



La gestion des risques internes au Canada

Résultats du sondage intersectoriel 2025-26 de Deloitte et du
Centre d'excellence canadien pour la gestion des risques internes

À propos de ce rapport

Ce rapport présente en détail les résultats du dernier sondage sur la gestion des risques internes mené par Deloitte Canada et le Centre d'excellence canadien pour la gestion des risques internes (CInRM CoE). Dans le cadre de ce sondage, des données ont été collectées auprès de professionnels canadiens en gestion des risques internes, portant sur leur perception des menaces internes ainsi que sur les mesures de contrôle mises en place au sein de leur organisation.

Les données de ce rapport sont fondées sur une enquête menée entre avril 2025 et juin 2026. Le sondage a été complété par des cadres dirigeants issus des secteurs de la sécurité, de la lutte contre la fraude, de la cybersécurité, des technologies de l'information et des ressources humaines. Les répondants provenaient d'un échantillon représentatif d'industries canadiennes, incluant des filiales de sociétés étrangères, des organisations du secteur public, des organismes sans but lucratif ainsi que d'autres entreprises privées.

Sauf indication contraire, les données numériques se réfèrent aux résultats des réponses à l'enquête. Le sondage de 2026 comprenait un échantillon d'organisations canadiennes considérablement plus vaste et plus diversifié que celui du sondage inaugural de 2025. Bien que les comparaisons directes d'une année à l'autre doivent être interprétées avec prudence, les tendances générales continuent de fournir des indications utiles sur l'évolution des pratiques de gestion des risques liés aux menaces internes au Canada. Par conséquent, les comparaisons d'une année à l'autre sont présentées à titre indicatif et ne doivent pas être interprétées comme des changements statistiquement validés à l'échelle de la population canadienne. Une attention accrue est accordée au classement relatif des capacités, aux thèmes récurrents ainsi qu'aux domaines où les organisations continuent de démontrer des forces ou présentent des opportunités d'amélioration. Les résultats sont anonymisés et seules des réponses agrégées sont présentées.

Merci à tous les participants au sondage pour votre soutien dans cet effort.

Avant propos



Pierre-Luc Pomerleau

Ph.D.
Deloitte Canada
Associé,
Crimes Financiers



Victor Munro

Ph.D.
Canadian Insider Risk
Management Centre
of Excellence
Président-
directeur général

La gestion du risque interne a considérablement évolué au cours de la dernière année. Ce qui était autrefois perçu par de nombreuses organisations comme un enjeu émergent de sécurité est désormais reconnu comme un impératif organisationnel. Le risque interne n'est plus uniquement une question de cybersécurité; il s'agit d'un défi stratégique qui touche les personnes, l'information, les opérations critiques, la réputation et, ultimement, la confiance qui soutient chaque organisation.

Les résultats présentés dans ce deuxième rapport annuel démontrent que les organisations canadiennes continuent de progresser. Un nombre croissant d'entre elles mettent en place des cadres de gouvernance, formalisent leurs politiques, déploient des capacités de surveillance et adoptent une vision plus globale du risque interne. Toutefois, cette progression demeure inégale. De nombreuses organisations s'appuient encore sur des approches réactives, les exposant à des risques de plus en plus détectables, évitables et coûteux lorsqu'ils ne sont pas pris en charge de façon proactive.

Ce rapport paraît à un moment charnière pour le Canada. Les attentes des organismes de réglementation continuent d'évoluer, les principes de *Zero Trust* s'imposent progressivement comme une pratique courante et l'intelligence artificielle (IA) transforme profondément la façon dont les employés accèdent à l'information, la partagent et l'utilisent. Parallèlement, le vol de propriété intellectuelle, la fraude, les inconduites en milieu de travail, le sabotage informatique et les activités d'acteurs étatiques continuent de rappeler une réalité fondamentale : l'accès de confiance demeure l'un des risques les plus complexes à gérer pour les organisations.

