

Directive sur l'audit interne en matière d'intelligence artificielle (IA)

Prise en vertu de la Politique sur l'audit interne

La présente directive appuie les objectifs de la Politique sur l'audit interne en établissant des exigences obligatoires applicables aux missions d'assurance et de conseil de l'audit interne portant sur la gouvernance, la gestion des risques et les contrôles internes liés à l'intelligence artificielle utilisée par les ministères. Elle complète la directive sur l'audit interne et doit être lue conjointement avec celle-ci, qu'elle ne remplace pas.

La présente directive doit être lue conjointement avec la Politique sur l'audit interne, la Directive sur l'audit interne, la Directive sur la prise de décisions automatisée, la Politique sur les services et le numérique, ainsi que la législation applicable en matière de protection de la vie privée, de sécurité, de gestion de l'information, d'approvisionnement et d'accessibilité.

Les missions d'audit interne menées en vertu de la présente directive, qu'elles soient d'assurance ou de conseil, doivent être réalisées conformément au Cadre international des pratiques professionnelles (IPPF), y compris les Normes mondiales d'audit interne, publiées par l'Institut des auditeurs internes. En cas de conflit entre une disposition des présentes normes professionnelles et la Politique sur l'audit interne, la Directive sur l'audit interne ou la présente directive, la politique ou la directive applicable prévaudra.

1. Date d'entrée en vigueur

1.1 La présente directive entre en vigueur le [date].

2. Autorités

2.1 La présente directive est prise en vertu des mêmes pouvoirs que ceux indiqués à l'article 2 de la Politique sur l'audit interne.

2.2 La présente directive est prise en vertu de la Directive sur l'audit interne et énonce des exigences supplémentaires applicables aux activités d'audit interne portant sur l'intelligence artificielle.

3 Définitions

3.1 Aux fins de la présente directive, on entend par « système d'intelligence artificielle » tout système, outil ou service qui utilise l'intelligence artificielle pour accomplir des tâches qui, autrement, exigeraient l'intelligence humaine, notamment :

- a. l'intelligence artificielle générative, définie comme un type d'IA capable de créer des contenus nouveaux et originaux, notamment du texte, du code, des images, des vidéos et du contenu audio;

- b. les modèles d'apprentissage automatique, c'est-à-dire des algorithmes et des modèles statistiques capables d'apprendre et de s'adapter sans être explicitement programmés;
- c. les grands modèles de langage, définis comme un type d'IA générative entraînée sur de vastes quantités de données et comportant de nombreux paramètres, qui génère de nouvelles réponses textuelles;
- d. outils d'analyse prédictive;
- e. l'intelligence artificielle intégrée à des logiciels commerciaux, prêts à l'emploi ou fournis par un fournisseur; et
- f. des solutions d'intelligence artificielle agentique capables d'agir de manière autonome ou semi-autonome.

3.2 Il est entendu que la présente directive s'applique aux systèmes d'intelligence artificielle décrits à l'article 3.1, qu'ils soient développés à l'interne, acquis dans le commerce, intégrés à d'autres logiciels, hébergés dans le nuage ou fournis en tant que service par un tiers, de sorte que les ministères ne l'interprètent pas de manière restrictive en excluant les plateformes dotées de fonctions d'IA.

3.3 Dans la présente directive, on entend par « mission d'assurance » une mission d'audit interne dans le cadre de laquelle les auditeurs internes fournissent une évaluation indépendante et objective de la gouvernance, de la gestion des risques ou des contrôles internes liés à l'intelligence artificielle, et dont les conclusions sont communiquées à la direction, à l'administrateur général et au comité ministériel d'audit.

3.4 Dans la présente directive, on entend par « mission de conseil » une mission d'audit interne dans le cadre de laquelle les auditeurs internes fournissent des conseils, des points de vue ou des services de facilitation concernant la gouvernance, la gestion des risques ou les contrôles internes liés à l'intelligence artificielle. La nature et la portée de la mission sont convenues avec la direction, et les auditeurs internes ne fournissent aucune assurance ni n'assument de responsabilités de gestion.

