Renforcer la résilience et la productivité malgré les perturbations

Par sa fonction de gouvernance et de surveillance de l'innovation, le comité d'audit joue un rôle crucial dans la résilience.

Virages brusques des marchés, incertitude économique et technologies transformatrices : les entreprises doivent composer avec des perturbations sans précédent. Dans ce contexte volatil, où les risques sont corrélés et imprévisibles, il est essentiel de renforcer la résilience de l'entreprise pour soutenir sa performance et sa croissance. Il ne suffit plus de réagir aux événements. De plus en plus, la résilience nécessite de faire appel à la planification de scénarios et à la gestion prédictive afin d'anticiper les risques, de vérifier par des tests si l'entreprise est prête à y faire face et de savoir prendre des décisions à point nommé. Les comités d'audit occupent un rôle déterminant dans la préservation de la résilience : ils orientent la gouvernance proactive des risques et favorisent la productivité en supervisant la transformation, l'adoption de l'IA et le perfectionnement de l'effectif.

> « Le comité d'audit doit voir plus loin que les risques aisément identifiables. Il doit acquérir une compréhension des risques de deuxième et de troisième ordre susceptibles d'entraver les services offerts à la clientèle de l'entreprise.

Akber Merchant
Associé, Services-conseils en réglementation et en gestion des risques
KPMG au Canada

Le risque géopolitique, un élément perturbateur de premier plan

Les forces géopolitiques sont devenues un vecteur prépondérant de la volatilité économique mondiale. En 2024, le nombre de conflits armés dans le monde était le plus élevé enregistré depuis 1946 – avec toutes les perturbations que cela entraîne pour les chaînes d'approvisionnement, les échanges commerciaux et les marchés mondiaux[1]. En 2025, les droits de douane annoncés par les États-Unis ont occasionné d'importantes turbulences sur les marchés et une volatilité semblable à celle du début de la pandémie de COVID-19.

[1] Université Uppsala, « UCDP: Sharp increase in conflicts and wars », consulté le 4 novembre 2025.

Alors que les États-Unis redéfinissent les relations commerciales, ce sont les organisations canadiennes de tous les secteurs qui s'en ressentent directement. Les droits de douane américains compromettent les revenus et les chaînes d'approvisionnement des entreprises, et les perspectives économiques du Canada s'assombrissent. D'après notre sondage de 2025 sur les perspectives des chefs de direction, la résilience de la chaîne d'approvisionnement est en tête des sujets de préoccupation des dirigeants canadiens[2]. La volatilité a influencé les préférences en matière de financement, ralenti les investissements des entreprises et l'embauche, et incité les banques à modérer la croissance des prêts. Le comité d'audit devrait interroger la direction sur les pratiques de planification de scénarios structurés et de prévision des risques, en s'éloignant des réponses réactives, en mettant à l'essai divers scénarios géopolitiques comme les régimes de droits de douane, les goulots d'étranglement de la chaîne d'approvisionnement ou les contrôles des capitaux, et en établissant à l'avance des déclencheurs, des mesures et des personnes responsables.

Le comité d'audit doit s'assurer que la direction évalue les ramifications des événements géopolitiques en cours et à venir et qu'elle cartographie les risques géographiques pour comprendre leurs effets sur les activités, la chaîne d'approvisionnement et les marchés, puis pour les associer au plan d'urgence. La direction pourrait par exemple tester périodiquement des scénarios fondés sur les données et l'analytique, portant sur des cas d'utilisation clairs et reposant sur des paramètres bien définis, pour rédiger des manuels d'instructions qui soient basés sur des signes avant-coureurs plutôt que sur des schémas historiques. À ce titre, les organisations doivent disposer d'un plan d'action bien défini en matière de risques géopolitiques, lié à des déclencheurs de scénarios et assorti des

Questions que les comités d'audit devraient poser :

- L'entreprise soumet-elle sa stratégie à long terme et ses modèles d'affectation des capitaux à des tests de résistance contre divers chocs géopolitiques éventuels, comme la dissociation ou les conflits régionaux?
- Est-ce que la direction identifie et gère convenablement les risques de deuxième et de troisième ordre découlant des événements et des nouveautés?
- L'entreprise a-t-elle une visibilité en temps réel sur la concentration du risque parmi ses principaux fournisseurs de technologie, surtout si leurs services sont liés à l'IA? Quel est le plan en cas de défaillance d'un fournisseur critique?
- La direction comprend-elle l'effet sur les contrôles de l'intégration des nouvelles technologies dans les systèmes et les procédures de l'entreprise?
- Les rapports trimestriels sont-ils suffisants, ou devons-nous procéder plus souvent et en profondeur à des simulations de crise?
- Notre comité d'audit possède-t-il les compétences nécessaires pour apprécier de nouveaux domaines de risque et les méthodologies servant à les évaluer?

