IA générative pour la vérification interne au sein du gouvernement canadien : Des projets pilotes à la preuve

Ce que les responsables des vérifications à l'échelle fédérale, provinciale et municipale peuvent faire maintenant pour tirer profit de l'utilisation de l'IA générative de manière sûre, mesurable et rapide.

Pourquoi le recours à l'IA est différent pour la vérification interne

La vérification interne (VI) dans le secteur public a toujours été motivée par une curiosité disciplinée : découvrir ce qui se passe réellement au sein d'institutions sans but lucratif complexes et aider les responsables à agir en conséquence. L'IA générative est un nouvel instrument utile à cette mission – elle est capable de résumer des quantités considérables de données, de mettre en évidence les anomalies et de rédiger des rapports clairs en quelques minutes. Cependant, elle crée des risques qui touchent les principaux atouts de la vérification : l'indépendance, la qualité des preuves et la reproductibilité. L'IA pose des défis sur le plan de la qualité et de l'accès aux données, nécessite un jugement humain et un esprit critique, présente des problèmes de transparence et d'explicabilité et comporte des risques en matière de partialité et de responsabilité. Bien qu'elle résume les renseignements existants, elle ne les interprète pas et ne formule pas d'opinion ou de conclusion.

Les équipes de vérification interne disposent d'une gamme d'outils d'IA générative, y compris des modèles en ligne gratuits et des versions commerciales payantes, telles que ChatGPT Enterprise, Microsoft Copilot M365 ou Gemini Enterprise, pour n'en nommer que quelques-unes, et chacune offre différents niveaux de fonctionnalité, de sécurité et d'accès à Internet. Les outils gratuits peuvent offrir des fonctions de synthèse et de rédaction de base, tandis que les solutions pour entreprises offrent généralement une meilleure protection des données, des options d'intégration et un accès contrôlé aux sources externes. Il est important de mettre en évidence la source des renseignements

utilisée par chaque outil, ainsi que toute limite en matière de fonctionnalité ou de confidentialité des données. Des distinctions claires entre les types d'outils aident les lecteurs à comprendre les conséquences pratiques et en matière de conformité pour les travaux de vérification du secteur public.

Cet article présente une synthèse des derniers signaux d'adoption par le secteur public et des dernières leçons pratiques tirées des équipes de vérification interne du gouvernement du Canada (GC) ainsi que du récent sondage de KPMG sur l'IA dans le secteur public afin d'offrir aux responsables de la vérification interne un guide pragmatique et tenant compte des risques qui est adapté aux contextes canadiens.

*« Seules **13 %** des organisations du secteur public interrogées déclarent avoir mis en œuvre l'IA; **32 %** font des essais ou mènent des projets pilotes. »*

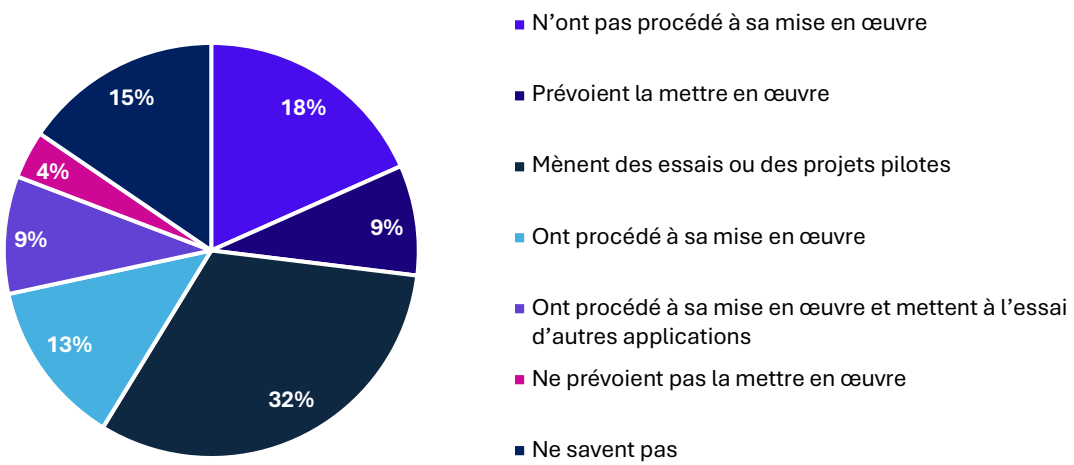
Sondage de 2025 de KPMG sur l'IA dans le secteur public.