4 Objectifs et résultats attendus

4.1 Objectifs

Les objectifs de la présente directive sont les suivants :

- a. étendre les exigences en matière d'audit interne prévues par la directive sur l'audit interne à la gouvernance, à la gestion des risques et au contrôle de l'intelligence artificielle;
- b. aider les administrateurs généraux à obtenir une assurance indépendante et des conseils objectifs concernant la gestion des risques liés à l'intelligence artificielle;
- c. Promouvoir une utilisation responsable et sécuritaire de l'intelligence artificielle dans l'ensemble de l'administration publique, en s'appuyant sur des mesures appropriées de transparence, de surveillance et de reddition de comptes; et

- d. permettre à l'audit interne de contribuer, dès les premières étapes et en temps opportun, à la conception et à la mise en œuvre d'une gouvernance, d'une gestion des risques et de contrôles efficaces en matière d'intelligence artificielle, tout en préservant son indépendance et son objectivité.

4.2 Résultats attendus

Les résultats attendus énoncés à la section 3 de la Politique sur l'audit interne s'appliquent à la présente directive, notamment la fourniture d'une assurance indépendante et fondée sur les risques concernant la gouvernance, la gestion des risques et les contrôles internes liés à l'utilisation de l'intelligence artificielle par les ministères et, le cas échéant, la formulation de conseils objectifs visant à renforcer ces mécanismes avant et après le déploiement des systèmes d'intelligence artificielle.

5 Exigences

5.1 Directeurs adjoints

Les directeurs adjoints ont pour responsabilité de veiller à ce que :

- a. les risques liés à l'intelligence artificielle sont intégrés dans la gouvernance et la gestion des risques du ministère;
- b. les équipes d'audit interne aient un accès sans restriction aux renseignements nécessaires pour évaluer la gouvernance et les contrôles relatifs à l'intelligence artificielle;
- c. les plans d'action de la direction visant à donner suite aux constatations de l'audit interne concernant l'intelligence artificielle soient mis en œuvre en temps opportun; et
- d. le service d'audit interne est informé dès les premières étapes des initiatives importantes en matière d'intelligence artificielle, notamment en ce qui concerne leur conception, leur acquisition et leur mise en œuvre, afin que le responsable de la vérification puisse déterminer si des missions de conseil ou d'assurance sont justifiées.

5.2 Responsables de l'audit

Outre les exigences prévues à l'article 4 de la Directive sur l'audit interne, les responsables de l'audit interne doivent :

- a. tenir compte des risques liés à l'intelligence artificielle lors de l'élaboration du plan d'audit interne ministériel axé sur les risques, y compris les missions d'assurance et de conseil prévues concernant l'intelligence artificielle;
- b. évaluer périodiquement la gouvernance, la gestion des risques et les contrôles internes du ministère en matière d'intelligence artificielle, conformément à l'annexe A;
- c. Communiquer en temps opportun à la direction générale et au comité ministériel d'audit les constatations d'audit importantes, les risques et les recommandations liés à la gouvernance et à l'utilisation de l'intelligence artificielle;

- d. Surveiller la mise en œuvre des plans d'action de la direction découlant des missions d'audit interne liées à l'intelligence artificielle et, lorsque la direction n'a pas pris de mesures opportunes et appropriées pour remédier aux risques importants identifiés ou donner suite aux recommandations, signaler la situation à la direction générale et au comité ministériel d'audit;
- e. le cas échéant, fournir des services de conseil en matière d'intelligence artificielle, conformément à la section A.7 de l'annexe A, de manière à ne pas compromettre l'indépendance de la fonction d'audit interne ni l'objectivité des auditeurs internes;
- f. veiller à ce que la direction conserve la responsabilité de toutes les décisions découlant des services de conseil, et à ce que l'audit interne ne conçoive, ne mette en œuvre, n'exploite ni n'approuve aucun système d'intelligence artificielle ou contrôle; et
- g. informer le comité ministériel d'audit des services de conseil fournis en matière d'intelligence artificielle, y compris toute intervention antérieure à titre de conseiller concernant un système, un cadre ou un contrôle qui fait par la suite l'objet d'une mission d'assurance, ainsi que des mesures de protection mises en œuvre.

5.3 comités ministériels d'audit

Les comités ministériels d'audit doivent examiner la pertinence de l'assurance fournie concernant les risques importants et les constatations d'audit significatives liées à l'intelligence artificielle, ainsi que le caractère approprié des services de conseil fournis par l'audit interne en matière d'intelligence artificielle, y compris l'équilibre entre la portée des services d'assurance et des services de conseil, ainsi que les mesures de protection mises en place pour préserver l'indépendance et l'objectivité, conformément aux responsabilités qui leur incombent en vertu de la Politique sur l'audit interne.