[2] KPMG au Canada, « Le leadership face à l'adversité », consulté le 20 octobre 2025.

niveaux de réponse qui peuvent être activés dès l'apparition de signaux, permettant ainsi de prendre des décisions plus rapides à l'échelle de l'organisation, puisqu'elles seraient préapprouvées.

Technologie et climat : intensification du contexte de risque

Les risques ne se limitent pas à la situation géopolitique. Les organisations doivent aussi composer avec des menaces grandissantes sur le plan des technologies et des changements climatiques. Les auteurs de cyberattaques ne leur laissent aucun répit, employant notamment l'IA pour créer de nouvelles tactiques encore plus sophistiquées qu'avant. L'IA perturbe pratiquement toutes les organisations, et ses possibilités nouvelles s'accompagnent inévitablement de nouveaux risques. Le comité d'audit doit comprendre où et comment l'IA est utilisée dans l'organisation, y compris dans les outils en cours de développement et l'IA qui s'installe dans les technologies déjà en usage par la voie des mises à niveau, afin de déceler les dépendances et les risques cachés.

Par ailleurs, les risques climatiques influent de plus en plus sur les états financiers, car les conditions météorologiques extrêmes touchent les activités, la chaîne d'approvisionnement et les assurances. Parmi les décideurs des entreprises canadiennes sondées, 93 % s'attendent à ce que leur entreprise soit exposée à des événements météo extrêmes dans le courant de l'année prochaine[3]. La plupart d'entre eux rapportent aussi que leur entreprise a subi des perturbations au cours de l'année écoulée, allant de l'arrêt des opérations et des pertes de productivité aux ruptures de la chaîne d'approvisionnement, en passant par la hausse des dépenses, les dommages matériels et la diminution des bénéfices[4].

Le comité d'audit devrait discuter avec la direction de la manière dont elle identifie, surveille et atténue les risques auxquels l'entreprise est exposée – et de la question de savoir si ses équipes disposent des capacités nécessaires pour le faire. En plus de surveiller les incidents, l'entreprise aurait intérêt à simuler des scénarios de changements climatiques et de cybersécurité afin de tester sa résilience en cas d'événements météorologiques extrêmes ou de cyberattaques propulsées par l'IA; elle pourrait aussi utiliser l'analytique prédictive pour cerner les vulnérabilités de toute l'organisation. Le comité d'audit devrait également collaborer avec la direction pour s'assurer que des contrôles limitent l'utilisation d'outils d'IA non approuvés sur les appareils de travail et exigent des attestations pour n'utiliser que des solutions autorisées.

Supervision de l'innovation : trouver l'équilibre entre les occasions et les risques

L'adoption de l'IA se généralise – 78 % des chefs de direction canadiens en font une principale priorité d'investissement – et sert essentiellement à améliorer la productivité[5]. Pourtant, l'évaluation des risques se contente souvent d'étudier les modèles d'IA.

Le comité d'audit devrait s'assurer que la direction évalue aussi les risques découlant de l'intégration de l'IA aux processus déjà en place en matière de protection des données, de confidentialité et de droit d'auteur. Les contrôles internes et les mesures de conformité doivent s'adapter pour rendre compte de l'effet de l'IA sur les profils de risque. Le constat est inquiétant : 42 % des employés ignorent si leur entreprise s'est dotée de contrôles à l'égard de l'IA. C'est même un peu plus que l'an dernier[6]. Ces chiffres rappellent la nécessité d'instaurer une gouvernance plus

[3] KPMG au Canada, « Les dirigeants canadiens intensifient leur préparation aux urgences météorologiques », consulté le 4 novembre 2025.
[4] KPMG au Canada, « Le leadership face à l'adversité », consulté le 20 octobre 2025.
[5] KPMG au Canada, « Le leadership face à l'adversité », consulté le 20 octobre 2025.
[6] KPMG au Canada, « Répertoire sur l'adoption de l'IA générative ».

stricte et de sensibiliser les employés à la gestion des risques liés à l'utilisation de l'IA.