Que révèlent les données du sondage de 2025 de KPMG sur l'IA dans le secteur public aux responsables de la vérification interne?

Dans l'ensemble du secteur public du Canada, l'adoption de l'IA se fait prudemment et de manière inégale. Dans un récent sondage mené par KPMG auprès de 349 répondants de tous les échelons de gouvernement au Canada, plus de la moitié (54 %) ont déclaré avoir mis à l'essai ou mis en œuvre des solutions. À l'échelle individuelle, 52 % des répondants n'ont pas utilisé l'IA au travail, tandis que 24 % utilisent des outils publics et 16 % utilisent des plateformes fournies par l'employeur. L'utilisation, lorsqu'elle a lieu, se concentre sur la synthèse de renseignements (64 %) et la rédaction ou la révision de documents (60 %) – l'efficacité reproductible est claire.

Figure 1 – Situation actuelle des organisations par rapport à l'IA

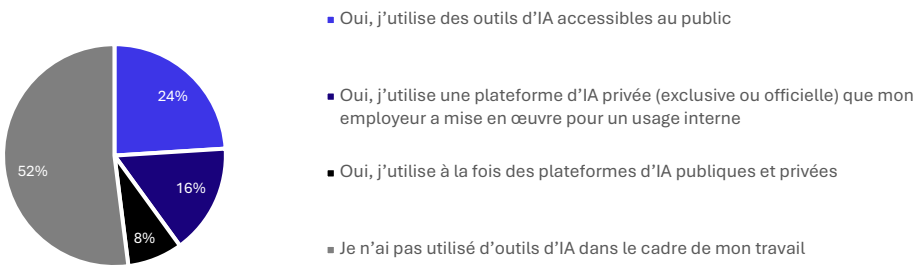
Les projets pilotes dominent; seule une petite minorité a procédé à sa mise en œuvre.



Pourquoi cela est important pour la vérification interne :
La prédominance des projets pilotes et des expériences, avec seulement une petite minorité d'organisations ayant pleinement mis en œuvre l'IA, indique que la plupart des entités du secteur public en sont encore à la phase de mise à l'essai et d'apprentissage. Pour la vérification interne, cela signifie qu'il existe une occasion unique de façonner les cadres de gouvernance, de gestion des risques et de contrôle avant que l'IA ne devienne profondément intégrée. Les vérificateurs peuvent apporter une valeur ajoutée en examinant les contrôles des projets pilotes, en donnant des conseils sur les stratégies d'atténuation des risques et en aidant les organisations à passer de la mise à l'essai à l'adoption durable et évolutive de l'IA. Les entités du secteur public se heurtent à certains obstacles dans la mise en œuvre de l'IA en ce qui concerne, entre autres, la protection des renseignements personnels, la sécurité, les délais d'approvisionnement plus longs et la qualité des données.

Figure 2 – Utilisation individuelle de l'IA au travail

Plus de la moitié des répondants n'ont pas utilisé l'IA au travail, ce qui crée une lacune en matière d'adoption que les responsables de la vérification interne doivent prendre en considération dans les plans de formation.