5.4 Gestion

La direction demeure responsable de la gouvernance, de la gestion des risques et des contrôles internes liés à l'intelligence artificielle. L'audit interne n'assume pas les responsabilités de la direction à cet égard, que ce soit dans le cadre de missions d'assurance ou de conseil. Lorsque l'audit interne formule des recommandations concernant l'intelligence artificielle, la direction demeure responsable de décider s'il y a lieu de donner suite à ces recommandations et de quelle manière, ainsi que de toutes les décisions relatives à la conception, à l'approbation, au déploiement, à l'exploitation et à la mise hors service des systèmes d'intelligence artificielle.

6 Rôles des autres organismes gouvernementaux

6.1 Les rôles et responsabilités des autres organismes gouvernementaux en matière de gouvernance, de surveillance, de sécurité, de protection des renseignements personnels et d'utilisation de l'intelligence artificielle continuent de s'appliquer conformément à leurs mandats respectifs. Aucune disposition de la présente directive ne modifie ces responsabilités ni ne transfère la responsabilité de la gestion de l'intelligence artificielle au

responsable de l'audit ou à la fonction d'audit interne, y compris lorsque l'audit interne a fourni des conseils concernant l'intelligence artificielle.

7 Champ d'application

7.1 La présente directive s'applique aux organisations décrites à la section 6 de la Politique sur l'audit interne.

7.2 La présente directive s'applique à tous les systèmes d'intelligence artificielle utilisés par les ministères, tels que définis à la section 3, y compris les systèmes développés à l'interne, acquis sur le marché, hébergés dans le nuage, intégrés et ceux provenant de tiers, tout au long de leur cycle de vie, notamment lors des étapes de planification, de conception et d'acquisition, moments où les services de consultation peuvent s'avérer particulièrement utiles.

8 Références

8.1 Législation

- Loi sur l'administration financière

8.2 Instruments de politique connexes

- Politique sur l'audit interne
- Directive sur l'audit interne
- Directive sur la prise de décisions automatisée
- Politique sur les services et le numérique
- Directive sur les pratiques en matière de protection de la vie privée
- Directive sur la gestion de la sécurité

9. Demandes de renseignements

9.1 Pour toute question relative à l'interprétation de la présente directive, veuillez communiquer avec le service des demandes de renseignements du Secrétariat du Conseil du Trésor du Canada.

9.2 Les membres d'une équipe d'audit interne d'un ministère peuvent communiquer avec le Secteur de l'audit interne pour obtenir des précisions.

Annexe A : Procédures obligatoires pour les missions d’audit interne portant sur l’intelligence artificielle

A.1 Date d'entrée en vigueur

A.1.1 Ces procédures entrent en vigueur à la même date que la présente directive.

A.2 Généralités

A.2.1 Les présentes procédures précisent les exigences énoncées à l'article 5 de la présente directive.

A.2.2 Les missions d’audit interne portant sur l’intelligence artificielle sont menées conformément au Cadre international des pratiques professionnelles, tel que publié par l’Institut des auditeurs internes, et aux procédures obligatoires suivantes.

A.2.3 Les sections A.3 à A.6 s’appliquent aux missions d’assurance et, le cas échéant, aux missions de conseil. La section A.7 énonce les procédures supplémentaires qui s'appliquent aux missions de conseil. Les considérations relatives à la vérification énoncées à la section A.4 peuvent également servir à définir la portée des missions de conseil.

A.3 Planification

A.3.1 Les responsables de l’audit interne devraient veiller à ce que les missions d’audit interne portant sur l’intelligence artificielle soient proportionnées au risque, en tenant compte des éléments suivants :

- a. les répercussions sur les Canadiens;
- b. le caractère significatif sur le plan financier;
- c. le caractère sensible des renseignements en cause;
- d. la sécurité nationale et l’intérêt public;
- e. le degré d’automatisation et la complexité des algorithmes;
- f. le recours à des technologies de tiers; et
- g. les constatations d’audit antérieures ou les incidents liés à l’intelligence artificielle.

