Deloitte.

Administrateurs avertis
AU-DELÀ DE LA CONFORMITÉ

# Réussir en période de changement et d'incertitude : plans d'action à l'intention des comités d'audit

## Tirer parti de l'évolution technologique

L'époque où la technologie était du seul ressort du service des TI, où elle ne sortait pas du cadre physique de l'organisation et où elle servait exclusivement à des activités liées au travail est révolue.

Pratiquement toutes les activités reposent aujourd'hui sur la technologie. Il n'y a plus de cloison entre l'utilisation des technologies à des fins personnelles et pour le travail, les travailleurs se servant des ordinateurs du bureau pour des tâches personnelles et de leurs propres appareils pour le travail.

La technologie faisant désormais partie intégrante de la quasi-totalité des activités et des projets, la responsabilité des comités d'audit ne s'arrête pas au contrôle des budgets et au déploiement des systèmes. Ils doivent aussi s'assurer que les contrôles appropriés sont en place pour garantir la sécurité des données et la confidentialité des renseignements personnels. Ces contrôles peuvent être des programmes de formation, les procédures habituelles relatives aux mots de passe, aux pare-feu et aux antivirus ainsi que des pratiques de suivi et de surveillance.

### AVEC (« Apportez votre équipement personnel de communication »)

Dans les entreprises adeptes de la philosophie AVEC, les employeurs s'attendent à joindre les employés à toute heure et ces derniers doivent être prêts à leur répondre quel que soit l'endroit où ils se trouvent. Ce courant donne aux organisations des possibilités de réduire les coûts d'approvisionnement, d'accroître l'efficience et de renforcer l'engagement des employés. Il leur impose toutefois aussi de prendre en charge le soutien technique et l'entretien matériel des appareils de leurs employés ainsi que la compatibilité de ces appareils avec les technologies qu'elles utilisent, la formation et le remboursement des dépenses des employés.

### L'infonuagique

Grâce à l'infonuagique, les données sont accessibles de pratiquement n'importe où, ce qui permet aux employés de travailler où ils veulent. Cette grande liberté d'accès aux données rend leur protection primordiale. Des programmes de protection robustes doivent être mis en place tant par l'organisation que par ses fournisseurs externes et doivent comprendre des enregistrements de sauvegarde fiables, des plans de reprise après sinistre, des mots de passe, des pare-feu et des programmes de cybersécurité.

### Les services partagés

L'impartition est un moyen efficace et efficient de se doter de ressources compétentes pour effectuer diverses tâches accessoires. Cependant, même si ces activités sont exécutées à l'extérieur de l'organisation, la direction en conserve la responsabilité. Les comités d'audit doivent donc s'assurer que les contrôles appropriés ont été mis en place pour protéger l'information utilisée par le fournisseur externe et pour garantir la fiabilité de l'information que le fournisseur crée pour l'organisation. Comme cette dernière demeure propriétaire des données, elle doit installer des programmes de protection pour récupérer les données, impartir le service à un autre fournisseur ou rapatrier le service dans l'organisation si des problèmes surviennent.

### Médias sociaux

Les entreprises utilisent les médias sociaux pour tisser des liens avec les clients et leurs autres parties prenantes importantes et pour accroître leur propre efficacité et leur efficience.

## Plan d'action du comité d'audit…

- S'assurer que la stratégie en matière de technologie de l'information est alignée sur la stratégie d'affaires globale de l'organisation.
- Comprendre et gérer les risques liés à la technologie auxquels est exposée l'organisation, y compris en ce qui a trait à la cybersécurité.
- Passer régulièrement en revue les politiques relatives à la technologie de l'information afin de s'assurer qu'elles tiennent compte des nouvelles technologies.

Les médias sociaux dispensent les organisations d'offrir des services d'abonnement, grands consommateurs de temps et de ressources, et dans nombre d'entre elles, les abonnés se connectent au moyen de leur profil de média social. C'est un peu comme confier la gestion de la relation client à un tiers et cela évite à l'organisation d'avoir à conserver des informations personnelles ou à se doter de plateformes spécialisées de publipostage.

De telles activités reposent sur les informations des abonnés et des contrôles doivent donc être mis en place pour protéger ces informations d'une utilisation répréhensible. Les organisations doivent aussi se doter d'un plan de reprise après sinistre pour pouvoir continuer à communiquer avec leurs abonnés advenant un problème avec les services de médias sociaux.

## Les cybermenaces

Les organisations ne doivent pas sous-estimer les menaces cybernétiques auxquelles elles sont exposées, directement ou du fait de leurs relations avec les autres.

Les cybermenaces sont en fait la nouvelle forme prise par des risques qui existaient déjà. Elles exigent que les mesures de gestion des risques prises pour des lieux physiques soient adaptées aux installations virtuelles et comprennent des procédures concernant les droits d'accès, des plans de reprise après sinistre, la vérification des antécédents, la vérification qu'une équipe qualifiée est en place, des programmes de formation pour accroître les compétences des employés, etc. De nouveaux outils sont aussi en cours de développement pour aider à atténuer les risques de cybermenaces. Ils s'apparentent aux logiciels antivirus, recueillent des renseignements sur les cyberattaques auprès d'organisations participantes et se servent de l'analyse des données pour déceler les indices de menaces potentielles en vue de déployer des stratégies de défense appropriées.

## L'analytique de données

Tous les logiciels collectent des données à diverses fins : approvisionnement, facturation, abonnements, recrutement et autres.

Grâce à l'arrivée de technologies moins chères et plus puissantes, les organisations de toutes tailles peuvent faire des recoupages entre les données brutes collectées afin de créer des renseignements utiles.

L'analytique de données est un outil puissant qui peut aider la direction à prendre des décisions éclairées, sous réserve de certaines conditions importantes :

- **Respect de la vie privée et confidentialité.** Les organisations collectent souvent des données dans un but précis, par exemple un abonnement. Elles ne doivent cependant pas utiliser ces données à d'autres fins, par exemple pour repérer les occasions de vendre des services supplémentaires, sans autorisation légale et sociale de le faire.
- **Expertise.** L'analytique de données, qui puise des données filtrées dans diverses bases de données, exige le recours à des experts bien informés pour évaluer toutes les variables et transformer ces données en renseignements utiles.

Les comités d'audit doivent s'assurer que des mesures de protection adéquates ont été prises pour préserver l'intégrité des activités liées à l'analytique de données. Parmi de telles mesures, on trouve les programmes de formation du personnel, l'instauration d'une politique sur le respect de la vie privée et la signature d'accords de confidentialité pour encadrer l'utilisation et la diffusion des données, la mise en place de droits d'accès aux données saisies et l'obtention du consentement exprès des personnes ayant fourni des renseignements confidentiels.

## Le service des TI

Bien que le service des TI ne soit plus le seul responsable de la technologie au sein de l'organisation, il joue encore un rôle pivot et ce rôle est appelé à être de plus en plus important à mesure que la technologie continue à se répandre. Un programme de formation continue doit être instauré à l'intention des membres de l'équipe des TI afin qu'ils actualisent leurs connaissances sur les nouvelles technologies et puissent soutenir l'organisation et agir comme conseillers stratégiques auprès de la haute direction et du conseil d'administration.

Pour télécharger le rapport complet ou communiquer avec un de nos experts, cliquez ici : www.deloitte.com/ca/comitesdauditperformants.