis que posent les TI aux comités d'audit

La sécurité et la confidentialité des systèmes d'information, la mise en œuvre ou la conversion de systèmes, le maintien des activités et la reprise après sinistre, de même que les ententes conclues avec des tiers ou le recours à des services d'externalisation comptent parmi les enjeux commerciaux courants liés aux TI qui peuvent présenter des risques et qui constituent souvent des sources de préoccupation pour les comités d'audit.

Selon eux, les risques découlant du rythme des changements technologiques (technologies émergentes, technologies mobiles, médias sociaux, analyse de données et informatique en nuage) ainsi que les risques liés à la cybersécurité (protection des données et propriété intellectuelle) sont les risques liés aux TI qui représentent maintenant les plus grands défis pour leur organisation[1].

La surveillance de la gestion des risques liés aux TI

Jusqu'à maintenant, le rôle du comité d'audit était surtout axé sur l'information financière et les processus de contrôle interne connexes. Toutefois, bien des comités d'audit doivent s'acquitter d'un mandat élargi qui comprend la surveillance des systèmes et processus de gestion des risques d'entreprise de leur organisation, s'agissant aussi bien des risques stratégiques et opérationnels que des risques environnementaux et des risques de non-conformité. Bien que l'on retrouve parfois un comité de gestion des risques dans certains conseils d'administration, au Canada, c'est surtout le cas dans les grandes institutions financières. En l'absence d'un comité de gestion des risques distinct, la responsabilité de la surveillance de la gestion des risques est souvent déléguée au comité d'audit. C'est pourquoi il importe que celui-ci connaisse bien les risques à l'échelle organisationnelle ainsi que les processus de gestion des risques connexes.

À de nombreux égards, les risques liés aux TI sont devenus des enjeux de gestion des risques à l'échelle de l'entreprise auxquels il convient de s'attaquer en faisant preuve de stratégie et en mettant à contribution de multiples fonctions, plutôt que de considérer qu'il s'agit de problèmes techniques ne relevant que du service informatique. Lorsque le comité d'audit assume la responsabilité de la surveillance du cadre de gestion des risques d'entreprise de l'organisation, il doit veiller à ce que celui-ci prenne en compte les risques appropriés liés aux TI et à ce que soient dressés un plan d'atténuation des risques et un plan d'intervention.

[1] KPMG 2015 Global Audit Committee Survey

La gestion de risques spécifiques liés aux TI

La direction a la responsabilité d'identifier, d'évaluer, de contrôler et d'atténuer au quotidien les risques liés aux TI. Une fois que les risques liés aux TI de l'organisation sont connus et que les processus et contrôles mis en place par la direction sont compris, le comité d'audit peut choisir de chercher à obtenir une opinion ou une assurance indépendante quant à savoir si la direction a su ou non atténuer ces risques et quant à la façon dont elle s'y est prise. Une telle opinion ou assurance peut être obtenue auprès de l'auditeur externe, de l'auditeur interne ou d'autres spécialistes externes à l'entreprise. Il importe que le comité d'audit ait, avec toutes les parties, des échanges lui permettant de cerner l'étendue de ses responsabilités et de ses capacités.

L'auditeur externe
L'auditeur externe a l'obligation de se familiariser avec l'environnement de contrôle des TI ainsi qu'avec la façon dont les systèmes informatiques sont utilisés aux fins de la prise en charge du processus d'information financière. Lorsqu'une stratégie axée sur les contrôles est privilégiée, l'auditeur externe évalue la conception et l'efficacité du fonctionnement des contrôles généraux informatiques (CGI) appliqués aux systèmes informatiques prenant en charge l'information financière, généralement en se concentrant sur les accès et les modifications à ces systèmes[2]. Toutefois, un bon nombre des aspects présentant des risques liés aux TI qui préoccupent de plus en plus les comités d'audit peuvent ne pas être considérés comme étant directement à l'origine d'un risque d'anomalie significative, ceux-ci étant amenés à les exclure du domaine de l'information financière, au moins jusqu'à ce que survienne un événement important.

L'auditeur interne
Dans les entreprises disposant d'une fonction d'audit interne, le mandat de l'auditeur interne peut englober les secteurs opérationnels et les principaux risques organisationnels, et l'amener à examiner une plus grande sélection de risques liés aux TI et de systèmes informatiques, qui ne sont pas liés uniquement à l'information financière. Le comité d'audit doit passer en revue le plan d'audit interne pour l'exercice visé, tout en veillant à ce qu'il soit harmonisé avec le cadre général de gestion des risques d'entreprise et à ce qu'il prenne en compte les secteurs de risque devant être ciblés par l'audit.