A.3.2 Lors de la planification des missions portant sur l’intelligence artificielle, les responsables de l’audit devraient également déterminer si le ministère :

- a. tient à jour un répertoire des systèmes d’intelligence artificielle actuellement utilisés ou en cours de développement;
- b. les systèmes d’intelligence artificielle ont, au sein de l’organisation, un propriétaire désigné ou une personne responsable qui assume la responsabilité ultime des actions et des résultats de ces systèmes;
- c. classe les systèmes d’intelligence artificielle en fonction de leur niveau de risque ou de leur incidence;
- d. a recensé les systèmes d’intelligence artificielle à fort impact nécessitant une surveillance renforcée; et

- e. a réalisé des analyses d'impact, notamment conformément à la Directive sur la prise de décisions automatisée, le cas échéant.

L'absence d'un inventaire ministériel des systèmes d'intelligence artificielle ou d'une classification des risques constitue en soi un facteur pertinent pour la planification de l'audit fondée sur les risques et peut indiquer les situations où une mission de conseil aiderait la direction à établir ces fondements avant la prestation d'une assurance.

A.3.3 Lors de l'élaboration du plan d'audit interne fondé sur les risques, les responsables de l'audit interne devraient déterminer dans quels cas une intervention précoce de l'audit interne, sous forme de missions de conseil, pourrait s'avérer utile, par exemple :

- a. les systèmes d'intelligence artificielle nouveaux ou à fort impact, qu'ils soient en phase de planification, de conception ou d'acquisition;
- b. l'élaboration ou la révision des cadres de gouvernance, des politiques, des inventaires ou des méthodes de classification des risques en matière d'intelligence artificielle au sein des ministères;
- c. l'élaboration de clauses contractuelles spécifiques à l'intelligence artificielle et de processus de vérification préalable des fournisseurs, y compris les ententes d'entreprise en matière d'intelligence artificielle;
- d. l'adoption à l'échelle de l'entreprise d'outils d'intelligence artificielle générative; et
- e. l'évaluation de la maturité visée à la section A.6.2.

A.4 Considérations relatives à la vérification

Les missions d'audit interne portant sur l'intelligence artificielle devraient prendre en compte, selon le cas, les éléments suivants :

A.4.1 Gouvernance — structures de gouvernance, rôles, responsabilités, obligation de rendre compte et contrôle éthique, notamment si le ministère a désigné un dirigeant responsable de l'intelligence artificielle, mis sur pied un comité de gouvernance de l'intelligence artificielle ou un organisme de surveillance équivalent, attribué clairement la responsabilité des risques liés à l'intelligence artificielle et des modèles ou systèmes individuels, et tient un inventaire officiel des systèmes d'intelligence artificielle;

A.4.2 Gestion des risques — identification, évaluation, atténuation et surveillance des risques, notamment en matière de protection de la vie privée, de cybersécurité, de partialité, de discrimination, d'explicabilité, de dérive des modèles, de conformité à la loi et de résilience opérationnelle. Les considérations en matière de cybersécurité devraient comprendre les menaces propres à l'intelligence artificielle, notamment les attaques par injection d'invites, l'empoisonnement de modèles, les attaques par exemples contradictoires, la sécurité des interfaces de programmation d'applications, le vol de modèles, la résilience des services d'intelligence artificielle et la surveillance des utilisations abusives des systèmes d'intelligence artificielle;

A.4.3 Contrôles internes — contrôles relatifs à la qualité des données, à l'élaboration et à la validation des modèles, à la gestion des accès et des modifications, au suivi, à la

gestion des incidents, à la documentation et à la tenue des dossiers, y compris les contrôles liés au cycle de vie des modèles, tels que les processus d’approbation des modèles, la validation indépendante, la revalidation périodique, la gestion des changements liés aux mises à jour des modèles, la gestion des données d’entraînement, ainsi que les procédures de retrait et de mise hors service, en reconnaissant que de nombreuses défaillances de l’intelligence artificielle surviennent après le déploiement en raison de la dérive des modèles et de changements non gérés;

A.4.4 Surveillance humaine — examen humain approprié des décisions importantes, maintien de l’obligation de rendre compte des agents publics et procédures de recours hiérarchique;