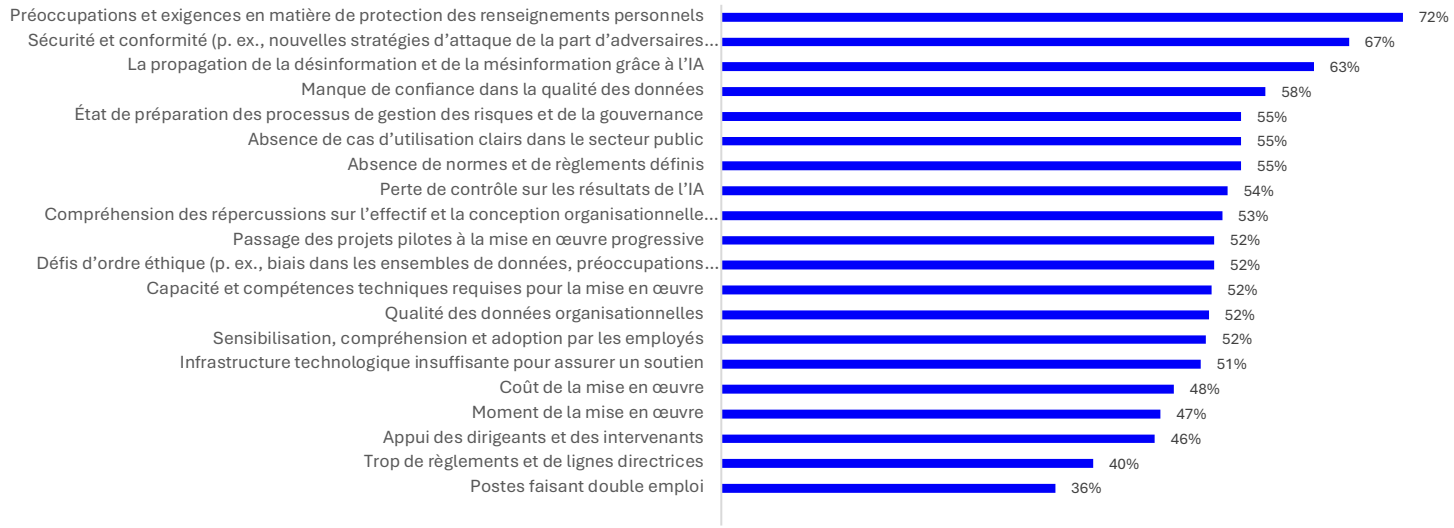


Pourquoi cela est important pour la vérification interne :
Puisque plus de la moitié des répondants n'utilisent pas d'outils d'IA au travail, il y a un écart manifeste en matière d'adoption qui pourrait entraîner une efficacité inégale des processus et une exposition aux risques incohérente dans les ministères. La vérification interne doit évaluer les causes profondes, telles que le manque d'accès, des politiques peu claires ou une formation insuffisante, et recommander des interventions ciblées. Les responsables de la vérification doivent s'assurer que l'adoption de l'IA correspond aux objectifs et à la propension à prendre des risques de l'organisation, tout en surveillant l'IA fantôme[1] et l'utilisation d'outils non autorisés.

[1] L'IA fantôme correspond à l'utilisation d'outils d'intelligence artificielle par les employés sans approbation ou supervision officielle, contournant souvent les contrôles de sécurité et de conformité de l'organisation. Cela peut exposer des données de nature délicate et créer des risques qui sont difficiles à surveiller ou à gérer dans les cadres de gouvernance standard.

Figure 3 – Principaux obstacles à l'adoption de l'IA

Voici les domaines où la vérification interne fournit une assurance qui peut être utilisée pour classer par ordre de priorité les procédures de vérification liées à l'IA.

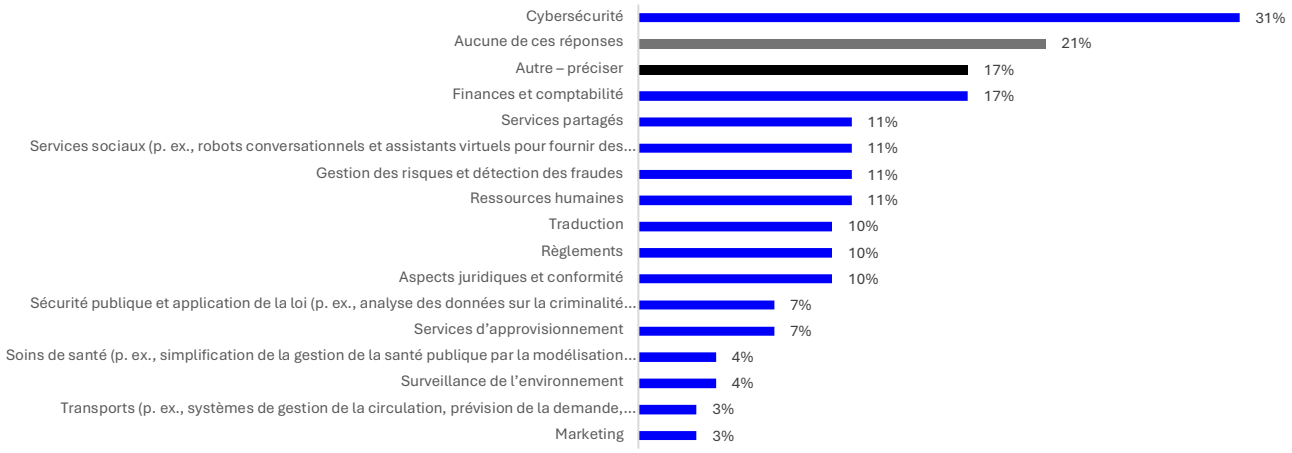


Pourquoi cela est important pour la vérification interne :