La question qui se pose aujourd'hui aux dirigeants n'est plus de savoir si le risque interne mérite leur attention, mais plutôt si leur organisation est prête à le gérer efficacement. Dans un contexte où les investissements sont soumis à un examen accru, les programmes de gestion du risque interne doivent démontrer une valeur tangible : non seulement en prévenant les incidents, mais également en renforçant la gouvernance, en protégeant la réputation, en réduisant les frictions opérationnelles et en permettant une transformation organisationnelle sécuritaire et durable.

Avant propos (suite)

Depuis la publication de notre rapport inaugural, Deloitte Canada et le Centre d'excellence canadien en gestion du risque interne ont eu le privilège de collaborer avec des organisations issues des infrastructures critiques, des services financiers, du gouvernement, et de l'enseignement supérieur afin de les aider à établir et à faire mûrir leurs programmes de risque interne. Ces mandats, combinés à nos recherches continues et à notre collaboration avec des partenaires internationaux, renforcent une leçon importante : bien que la technologie continue d'évoluer rapidement, la gestion réussie du risque interne demeure fondamentalement une question de personnes, de gouvernance et de prise de décision éclairée.

Le rapport de cette année s'appuie sur les fondations établies dans notre publication inaugurale, tout en offrant des données de référence actualisées, des observations pratiques de praticiens et des recommandations concrètes pour les organisations qui souhaitent faire mûrir leurs capacités. Que votre organisation mette en place un programme de risque interne pour la première fois ou perfectionne une capacité existante, nous espérons que ces constats offriront un éclairage précieux sur la situation actuelle du marché canadien, et sur la direction qu'il doit continuer de prendre.

En définitive, la gestion du risque interne ne consiste plus simplement à prévenir le prochain incident. Elle vise à permettre aux organisations d'évoluer avec plus d'assurance, de résilience et de confiance dans un monde de plus en plus interconnecté. Nous espérons que ce rapport continuera de servir à la fois de référence nationale et de guide pratique pour les dirigeants engagés à bâtir des organisations résilientes, capables de gérer les risques et les occasions associés à leur atout le plus précieux : leurs employés.

Pierre-Luc Pomerleau, Ph.D.

Associé, Deloitte Canada

Conseil consultatif de l'industrie, Insider Risk Practitioner Alliance

Victor Munro, Ph.D.

Chef de la direction, Centre d'excellence canadien en gestion du risque interne

Secrétaire général, Insider Risk Practitioner Alliance

Table des matières

Résumé	6-7
Introduction	8
Évolution de la menace interne	9-10
Capacités de gestion de la menace interne	11-14
Comparaison sectorielle	15
Conclusion	16
Contacts clés	17

Résumé

Les résultats du sondage intersectoriel 2025-2026 démontrent que la menace interne demeure un risque important pour les organisations canadiennes, alors que près des **trois quarts des répondants rapportent au moins un incident au cours des 12 derniers mois**. Malgré une légère progression de la sensibilisation et de certaines capacités de détection, la maturité globale des programmes demeure inégale. Les organisations continuent de privilégier des contrôles traditionnels bien établis, comme les vérifications de pré-emploi et la gestion des accès, alors que les capacités plus avancées de gouvernance, de surveillance continue et d'analyse comportementale peinent à se structurer. Les résultats révèlent également des écarts importants entre les secteurs ; le secteur financier affichant la maturité la plus élevée, tandis que les organisations gouvernementales et du secteur de l'énergie font face à des défis distincts en matière de gouvernance, de détection et de priorisation du risque.



Les résultats mettent en évidence un **besoin critique d'accélérer la formalisation des programmes et de renforcer la coordination entre les fonctions** afin d'assurer une gestion proactive et efficace de la menace interne.

01

La menace interne demeure omniprésente et le volume d'incidents augmente

Près de 73 % des organisations ont déclaré au moins un incident de menace interne dans les 12 derniers mois. Les organisations touchées rapportent davantage d'incidents qu'auparavant, indiquant une intensification du risque ou une meilleure capacité de détection¹. La négligence demeure la menace interne la plus fréquemment signalée, tandis que le harcèlement et la violence en milieu de travail constituent la catégorie d'incidents dont la croissance est la plus rapide.