> **La cybersécurité et l'audit externe**
>
> Étant donné les cas persistants et très médiatisés d'atteinte à la sécurité de l'information, la cybersécurité reste à l'avant-plan des préoccupations de la plupart des conseils d'administration et des comités d'audit. Dans le cadre de l'audit des états financiers, l'auditeur externe est amené à se concentrer surtout sur le risque d'accès ou de modification non autorisés aux systèmes les plus près de l'application prenant en charge le processus d'information financière, soit, outre l'application même, la base de données et le système d'exploitation sur lesquels elle repose. Toutefois, le risque de cyberincident est généralement plus élevé du côté du périmètre externe et du réseau interne, qui ne font actuellement pas partie de l'étendue de l'audit, car ils sont plus éloignés des données des applications et qu'ils sont donc moins susceptibles de présenter un risque d'anomalie significative.
>
> De plus, alors que les auditeurs externes se concentrent sur les systèmes qui pourraient influer sur l'information financière, d'autres systèmes, sans lien avec l'information financière, peuvent s'avérer essentiels au maintien des activités permanentes d'une entreprise et être vulnérables aux attaques. Sur le plan de la cybersécurité, il importe que les comités d'audit sachent ce qui est vérifié ou non par les auditeurs externes.

Où chercher de l'aide

Après avoir identifié les risques spécifiques liés aux TI et avoir pris en compte les risques qui font partie de l'étendue de l'audit externe ou qui sont examinés par l'auditeur interne, le comité d'audit doit identifier les aspects à l'égard desquels il est nécessaire d'obtenir un niveau d'assurance plus élevé. Le comité d'audit peut demander le soutien de diverses parties, notamment celui de l'auditeur externe, de l'auditeur interne et d'autres spécialistes externes à l'entreprise. Ce faisant, il peut prendre en compte ce qui suit :

- De nombreux cabinets d'experts-comptables disposent de ressources spécialisées dans le domaine des risques liés aux TI et peuvent fournir du soutien à d'autres égards que l'audit externe. Lorsque les services de l'auditeur externe sont retenus, son indépendance doit être prise en compte. Toutefois, dans la plupart des cas, l'auditeur externe peut fournir d'autres services que l'audit des états financiers sans pour autant enfreindre les règles d'indépendance, pourvu qu'il n'assume pas la responsabilité de la conception ou de la mise en œuvre du système de contrôle interne. Avant de faire appel à l'auditeur externe pour la prestation de services supplémentaires, la direction et le comité d'audit doivent passer en revue les exigences en matière d'indépendance.
- En raison de facteurs tels que les restrictions relatives à l'indépendance de l'auditeur externe ou les ressources et/ou les compétences limitées du service d'audit interne, le comité d'audit peut être amené à envisager de confier à d'autres spécialistes externes à l'entreprise l'évaluation des risques liés aux TI de l'organisation.

[2] Dans les cas où l'auditeur s'appuie sur des contrôles informatisés ou sur des contrôles dépendant de systèmes informatiques.

Questions pour les comités d'audit

Les comités d'audit doivent adopter une approche proactive afin de se familiariser avec les principaux risques liés aux TI et la façon d'y répondre. Cette approche consiste à faire en sorte que la direction rende des comptes à l'égard de l'identification et de l'atténuation des risques liés aux TI, à savoir quels sont les risques que l'auditeur externe et l'auditeur interne évaluent et à identifier les aspects qui ne sont pas pris en compte, lesquels pourraient être confiés à d'autres spécialistes externes à l'entreprise. Voici une liste de questions que les comités d'audit doivent prendre en considération :

1. De quel(s) administrateur(s) la responsabilité de la surveillance des risques liés aux TI relève t-elle? Si cette responsabilité a été confiée au comité d'audit, celui-ci est-il suffisamment informé et a-t-il le savoir-faire nécessaire pour s'en acquitter adéquatement?
2. L'organisation dispose-t-elle d'un cadre de gestion des risques d'entreprise prenant en compte les risques liés aux TI?
3. Le conseil d'administration et le comité d'audit conviennent-ils que la direction a su identifier et atténuer les principaux risques liés aux TI?
4. Quels sont les applications et les systèmes connexes que l'auditeur externe a intégrés à l'étendue de l'audit des états financiers?
5. Quelles sont les procédures d'audit que l'auditeur externe a mises en œuvre pour répondre aux risques liés aux TI?
6. L'auditeur externe a-t-il identifié toutes les déficiences sur le plan des TI? Le cas échéant, où ces déficiences se trouvaient-elles? Comment ont-elles été corrigées? Quelles ont été les répercussions pour l'entreprise?
7. L'auditeur externe a-t-il identifié d'autres aspects potentiellement vulnérables qui n'influent peut-être pas directement sur l'information financière?
8. Le plan d'audit interne est-il harmonisé avec le cadre de gestion des risques d'entreprise?
9. Le service d'audit interne a-t-il les compétences, les ressources et le savoir-faire nécessaires pour mettre en œuvre un plan d'audit répondant aux principaux risques liés aux TI au sein de l'organisation?
10. En combinant l'étendue des travaux de l'auditeur externe à celle des travaux de l'auditeur interne, obtient-on un niveau d'assurance adéquat quant aux principaux risques liés aux TI?

Pour en apprendre davantage

Rendez-vous sur notre site Internet à l'adresse www.cpab-ccrc.ca et inscrivez-vous à notre liste de diffusion.
Suivez-nous sur Twitter — @CPAB-CCRC

www.cpab-ccrc.ca / Courriel: info@cpab-ccrc.ca

CPAB
CCRC