Les principaux obstacles sont la protection des renseignements personnels, la sécurité ou la conformité et la mésinformation, qui sont des domaines où la vérification interne fournit une assurance et une supervision. Le manque de confiance dans les données est également important, surtout à la lumière des répondants qui ont indiqué un manque de politiques ou de formation relatives aux données. Les vérificateurs doivent accorder la priorité aux examens des contrôles de protection des renseignements personnels, des mesures de cybersécurité et des cadres de gouvernance des données liés à l'IA. En s'attaquant de manière proactive à ces obstacles, la vérification interne peut aider les organisations à renforcer la confiance dans les systèmes d'IA, à réduire les risques réglementaires et à garantir une utilisation éthique des technologies émergentes.

Figure 4 – Où les organisations prévoient-elles investir dans l'IA (au cours des trois prochaines années)?

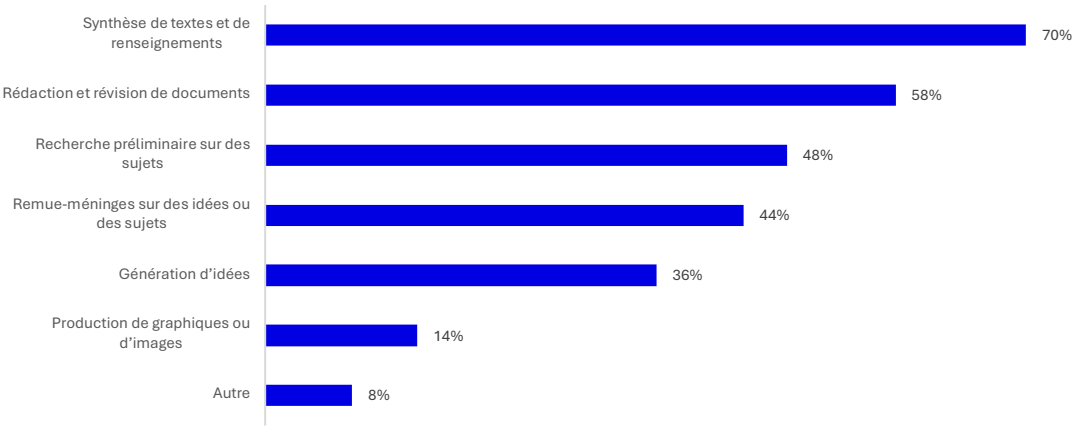
L'investissement cadre avec l'univers de vérification de base (cybersécurité, finances, risques) de la vérification interne, ce qui sert de référence pour les travaux d'assurance ciblés en matière d'IA.



Pourquoi cela est important pour la vérification interne :
Les investissements prévus dans la cybersécurité, les finances, la gestion des risques et les services partagés cadrent étroitement avec l'univers de vérification de base. La vérification interne doit s'attendre à une demande accrue d'assurance par rapport aux processus fondés sur l'IA dans ces domaines, y compris les contrôles en matière de données financières, la détection des fraudes et la gestion des cybermenaces. Les vérificateurs peuvent soutenir la direction en évaluant l'efficacité des investissements dans l'IA, en cernant les lacunes dans les environnements de contrôle et en recommandant des améliorations pour maximiser la valeur et réduire les risques au minimum, tout en utilisant les outils d'IA générative dans leurs travaux de vérification.

Figure 5 – Quel usage les gens font-ils de l'IA aujourd'hui?

L'IA peut répondre aux besoins des utilisateurs de la vérification interne dès le début du processus, avec la synthèse et la rédaction, puis s'étendre aux éléments de vérification structurés.