02

La gouvernance de la menace interne demeure le principal point faible

La formalisation des programmes continue de représenter le plus grand défi. La proportion d'organisations disposant d'un groupe de travail dédié est à 51 %, tandis que seulement 5 % déclarent avoir des politiques et cadres robustes en 2026. Ces résultats révèlent un déficit persistant de gouvernance intégrée et de coordination interfonctionnelle.

1. Mise en garde : L'absence ou le faible nombre d'incidents rapportés dans certains secteurs pourrait refléter des capacités de détection ou de signalement limitées, plutôt qu'une exposition moindre au risque de menace interne.

Résumé (suite)

03

Les contrôles traditionnels demeurent les plus matures; toutefois, des améliorations peuvent encore être apportées à l’assurance tout au long du cycle de vie des employés.

Les vérifications d’antécédents pré-emploi restent largement implantées (89 %). Les vérifications continues (57 %) et les procédures formalisées de départ (70 %) signalent une érosion de certains mécanismes clés du cycle de vie des employés.

04

Les capacités de détection avancées demeurent loin d’un état cible optimal

L’adoption des capacités d’analyse comportementale des utilisateurs et des entités (UEBA) progresse, 50 % des organisations ayant atteint au moins un niveau de maturité opérationnel. Toutefois, les capacités de surveillance continue, de formation et de sensibilisation, ainsi que de triage des incidents, demeurent peu matures dans la plupart des organisations.

05

La maturité varie fortement selon les secteurs

Le secteur financier affiche le niveau de maturité le plus élevé (3,67/5), mais demeure également le plus exposé aux incidents de menace interne. Les organisations gouvernementales affichent une maturité plus faible en matière de gouvernance et de formalisation, tandis que les incidents déclarés dans le secteur de l’énergie semblent relativement peu nombreux malgré des risques élevés, notamment en matière de sabotage informatique et d’incidents de harcèlement ou de violence.

Les organisations canadiennes continuent de faire progresser leur gestion des risques liés aux menaces internes, mais la maturité des programmes demeure limitée par une gouvernance insuffisamment structurée, une surveillance continue restreinte et une faible adoption de capacités de prévention avancées.



La maturité face au risque interne doit être considérée dans un contexte de menace en constante évolution. Alors que les menaces internes, les technologies et les modèles d’exploitation continuent d’évoluer, les organisations qui ne réévaluent pas périodiquement leurs risques, ne comparent pas leurs programmes et n’adaptent pas leurs contrôles pourraient voir leur maturité relative décliner au fil du temps, malgré le maintien de leurs capacités existantes. Toute extrapolation entre secteurs d’activité doit être effectuée avec prudence.

Introduction

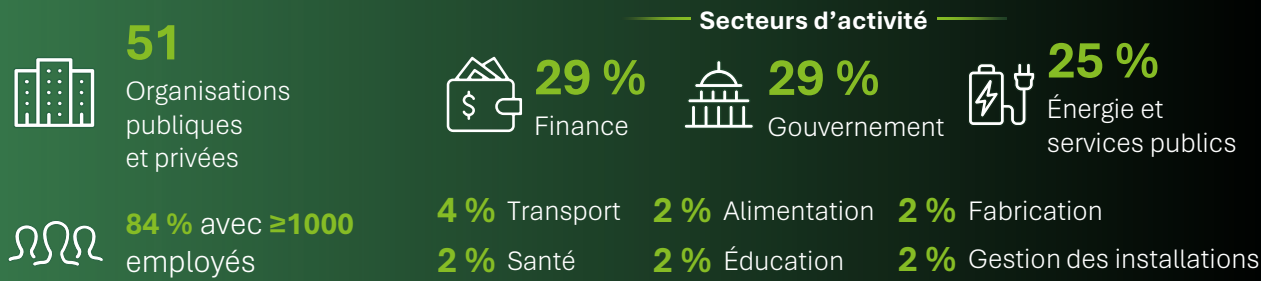
Le paysage des menaces internes au Canada continue d’évoluer rapidement. Dans un contexte marqué par la transformation numérique, le travail hybride et l’expansion des écosystèmes de données, les organisations des secteurs public et privé font face à des risques internes croissants, qu’ils soient malveillants ou non.

