

Risques et occasions liés à l'IA au cœur de l'ordre du jour des comités d'audit

Alors que l'IA gagne en importance et se déploie rapidement, les comités d'audit devraient se pencher sur la gestion des risques et la gouvernance.

Tous les comités d'audit doivent réfléchir à l'intelligence artificielle. Aucun ne peut fermer les yeux sur l'innovation accélérée que l'IA représente, son adoption généralisée, ses effets sur la productivité et son omniprésence. D'après notre récent sondage sur les perspectives des chefs de direction, la priorité opérationnelle des entreprises consiste à comprendre et à mettre en œuvre l'IA générative dans toute l'organisation



L'IA a le potentiel considérable d'accroître l'efficience et la productivité des organisations et de maintenir leur compétitivité sur les marchés mondiaux. Il faut que les comités d'audit évaluent soigneusement l'équilibre entre l'atténuation des risques et la possibilité de nuire à la compétitivité de l'organisation.

Stephanie Terrill

Associée directrice canadienne, Transformation numérique et leader nationale, Services-conseils en gestion, KPMG au Canada



afin d'atteindre les objectifs de croissance des trois prochaines années^[1]. Les entreprises adoptent de plus en plus l'IA agentique, celle qui sait exécuter des tâches presque sans intervention humaine : 86 % des dirigeants en font une principale priorité d'investissement pour leur entreprise^[2]. Cela a une incidence sur les processus, les systèmes et les contrôles à l'échelle de l'entreprise, ainsi que la manière de tenir les personnes informées. C'est pourquoi les comités d'audit doivent discuter de l'IA lors de leurs réunions, et ce, que leur mandat englobe la surveillance de toute la gestion des risques de l'entreprise ou qu'il soit plus traditionnel et se concentre sur la fonction finance.

Parmi les employés interrogés, 62 % utilisent des outils accessibles au public et 28 %, des versions fournies par leur entreprise. Et pourtant, 91 % des dirigeants sont inquiets à l'idée que des outils grand public aient accès à des informations sensibles^[3].

¹ KPMG au Canada, « La productivité sous la loupe », consulté le 21 octobre 2025.

² KPMG au Canada, « Les entreprises du Canada recourent à l'IA agentique », consulté le 7 novembre 2025.

³ KPMG au Canada, « Répertoire sur l'adoption de l'IA générative ».

Les comités d'audit doivent comprendre où et comment l'IA est utilisée

Les comités d'audit doivent s'affairer à comprendre quelles parties du processus d'information financière sont touchées par l'IA et quels sont les risques associés à son utilisation. Selon leur mandat, certains comités pourraient même devoir s'informer de l'utilisation de l'IA dans toute l'organisation. Peu importe le rayon d'influence du comité, son inventaire doit tenir compte de l'utilisation de l'IA dans les applications en cours de développement et de l'IA qui s'installe dans les technologies déjà en usage par la voie des mises à niveau.

Les entreprises devraient aussi s'assurer que les membres du personnel ne se servent pas d'outils fondés sur l'IA non autorisés, car ces derniers ne conviennent pas nécessairement à l'organisation ou aux tâches qui leur sont confiées et risquent de produire des résultats erronés, d'accroître les risques liés à la cybersécurité, de compromettre la sécurité et la confidentialité des données et de nuire aux avantages concurrentiels.

Les entreprises ont tout intérêt à renforcer la gouvernance de leurs TI en encourageant leurs employés à utiliser des outils autorisés et adaptés à leurs rôles et responsabilités. Dans le cadre d'une stratégie plus vaste de gestion des risques, certaines entreprises explorent des mesures, comme des attestations décernées à leurs employés et des contrôles techniques, pour s'assurer que seules des solutions d'IA approuvées et conformes soient accessibles sur les appareils fournis au travail. Ce type de mesures pourrait contribuer à l'instauration d'un environnement bien géré et sécurisé pour l'adoption de l'IA et appuierait en même temps les objectifs organisationnels et les exigences de conformité.

Questions que les comités d'audit devraient poser :

Où l'IA est-elle utilisée au sein de notre organisation actuellement?

Notre organisation a-t-elle une politique en matière d'IA définissant la gouvernance, la sécurité et la confidentialité des données, ainsi que l'initiation et la formation à l'IA?

Les membres du conseil possèdent-ils, en numérique ou en IA, les compétences nécessaires pour assurer une gouvernance efficace?

Quel est notre cadre global pour gouverner l'utilisation de l'IA?

Par quels moyens veillons-nous à la formation du personnel sur les risques et les politiques liés à l'IA et sur son utilisation appropriée?

Comment faisons-nous l'évaluation et le suivi du risque lié aux tiers quand l'entreprise fait appel à de nouveaux fournisseurs, en ce qui concerne l'IA, et à des fournisseurs qui utilisent l'IA?

Quelle est l'incidence de l'IA sur l'auditeur externe, dans l'utilisation que lui et l'entreprise en font?