A.4.5 Gestion de l’information — collecte licite, exactitude, protection, conservation et élimination des renseignements utilisés par les systèmes d’intelligence artificielle, y compris la traçabilité des données d’apprentissage, les contrôles de qualité des données, la détection des biais dans les données d’apprentissage, la provenance des données, le consentement et la fondement juridique pour l’utilisation des données, ainsi que les contrôles relatifs aux transferts transfrontaliers de données;

A.4.6 Approvisionnement — respect des exigences en matière d’approvisionnement, adéquation des contrôles contractuels, droits d’audit et gestion des risques liés aux fournisseurs, lorsque des services d’intelligence artificielle sont obtenus auprès de tiers, y compris la prise en compte de l’emplacement d’hébergement des modèles et de la souveraineté des données, la transparence des sous-traitants, les droits des fournisseurs de mettre à jour ou de réentraîner les modèles sans l’approbation du client, la propriété des invites, des résultats et des données d’entraînement, les protections contractuelles propres à l’intelligence artificielle, ainsi que les engagements des fournisseurs en matière d’explicabilité; et

A.4.7 Contrôles relatifs à l’intelligence artificielle générative — contrôles propres aux outils d’intelligence artificielle générative, notamment les contrôles relatifs à la gestion des invites, la protection des renseignements sensibles saisis dans ces outils, la validation des résultats générés par l’intelligence artificielle, les risques de violation de la propriété intellectuelle, la gestion du risque d’« hallucinations », les exigences en matière de validation par une personne des résultats utilisés dans la prise de décision, la surveillance de l’utilisation des résultats de l’intelligence artificielle, ainsi que la formation des utilisateurs et les exigences relatives à l’utilisation acceptable.

A.5 Rapports

A.5.1 Les rapports de mission d’assurance de l’audit interne portant sur l’intelligence artificielle doivent être finalisés conformément à l’article 4 de la Directive sur l’audit interne et doivent inclure, le cas échéant, des observations relatives à la gouvernance, les risques importants, les lacunes de contrôle, les causes profondes, les recommandations, les réponses de la direction et les échéanciers de mise en œuvre.

A.5.2 Les questions importantes doivent être portées sans délai à l'attention de la direction générale et du comité d'audit du ministère, y compris celles qui sont relevées dans le cadre d'une mission de conseil, qu'elles relèvent ou non du champ d'application convenu de la mission.

A.5.3 Les résultats des missions de conseil relatives à l'intelligence artificielle doivent être communiqués sous la forme convenue avec la direction conformément à la section A.7.2 et ne doivent pas nécessairement comporter une conclusion d'assurance ou une note d'évaluation.

A.6 Suivi

A.6.1 Les responsables de l'audit devraient surveiller la mise en œuvre des plans d'action de la direction découlant des missions d'audit interne portant sur l'intelligence artificielle.

A.6.2 Étant donné que les risques liés à l'intelligence artificielle évoluent constamment et ne peuvent être gérés uniquement au moyen d'audits périodiques, les ministères devraient évaluer régulièrement le niveau de maturité de la gouvernance et des contrôles internes qui sous-tendent l'intelligence artificielle, et devraient envisager un suivi continu du rendement, des biais et de la précision des modèles, ainsi que la détection des dérives et l'analyse des tendances en matière d'incidents. Les responsables de l'audit peuvent apporter leur soutien à cette évaluation de la maturité à titre consultatif, par exemple en proposant une méthodologie ou en facilitant la réalisation d'une auto-évaluation, à condition que la direction conserve la responsabilité de l'évaluation et de ses résultats.

A.6.3 L'évaluation de la maturité mentionnée au paragraphe A.6.2 devrait porter, au minimum, sur les domaines suivants :

Domaine	Exemples de critères
Gouvernance	Rôles, surveillance par les comités, reddition de comptes
Gestion des risques	Évaluations des risques liés à l'IA, évaluations d'impact
Contrôles	Contrôles techniques et opérationnels
Gestion des données	Qualité des données, traçabilité, protection de la vie privée
Risques liés aux tiers	Surveillance des fournisseurs
Gestion des risques liés aux modèles	Validation, surveillance de la dérive
Vérification et assurance	Services d'assurance et de conseil, mesures de protection de l'indépendance et rapports

Ce cadre d'évaluation de la maturité offre aux ministères une démarche d'amélioration reproductible dans les domaines suivants : gouvernance, gestion des risques, contrôles,

gestion des données, risques liés aux tiers, gestion des risques liés aux modèles, ainsi qu'audit et assurance.