L’édition 2026 de l’enquête de Deloitte s’inscrit dans la continuité de l’étude menée en 2025, permettant de mesurer l’évolution des pratiques et de la maturité des organisations canadiennes en matière de gestion des risques internes.

Dotés d’un accès légitime et d’une connaissance approfondie des systèmes, les acteurs de menace interne présentent un profil de risque particulièrement complexe, incitant les organisations à repenser leurs approches en matière de confiance, de surveillance et de responsabilité. Face à des menaces de plus en plus sophistiquées, les organisations doivent poursuivre le développement de programmes de gestion des risques internes plus matures, intégrant une collaboration interfonctionnelle accrue, une sensibilisation organisationnelle renforcée et une capacité d’adaptation continue.

Basée sur une méthodologie alignée sur les travaux antérieurs, cette seconde édition vise à offrir un éclairage comparatif et à identifier les tendances émergentes afin de soutenir les organisations dans le renforcement de leurs capacités.

2026 Portrait des organisations participantes



2025 Comparativement à la 1^{ère} édition du sondage

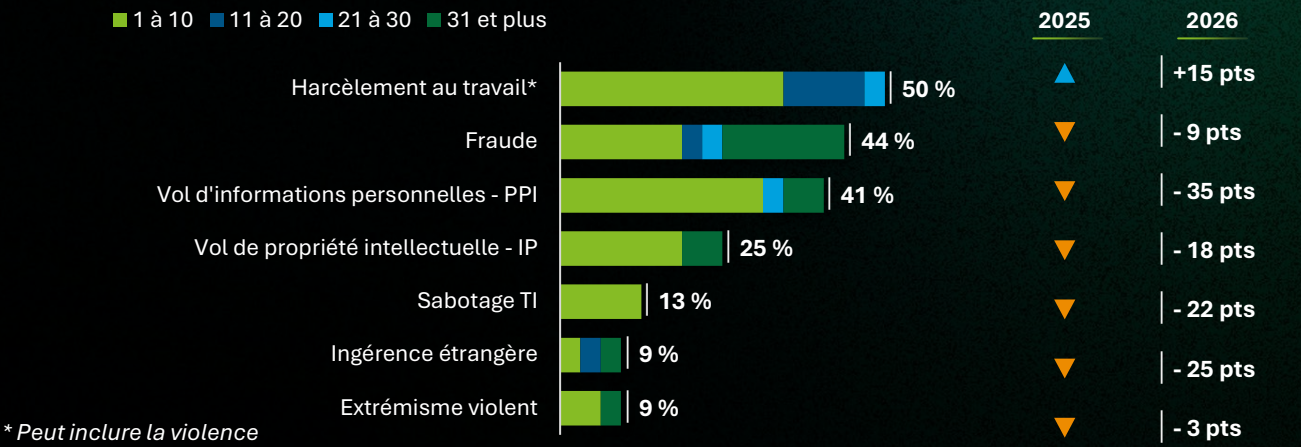


Les résultats mettent en lumière des tendances importantes; toutefois, ils doivent être interprétés avec prudence. L’augmentation de la taille de l’échantillon, l’évolution de la représentation sectorielle et le caractère déclaratif des évaluations de maturité peuvent influencer les résultats observés. Les variations de maturité reflètent donc potentiellement autant la composition de l’échantillon et la perception des répondants qu’une évolution réelle des capacités organisationnelles.