Pour que ces mesures de gouvernance ne s'arrêtent pas là, il importe aussi que les comités d'audit discutent avec la direction du caractère approprié des outils d'IA dans la pratique et de leur surveillance. Il convient d'interroger la direction sur la manière dont elle s'assure que les outils d'IA sont adaptés à leur usage et que leurs résultats sont appropriés sur le plan comptable et sur le plan éthique. Les outils utilisés pour les ressources humaines, par exemple dans le processus de recrutement, risquent d'être entachés de parti pris; ils doivent donc être surveillés et rectifiés. Comme la plupart des outils sont nouveaux, il faut soumettre les résultats à l'examen et au jugement d'un être humain et corriger les outils qui commettent des erreurs. La direction doit démontrer au comité d'audit que des contrôles stricts ont été mis en place pour gérer les risques découlant de ces outils et des modifications apportées aux systèmes et aux processus par suite de l'intégration de l'IA.

La qualité des données est considérée par 71 % des dirigeants comme le principal facteur de la croissance attribuable à l'IA. Pourtant, près de la moitié (49 %) des employés ont déjà obtenu des résultats erronés ou entachés de parti pris; 58 % sont très, voire extrêmement préoccupés par les hallucinations; c'est même un frein pour 46 % des employés, et 37 % évitent les outils d'IA parce que la vérification des résultats occasionne un surcroît de travail^[4].

Examen de l'incidence de l'IA sur l'auditeur externe

Pour que leur surveillance des risques et des occasions liés à l'IA soit exhaustive, les comités d'audit devraient s'intéresser non seulement aux pratiques internes de l'entreprise, mais

considérer également l'usage que les parties externes, comme les auditeurs, font de l'IA. Le comité d'audit devrait demander à l'auditeur externe comment il utilise et supervise l'IA dans le cadre de sa pratique et dans quelle mesure l'utilisation de l'IA par l'entreprise influe sur son travail – en mettant l'accent sur l'explicabilité des résultats plutôt que de les accepter d'emblée. Le comité peut par exemple explorer l'évaluation des éléments probants réunis par l'IA en demandant à l'auditeur externe de lui expliquer l'objectif du modèle, la provenance des données d'entrée, les hypothèses et les limites, et de lui démontrer la validation des résultats et leur examen par un être humain. Le comité devrait aussi confirmer que l'auditeur forme son personnel sur le principe d'explicabilité, l'utilisation responsable de l'IA et les politiques de l'entreprise pour que les compétences en matière d'IA restent actuelles.

L'IA peut donner de nouvelles dimensions à d'anciens risques

Puisque l'IA a le potentiel d'apporter de nouveaux défis à la cybersécurité, les mesures de protection des données organisationnelles et des renseignements personnels deviennent primordiales. Avec certaines applications de l'IA, par exemple, les données sont stockées et traitées ailleurs qu'à l'emplacement de l'entreprise. Le comité d'audit devrait vérifier que la direction adapte les pratiques en matière de cybersécurité et de confidentialité pour tenir compte de l'IA. La direction devrait savoir où les données sont stockées et, si elles quittent l'emplacement de l'entreprise, elle doit évaluer périodiquement la sécurité du lieu de stockage externe. La direction doit aussi savoir si un fournisseur d'IA externe utilise les données de l'entreprise pour entraîner ou perfectionner ses modèles; le cas échéant,

⁴ KPMG au Canada, « Répertoire sur l'adoption de l'IA générative ».

elle doit connaître les modalités de partage des données ainsi que les mesures de protection mises en place, et vérifier si les pratiques du fournisseur respectent les exigences de l'entreprise quant à la confidentialité, à la sécurité et à la propriété intellectuelle.

De manière générale, s'agissant d'IA, le risque lié aux tiers augmente. De grandes sociétés de technologie intègrent l'IA à leurs produits, de nombreux nouveaux fournisseurs proposent des solutions d'IA et bon nombre de fournisseurs d'autres services utilisent l'IA dans leurs activités. Le comité d'audit devrait interroger la direction pour savoir comment les nouveaux fournisseurs d'IA sont évalués et comment l'IA utilisée dans les activités des tiers est surveillée. Le profil de risque et la position concurrentielle des entreprises sont appelés à évoluer encore à mesure que l'IA se généralise dans l'industrie.

Les organismes de réglementation et la surveillance de l'IA

La plupart des pays et des organismes de réglementation des valeurs mobilières passent en revue la réglementation et les obligations d'information en ce qui concerne l'IA, mais jusqu'à présent, bien peu de règles officielles ont été promulguées. Le *Règlement sur l'intelligence artificielle* de l'Union européenne est entré en vigueur le 1^{er} août 2024. Il interdit certaines utilisations de l'IA et en encadre d'autres, en fonction de leur niveau de risque, en rendant obligatoires certaines pratiques telles que la gestion des risques, la gouvernance des données, la tenue de registres et la documentation, de même que le contrôle humain.