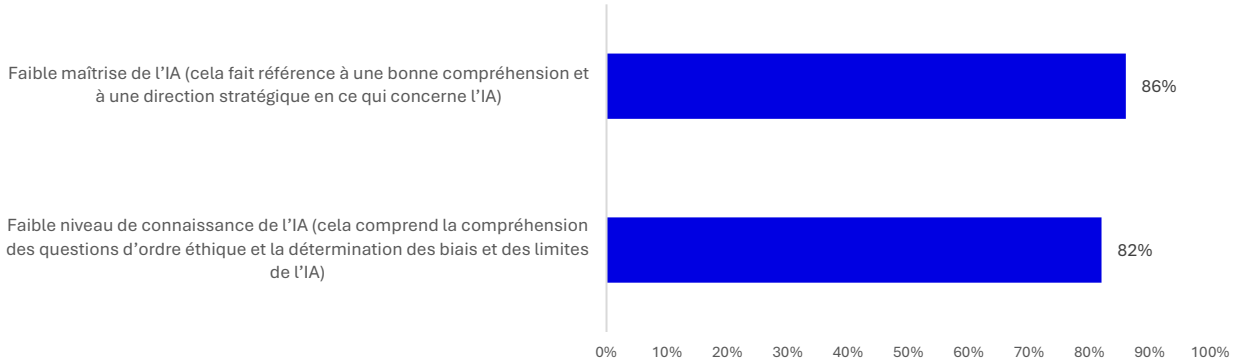


Pourquoi cela est important pour la vérification interne :

Les utilisations les plus courantes de l'IA comprennent la synthèse de renseignements, la rédaction ou la révision de documents et la réalisation de recherches préliminaires axées sur l'efficience et portant sur les processus opérationnels de base. La vérification interne doit évaluer si ces utilisations sont régies par des politiques claires, si les résultats sont fiables et traçables, et si le personnel a la formation requise pour reconnaître les limites de l'IA. Les vérificateurs peuvent également aider les organisations à tirer parti de l'IA pour améliorer les rapports et les analyses, tout en veillant à ce que l'automatisation ne compromette pas l'intégrité des données ou l'exhaustivité des pistes de vérification.

Figure 6 – État de préparation de l'effectif

La grande majorité des répondants considèrent que la connaissance et la maîtrise de l'IA sont faibles chez les employés du secteur public, ce qui met en évidence un besoin critique de formation et de supervision ciblées.

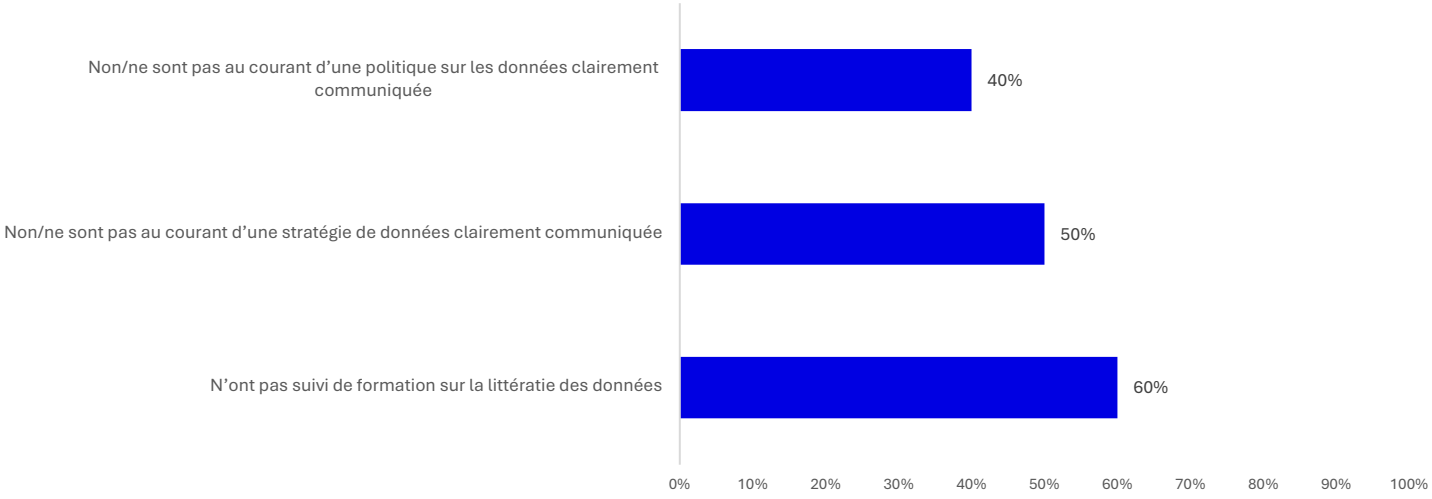


Pourquoi cela est important pour la vérification interne :