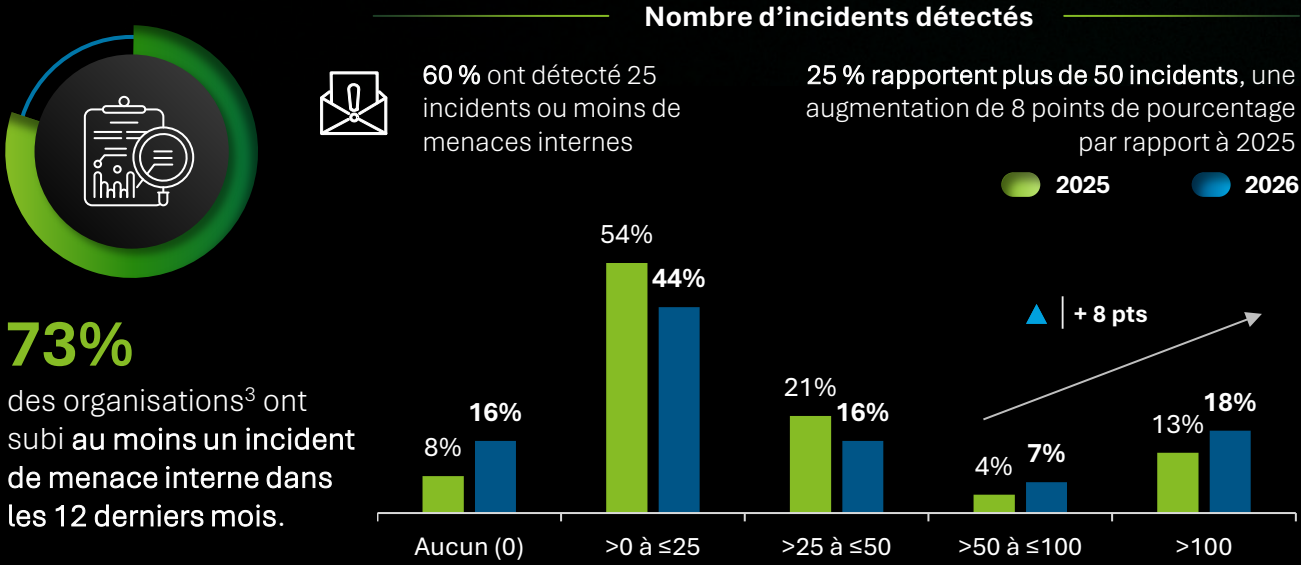
Évolution de la menace interne

Types d'incidents et prévalence

Proportion d'organisations ayant subi ≥ 1 incident



 **Le harcèlement au travail se démarque nettement en 2026.** Ce signal pointe vers un déplacement du profil de risque, alimenté par la composition sectorielle², l'évolution des **pratiques de signalement** ou une **meilleure visibilité** sur les incidents en milieu de travail.



 Près de **trois organisations sur quatre** rapportent **au moins un incident de menace interne**, confirmant l'ampleur persistante du risque.

2. Cette hausse s'inscrit dans une tendance plus large observée au sein des entités gouvernementales canadiennes, où les cas déclarés de harcèlement et de violence en milieu de travail ont progressé de 13 % en 2023, atteignant 2 129 cas dans la fonction publique fédérale. [Daniel Leblanc, CBC News, 2 mars 2026.](#)

3. Note : Les résultats sont fondés sur 51 répondants; 12 % ont refusé de répondre à cette question ou n'ont pas fourni de réponse.

Évolution de la menace interne

Types d'intention et prévalence

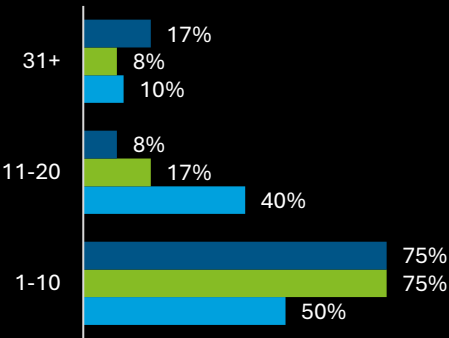
Parmi les organisations qui suivent les incidents de menace interne selon les intentions sous-jacentes



35%

Des organisations, en moyenne, ne suivent pas formellement les incidents de menace interne selon les intentions sous-jacentes.