Les cybercriminels font de plus en plus appel à l'IA pour attaquer les organisations. Selon une étude réalisée par KPMG, près de 9 dirigeants d'entreprise sur 10 au Canada sont d'avis que les cyberattaques sont la plus grande menace pour leurs plans de croissance des trois prochaines années, et 83 % craignent de ne pas pouvoir résister à une cyberattaque actuelle – et encore moins à une de la prochaine génération[7].

> « Le comité d'audit doit s'intéresser à tout : les algorithmes de l'IA, les ouragans, les différends commerciaux. Pour exercer une véritable surveillance, il doit constamment remettre en question la façon dont l'entreprise anticipe les chocs à venir et ce qu'elle fera pour les absorber et s'y adapter.

Jas Hothi
Associée, Services-conseils en gestion des risques, Services financiers, KPMG au Canada

À mesure que l'innovation s'accélère et que les entreprises adoptent de nouveaux produits et modèles d'affaires, le comité d'audit devra superviser les moyens mis en œuvre pour évaluer les effets immédiats et les contrecoups des nouvelles technologies. La hausse de l'emploi d'actifs numériques comme les cryptomonnaies stables, par exemple, peut avoir une incidence sur l'entreprise en raison de la volatilité du marché et des coûts de financement. Le coût du capital étant en hausse, le comité d'audit devrait jeter un regard critique sur la compréhension par la direction des risques associés à l'adoption des technologies émergentes et à leurs répercussions potentielles sur la résilience et la santé financière de l'entreprise. Étant donné l'intensification des cyberattaques utilisant l'IA, le comité devrait aussi encourager la surveillance prédictive des menaces et les exercices théoriques simulant des attaques de prochaine génération pour valider les capacités de détection, de réponse et de reprise après sinistre.

Des capacités organisationnelles renforcées pour une gestion efficace des risques

La gestion des risques actuels et de leurs interrelations exige de solides capacités pour les trois lignes de défense : les gammes de services, la gestion des risques et de la conformité, et l'audit interne. Le comité d'audit doit vérifier auprès de la direction que l'entreprise possède les compétences voulues, que la gestion des risques exploite bien les technologies de pointe, que les employés reçoivent la formation nécessaire pour déceler et gérer les risques émergents et que toutes les fonctions de gestion des risques disposent des ressources nécessaires. Le comité d'audit pourrait devoir perfectionner ses membres ou en recruter qui possèdent une expertise en IA, en cybersécurité, en risques climatiques et en analyse géopolitique. Certes, les compétences financières demeurent essentielles, mais l'évolution des risques demande que les membres du comité aient des compétences plus larges et comprennent par exemple les technologies, les risques qui les accompagnent et les problèmes qu'ils pourraient causer à l'entreprise.

[7] KPMG au Canada, « Le leadership face à l'adversité », consulté le 20 octobre 2025.

Adapter la gouvernance à un environnement de risque dynamique

Pour suivre l'évolution effrénée de l'environnement de risque, il se peut que le comité d'audit doive se réunir plus fréquemment qu'une fois par trimestre. Il partagerait plus souvent l'information et pourrait procéder à des examens approfondis des nouvelles problématiques qui surgissent, ce qui favoriserait la proactivité de l'entreprise. Le suivi en temps réel des indicateurs de résilience (concentration du risque lié aux fournisseurs, capacités de reprise après sinistre des TI, dépendances à l'égard des tiers) est devenu vital. Le comité devrait s'assurer que la direction tient à jour la liste des services essentiels, avec une cote de risque pour chacun, et qu'elle communique sans délai les cas préoccupants.

En adaptant ses propres pratiques, le comité d'audit peut guider l'organisation en période de turbulences. L'entreprise qui ajoute la résilience à son programme de productivité disciplinée fait en sorte que les gains au chapitre de la performance soient durables, transparents et conformes aux objectifs à long terme. Elle ne se contente pas de survivre aux perturbations, elle s'en nourrit.

Nous contacter

Akber Merchant

Associé, Services-conseils en réglementation et en gestion des risques, KPMG au Canada
akbermerchant@kpmg.ca

Jas Hothi

Associée, Services-conseils en gestion des risques, Services financiers, KPMG au Canada
jashothi@kpmg.ca

kpmg.com/ca/audit-fr