Un faible niveau de connaissance et de maîtrise augmente les risques d'utilisation non appropriée, de supervision insuffisante et d'adoption inégale. La vérification interne doit planifier les points de référence de l'état de préparation, accorder la priorité aux contrôles de formation (p. ex., des programmes de formation adaptés aux rôles avec des mesures de protection éthiques) et intégrer des examens des préjugés et des limites dans les vérifications des processus fondés sur l'IA.

Figure 7 – Lacunes importantes dans les fondements relatifs aux données

Une grande partie des répondants ne disposent pas des principales politiques, stratégies et formations en matière de données, ou n'ont pas connaissance de celles-ci, ce qui représente un risque important pour la gouvernance de l'IA et l'assurance de la vérification.



Pourquoi cela est important pour la vérification interne :

Des fondements relatifs aux données faibles amplifient les risques liés aux modèles (mauvaise traçabilité des données, consentement, sécurité) et entraînent des résultats incohérents. La vérification interne doit évaluer l'existence et la communication de politiques ou de stratégies en matière de données, mesurer la connaissance des rôles et vérifier la portée et l'efficacité de la formation, ce qui en fait des éléments essentiels de l'univers de risque annuel.

Leçons tirées des équipes d'évaluation du GC dont la vérification interne peut tirer parti

Des groupes d'évaluation à l'échelle du GC mettent déjà à l'essai l'IA générative dans des flux de travail réels. Plus particulièrement, **Services partagés Canada (SPC)** a utilisé **CANChat** (une version d'entreprise de ChatGPT) tout au long du cycle de vie d'une évaluation (planification, collecte de données, analyse et production de rapports), tandis que les projets antérieurs de SPC ont utilisé l'IA générative dans les phases de production de rapports et de publication. Les évaluateurs font état de son utilité pour **rédiger des guides d'entrevue**, **résumer des transcriptions**, **extraire des thèmes ou des codes** et **améliorer la clarté** des rapports, activités qui sont étroitement liées à la vérification interne.

Ces exercices ont permis de dégager deux conclusions opérationnelles :

- **Des invites disciplinées sont importantes.** De petites modifications à la formulation réduisent les hallucinations. Par exemple, le fait de demander aux modèles de « privilégier l'exactitude et l'exhaustivité plutôt que la concision » peut améliorer considérablement les résultats.
- **Les économies de temps ne sont pas automatiques au niveau de la mobilisation.** L'IA générative peut accélérer les tâches, mais les délais d'évaluation du début à la fin n'ont pas toujours été réduits; la valeur humaine évolue vers la rigueur méthodologique, le jugement contextuel et la justifiabilité, ce qui est une leçon que la vérification interne doit intérioriser. Cette observation concorde avec le récent rapport du Massachusetts Institute of Technology (MIT) sur l'état de l'IA dans les entreprises, qui a révélé que 95 % des projets pilotes sur l'IA générative réalisés ont eu peu ou pas d'incidence mesurable sur la rentabilité des entreprises; cependant, le principal problème a mis en évidence une « lacune d'apprentissage » pour les organisations, ce qui a mené à une intégration imparfaite des entreprises.

Le milieu de l'évaluation signale également les **limites liées à la sécurité, à la protection des renseignements personnels et à l'éthique** qui s'appliquent grandement à la vérification : les outils approuvés par le gouvernement du Canada pour l'IA générative sont généralement **non classifiés seulement** jusqu'à ce que l'**autorisation d'exploitation** soit obtenue. De nombreux contextes d'évaluation requièrent des environnements **Protégé B**, qui constituent de véritables contraintes auxquelles la vérification interne est confrontée lorsque les vérifications portent sur des données personnelles ou financières de nature délicate. La pratique relative à la protection des renseignements personnels interdit

l'inclusion d'identificateurs personnels dans les invites et met en garde contre **« l'effet de mosaïque »** (repersonnalisation par le regroupement de données anodines).