A.7 Missions de conseil

A.7.1 Nature et portée. Les responsables de l'audit peuvent offrir des services de conseil en matière d'intelligence artificielle, notamment :

- a. des conseils sur la conception de cadres de gouvernance en matière d'intelligence artificielle, notamment en ce qui concerne les mandats des organismes de surveillance, les responsabilités et la propriété des systèmes et des modèles;
- b. les examens de conception ou de pré-mise en œuvre des contrôles relatifs aux systèmes d'intelligence artificielle, y compris les contrôles liés au cycle de vie des modèles décrits à la section A.4.3;
- c. des conseils sur les méthodes d'évaluation des risques et des répercussions, y compris les évaluations d'impact algorithmiques prévues par la Directive sur la prise de décisions automatisée;
- d. des conseils sur les mesures de protection contractuelles propres à l'intelligence artificielle, les droits d'audit et la vérification préalable des fournisseurs, tels que décrits à la section A.4.6;
- e. la facilitation des autoévaluations des risques et des contrôles, y compris l'évaluation de la maturité mentionnée à la section A.6.2;
- f. la formation et la sensibilisation de la direction et du personnel aux risques liés à l'intelligence artificielle et aux mesures de contrôle; et
- g. la participation, à titre consultatif et sans droit de vote, à des comités de gouvernance en matière d'intelligence artificielle ou à des organismes de surveillance équivalents.

A.7.2 Entente avec la direction. Avant le début d'une mission de conseil, le chef de l'audit et le gestionnaire responsable doivent s'entendre par écrit sur les objectifs, la portée, les responsabilités respectives, les livrables, les échéanciers et la manière dont les résultats seront communiqués.

A.7.3 Mesures visant à garantir l'indépendance et l'objectivité. Lorsqu'ils fournissent des services de conseil en matière d'intelligence artificielle, les auditeurs internes ne doivent pas :

- a. concevoir, développer, mettre en œuvre, exploiter ou approuver des systèmes, des modèles ou des contrôles d'intelligence artificielle;
- b. prendre des décisions de gestion ou assumer la responsabilité des risques liés à l'intelligence artificielle;
- c. gérer ou tenir à jour l'inventaire ministériel en matière d'intelligence artificielle, la classification des risques ou tout modèle;
- d. exercer, pour le compte de la direction, la fonction de validation indépendante des modèles visée à la section A.4.3; ou

e. siéger à titre de membre votant au sein d'un comité de gouvernance en matière d'intelligence artificielle ou d'un organisme de surveillance équivalent.

A.7.4 Missions d'assurance ultérieures. Lorsque l'audit interne a fourni des conseils concernant un système, un cadre ou un contrôle d'intelligence artificielle qui fait par la suite l'objet d'une mission d'assurance, le responsable de l'audit interne doit évaluer si l'objectivité risque d'être compromise, envisager de confier la mission à des auditeurs internes n'ayant pas participé à la mission de conseil, et divulguer cette intervention antérieure dans le rapport de mission ainsi qu'au comité ministériel d'audit.

A.7.5 Équilibre avec la couverture d'assurance. Les responsables de l'audit doivent veiller à ce que les services de conseil en matière d'intelligence artificielle ne se substituent pas à une couverture d'assurance adéquate des risques importants liés à l'intelligence artificielle.

A.7.6 Compétences. Les responsables de l'audit interne doivent s'assurer que les auditeurs internes chargés de missions de conseil en matière d'intelligence artificielle possèdent collectivement les connaissances, les aptitudes et les compétences nécessaires, et qu'ils peuvent, au besoin, faire appel à des experts externes qualifiés, conformément aux Normes mondiales d'audit interne.

A.7.7 Documentation Les missions de conseil portant sur l'intelligence artificielle devraient être documentées, notamment l'entente visée à l'article A.7.2, les travaux réalisés, les conseils fournis et les mesures de protection appliquées en vertu des articles A.7.3 et A.7.4.

Pour toute question concernant cette proposition ou pour obtenir une séance d'information sur la profession de l'audit interne, veuillez communiquer avec Ryan Singh à l'adresse Ryan.Singh@TheIIA.org.