Répartition du nombre d'incidents détectés par intention sous-jacente



En 2026, les menaces internes demeurent un défi multidimensionnel : la **négligence** reste la source la plus fréquente d'incidents, mais les activités malveillantes sont presque aussi répandues, ce qui souligne la **persistance du risque interne intentionnel**.



Les incidents déclarés demeurent **principalement concentrés dans la tranche de 1 à 10 incidents**, indépendamment de l'intention. Une part appréciable des **incidents accidentels** sont néanmoins rapportés en plus grand volume.

Engagement organisationnel



Compréhension et sensibilisation

2025 2026

3,1/5 3,3/5

▲ +0,2



Priorisation des menaces internes

2025 2026

3,1/5 3,1/5

▲ +0,0



Soutien de la haute direction

2025 2026

3,1/5 3,2/5

▲ +0,1



Les priorités des organisations sont **demeurées relativement stables au cours des deux dernières années**. L'intégration des risques liés aux menaces internes dans les stratégies de gestion des risques et de sécurité **continue d'exiger un fort engagement de la haute direction** ainsi qu'une plus **grande priorisation à l'échelle de l'organisation** afin de générer des progrès durables.

“ Un groupe de travail sur les risques internes est déjà en place et travaille actuellement à l'élaboration d'un cadre de programme ainsi que de protocoles de réponse. **Des efforts se poursuivent afin d'obtenir la mise en place d'un comité directeur de niveau exécutif, bien que l'obtention de l'adhésion et de l'engagement nécessaires demeure difficile.** Le groupe de travail a néanmoins réalisé des progrès importants en favorisant une reconnaissance collective de la valeur d'un programme viable de gestion des risques internes. ”

Répondant de l'industrie de l'Énergie et services publics

Maturité des capacités de gestion de la menace interne

Maturité des capacités par secteur

Capacités	Financier	Gouvernement	Énergie	Autres*
Groupe de travail multifonctionnel	3,50	2,56	2,45	2,80
Cadre et politiques de menace interne	3,63	2,78	2,50	2,75
Vérifications d'antécédent pré-emploi	4,50	4,44	4,27	4,00
Vérifications d'antécédents en continu ou périodique	3,00	3,78	2,70	2,40
Formation et sensibilisation	3,13	2,67	3,30	3,20
Procédure de départ formalisée	3,86	3,33	4,00	3,00
Processus de triage et d'escalade des incidents	3,38	2,78	3,40	3,75
Contrôle des accès physiques	4,13	4,13	4,00	4,80
Contrôle des accès logiques	4,25	4,38	4,64	5,00
UEBA	3,38	2,57	3,44	2,50
Score moyen par secteur	3,67	3,34	3,47	3,42

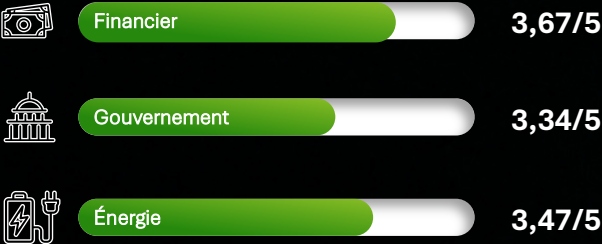
* Les autres industries sont : Transport, Alimentation, Santé, Éducation, Fabrication et Gestion des installations

Légende du continuum de maturité

				
1 = N'existe pas/ Non planifiée	2= Planifiée ou en développement	3= Capacité initiale/ Ad hoc	4= Capacité de base/ amélioration souhaitée	5= Capacité robuste/ état cible