Pour sa part, la Securities and Exchange Commission (« SEC ») n'a pas encore publié de règle définitive sur l'IA, mais elle s'attend à ce que les risques et les événements significatifs soient divulgués comme le prévoient déjà les

cadres d'information actuels. La SEC a d'ailleurs mis en garde les sociétés contre les déclarations trompeuses concernant leur utilisation de l'IA. Au Canada, le gouvernement fédéral a mis en place un code de conduite volontaire pour encadrer les systèmes d'IA générative avancés. Le personnel des Autorités canadiennes en valeurs mobilières (« ACVM ») a pour sa part publié un Avis qui n'impose pas de nouvelles obligations, mais fournit des indications sur l'application à l'IA des lois sur les valeurs mobilières déjà en vigueur. Les comités d'audit devront s'assurer que la direction reste au courant des changements apportés à la réglementation et, le cas échéant, que l'entreprise les respecte.

De son côté, le Conseil canadien sur la reddition de comptes (« CCRC ») est l'auteur d'un rapport sur l'utilisation de l'IA en audit. Le rapport fait le point sur la nécessité d'« équilibrer l'innovation et le risque », tâche ardue et délicate qui attend les conseils d'administration, les comités d'audit et les équipes de direction quand il s'agit de gouvernance de l'IA^[5]. L'IA entraîne avec elle de nombreux risques qu'il faut gérer, mais la crainte de ces risques ne doit pas occulter les possibilités que l'IA fait naître.



L'IA touche maintenant toutes les organisations et doit figurer à l'ordre du jour de tous les comités d'audit. Ils doivent s'intéresser à la gouvernance de l'IA, à la gestion des risques qu'elle représente et à ses effets sur l'information financière.

Bryant Ramdoo

Leader national, Innovation en audit et en certification, KPMG au Canada



⁵ Conseil canadien sur la reddition de comptes, « L'utilisation de l'intelligence artificielle dans l'audit : équilibrer l'innovation et le risque », consulté le 29 octobre 2025

La gouvernance de l'IA commence par un cadre global

Il ne sera pas facile d'adapter la gouvernance à chaque innovation ou application de l'IA, mais un cadre de base bien conçu, comprenant des politiques générales, pourra servir de point de départ pour l'évaluation des risques et leur saine gouvernance. Élaboré dans une visée globale, il se prêtera aisément à des améliorations successives.

La littéracie en IA devrait être au cœur de ce cadre global; or les enquêtes démontrent que les entreprises canadiennes ont encore des progrès à faire à ce chapitre. D'après une étude de KPMG International et de l'Université de Melbourne, intitulée *Trust, attitudes and use of artificial intelligence: A global study 2025*, le Canada se classe au 44^e rang sur 47 pays en matière de littéracie en IA. Seuls 24 % des répondants canadiens disent avoir reçu une formation sur l'IA, et moins de la moitié (47 %) croient pouvoir utiliser efficacement les outils d'IA^[6].

Les employés sont 83 % à souhaiter se perfectionner, et 82 % à réclamer de la formation à leur employeur. Ils sont seulement 48 % environ à estimer qu'ils reçoivent une formation suffisante^[7].

La formation en IA : une nécessité

La formation en IA doit dépasser les simples instructions sur l'utilisation d'un outil donné; elle doit être adaptée aux différentes fonctions et aux multiples profils de risque de l'organisation. Toute formation devrait comprendre un volet sur les risques que l'IA représente et les politiques de l'entreprise quant à son utilisation efficace et acceptable, de même qu'une analyse de la contribution possible de l'IA aux grands objectifs de l'entreprise. La formation devrait aussi être adaptée sur mesure aux besoins des différents services de l'entreprise, chacun ayant accès à des types de données qui lui sont propres. Les mêmes outils seront en effet utilisés différemment; pour être optimal, leur usage devra être encadré par des procédures et des précautions particulières.

Pour superviser l'IA correctement au sein de l'entreprise, le comité d'audit devrait interroger les membres de la direction sur les moyens mis en œuvre pour se former eux-mêmes et former les employés, ainsi que sur le suivi des résultats. Il doit aussi pouvoir évaluer le niveau de connaissances de ses membres, déterminer si une formation supplémentaire est nécessaire et même envisager de recourir au recrutement pour augmenter le niveau de littéracie en IA.

L'IA est partout et exige notre attention; mais il faut d'abord la comprendre.

⁶ KPMG au Canada, « Confiance et formation en matière d'IA : le Canada à la traîne », consulté le 7 novembre 2025.

⁷ KPMG au Canada, « Répertoire sur l'adoption de l'IA générative ».

Nous contacter

Stephanie Terrill

Associée directrice canadienne,
Transformation numérique et
leader nationale, Services-conseils
en gestion, KPMG au Canada
sterrill@kpmg.ca

Bryant Ramdoo

Leader national,
Innovation en audit
et en certification
KPMG au Canada
bramadoo@kpmg.ca



kpmg.com/ca/audit-fr