Les lignes directrices nationales et internationales convergent vers des principes (axés sur la personne, responsables, sécurisés, transparents) et sur le cadre **PRETES** (pertinente, responsable, équitable, transparente, éclairée, sécurisée) du gouvernement du Canada. La vérification interne peut les adapter en tant que **points d'ancrage stratégiques** pour les outils, les normes relatives aux documents de travail et les plans de formation.

Par où la vérification interne doit commencer : cas d'utilisation de grande valeur et à faible risque

1. **Planification et établissement de la portée**
    - **Analyses** rapides **de la conjoncture** et **synthèse des documents** (présentations au Conseil du Trésor, politiques, vérifications antérieures) pour formuler des champs d'enquête tout en conservant toujours les résultats dans le dossier de vérification.
    - **Catalogues des contrôles préliminaires** et des **matrices de risque ou de contrôle** issus de **cadres publics, puis adaptés par les vérificateurs**.
2. **Travail sur le terrain et manipulation des preuves**
    - **Rédaction d'un guide d'entrevue** et ensembles de questions **bilingues**; **transcription** et **codage thématique** des notes pour soutenir une synthèse cohérente des données probantes.
    - **Mise en correspondance** assistée **des politiques et des contrôles** et **analyse des lacunes des procédures** dans de grands ensembles de documents que les vérificateurs valident et dont ils déterminent la source.
3. **Production de rapports et suivi**
    - **Synthèse de la première ébauche des constatations ou des constatations préliminaires** (condition, critères, cause, effet, recommandation) dans un modèle normalisé; les modèles permettent d'assurer la clarté et la cohérence, tandis que les vérificateurs continuent d'exercer leur jugement.
    - **Analyse du plan d'action** pour vérifier la faisabilité et la clarté; résumés des leçons apprises des différentes vérifications.

Mesures de protection pour les trois éléments : Utiliser des outils approuvés et hébergés au Canada pour les données non classifiées; ne jamais coller de contenu de nature délicate dans des modèles publics; conserver un journal des invites et des résultats dans le fichier de vérification aux fins de reproductibilité.

Cadre de contrôle de la vérification interne pour l'IA générative (adapté aux gouvernements canadiens)

Pour préserver **la qualité de la vérification tout en favorisant la rapidité, intégrer l'IA générative dans un cadre de contrôle léger, mais explicite :**

1. **Objectif et classification des risques.** Marquer chaque tâche d'IA générative comme suit : **consultation/rédaction**, **analyse assistée** ou **production de preuves**. Interdire l'utilisation de l'IA générative pour les **jugements définitifs** ou les **preuves absolues** sans corroboration par des humains.
2. **Gouvernance des données.** Définir les **catégories de données** qui peuvent être traitées (non classifiées ou Protégé B), les outils approuvés et les lieux de conservation. Inclure des vérifications par rapport à l'**effet de mosaïque**.
3. **Intégrité méthodologique.** Exiger des **dépôts d'invites**, un contrôle des versions et le **caviardage de la décomposition en étapes** dans les produits livrables finaux tout en préservant les éléments de travail pour l'assurance de la qualité. Utiliser les critères de qualité du milieu de l'évaluation (p. ex., **efficacité, équité, confiance, compréhensibilité**) comme points d'acceptation pour les résultats obtenus à l'aide de l'IA générative.
4. **Harmonisation de la sécurité et de l'autorisation d'exploitation.** Seuls les outils dotés d'une **autorisation d'exploitation** ministérielle; **non classifié** par défaut, jusqu'à ce que des environnements protégés soient disponibles. Faire participer le dirigeant principal de l'Information (DPI) ou le dirigeant principal de l'Information et de la Sécurité (DPIS) dès le début pour les vérifications portant sur des données personnelles ou financières.
5. **Supervision humaine.** Définir les **niveaux d'examen** : Attestation du vérificateur principal que le contenu provenant de l'IA générative a fait l'objet d'une vérification des faits; confirmation que les sources sont conservées et traçables.
6. **Mesure.** Suivre la **durée du cycle**, les **pages examinées par heure**, le **ratio entre la version provisoire et la version finale** et les **taux de révision** des tâches assistées

par l'IA générative afin de démontrer le rendement des investissements, ce qui est particulièrement utile lorsque la mesure au niveau de l'entreprise est embryonnaire (**47 %** « ne savent pas » comment ce rendement est mesuré).