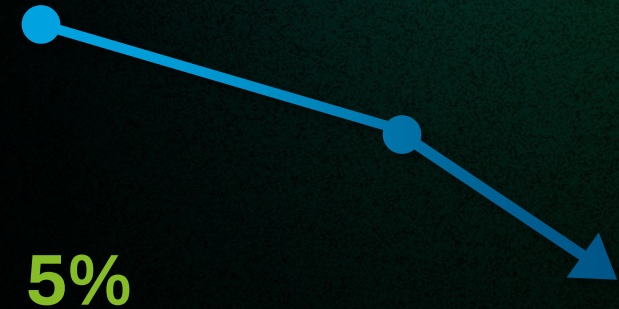
Capacités de gestion de la menace interne

Écarts de maturité sectoriels



Le **secteur financier** se distingue avec le **niveau de maturité le plus élevé** en matière de gestion des menaces internes. À l'inverse, les entités **gouvernementales** affichent une **maturité plus limitée**, reflétant une progression moins avancée vers des capacités structurées.

Recul des politiques et cadres robustes

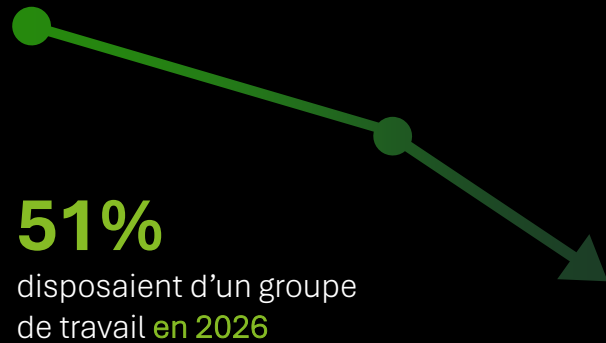


disposaient de politiques et cadres **robustes en 2026**

38 % des organisations ne disposent d'aucune politique ou cadre formel ce qui indique que plusieurs programmes demeurent peu structurés pour prévenir, détecter et encadrer les risques de menace interne.

Une gouvernance encore peu formalisée face à la menace interne

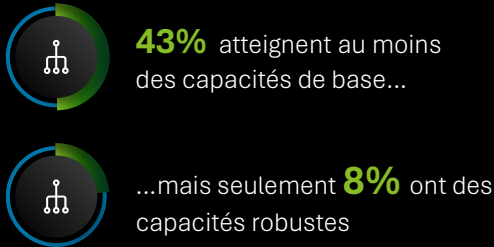
Recul des groupes de travail dédiés



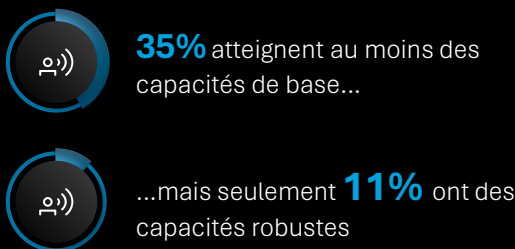
Le **groupe de travail multifonctionnel** demeure l'un des maillons les **moins matures** du dispositif de gestion de la menace interne, illustrant un **déficit persistant** de gouvernance intégrée et de coordination interfonctionnelle.

Formation, sensibilisation, escalade et triage peu robustes

Processus d'escalade et de triage



Programmes de formation/sensibilisation



Capacités de gestion de la menace interne

Certains contrôles fondamentaux affichent des niveaux de maturité inférieurs

Vérifications d'antécédents pré-emploi



86%
effectuaient une
vérification des
antécédents pré-emploi



89%
effectuaient une
vérification des
antécédents pré-emploi



Les **vérifications d'antécédents pré-emploi** sont toujours bien implantées dans l'ensemble des secteurs, avec peu d'écart restant à combler vers **une adoption généralisée**.

Vérifications d'antécédent en continu



62%
effectuaient une
vérification des
antécédents en continu



57%
effectuaient une
vérification des
antécédents en continu



Les **vérifications d'antécédents en continu ou périodiques** demeurent **moins systématiques**, à l'exception des organisations gouvernementales*, qui affichent un niveau de maturité plus élevé dans ce domaine.