Renforcement des capacités : Personnes, outils et modèle opérationnel

Accent sur le perfectionnement des compétences. Les évaluateurs canadiens mettent en évidence cinq groupes de compétences qui s'appliquent bien au domaine de la vérification interne : la connaissance du numérique, l'analyse des données, le codage de base, l'éthique et la confidentialité des données et la collaboration (reliant les domaines techniques et de la vérification). Privilégier la formation pratique par scénarios – p. ex., « Générer une première ébauche des constatations et l'évaluer par rapport à notre norme relative aux preuves. »

Bibliothèque d'invites en tant qu'infrastructure partagée. Établir une **bibliothèque organisée** d'invites pour les tâches de vérification (notes de service en matière de planification, guides d'entrevue, scripts d'évaluation, sections de rapports). Avantages : une intégration plus rapide, des résultats plus cohérents, moins d'erreurs et une mémoire institutionnelle de ce qui fonctionne dans votre environnement.

Réalité relative aux outils. S'attendre à un décalage entre la capacité du modèle public et ce qui est approuvé à l'interne; tenir compte des coûts liés aux licences, à l'infrastructure et à la formation, en notant que l'IA n'est pas gratuite. Élaborer des analyses de rentabilisation qui établissent un lien entre les gains d'efficience (objectif de 49 %) et la portée du plan de vérification et la réduction des risques.

Gestion du changement. Traiter l'adoption de l'IA générative comme un programme de changement : parrainage visible des dirigeants, lignes directrices claires sur ce qui est autorisé et reconnaissance transparente de l'anxiété liée à l'IA – de nombreux employés s'inquiètent de la qualité, de l'équité ou des répercussions sur l'emploi.

Feuille de route pragmatique de 100 jours pour la vérification interne

Jours 0 à 30 : « Renforcer l'échafaudage »

- Approuver un outil d'IA générative dans la politique sur la vérification interne (objectif, tâches autorisées, catégories de données, niveaux d'examen).

- Mettre en place un outil approuvé pour une utilisation non classifiée; créer un modèle de fichier de vérification avec une section pour le journal d'IA générative.
- Lancer une microformation (1 à 2 heures) sur les normes relatives à la protection des invites et aux données probantes. Communiquer les pratiques et les leçons apprises, et créer un environnement où la mise à l'essai est encouragée en toute sécurité.

Jours 31 à 60 : « Prouver la tendance »

- Mener deux microprojets pilotes : l'un sur la planification (tri rapide des documents) et l'autre sur la rédaction de rapports (première ébauche des constatations).
- Mesurer la durée du cycle et les écarts de qualité par rapport aux points de référence; saisir les leçons dans la bibliothèque d'invites.

Jours 61 à 100 : « Établir des mesures de protection »

- Élargir la portée pour inclure le soutien aux entrevues (rédaction de guides, transcription, codage thématique).
- Ajouter des grilles d'évaluation de l'examen par les pairs qui correspondent aux critères de qualité (efficacité, confiance, compréhensibilité).
- Présenter un exposé sur le rendement des investissements au Comité de vérification (mesures d'efficacité, niveau des risques, cas d'utilisation de la prochaine vague en cybersécurité et en finances).

Conclusion : Adopter une solution sécuritaire et mesurée

Les institutions canadiennes font preuve de prudence. L'adoption s'étend au-delà de la mise à l'essai et est axée sur les gains d'efficience, même si la confidentialité, la sécurité et la confiance restent au premier plan. La vérification interne peut montrer l'exemple : choisir des cas d'utilisation pouvant faire l'objet d'une vérification, mettre en place des mesures de protection claires et mesurer les améliorations. Si la vérification interne permet d'assurer un établissement de la portée plus rapide, des constatations plus claires et un meilleur transfert de connaissances sans compromettre l'indépendance ou la qualité des preuves, alors l'IA générative devient non seulement un autre outil, mais un multiplicateur de force pour la valeur.