Procédure de départ formalisée



81%
avaient en place des
procédures pour gérer
le risque lié aux
employés sortants



70%
avaient en place des
procédures pour gérer
le risque lié aux
employés sortants

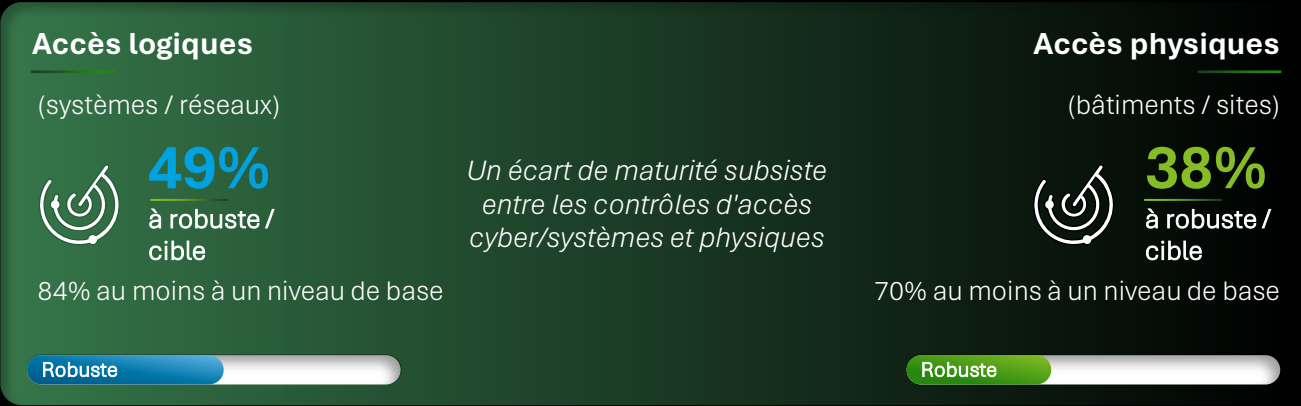


Les réponses indiquent que les organisations n'ont pas encore pleinement standardisé la formalisation des processus de **départ des employés**.

** Cette situation pourrait s'expliquer par l'entrée en vigueur, le 6 janvier 2025, de la version adaptée de la Directive du Secrétariat du Conseil du Trésor (SCT) sur le filtrage de sécurité, laquelle exige que les organisations fédérales mettent en œuvre un processus d'assurance continue basé sur une approche d'évaluation des risques.*

Capacités de gestion de la menace interne

Réduction de l'écart entre les contrôles d'accès logique et physique robuste

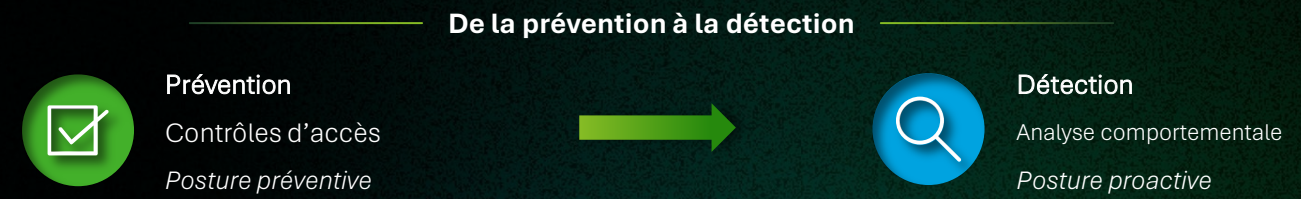


 Les **contrôles d'accès physiques et logiques** demeurent parmi les capacités **les plus développées**

L'adoption de l'UEBA semble être en progression



 Cependant, l'UEBA demeure **l'une des capacités les moins matures** : son adoption est portée par **l'exposition sectorielle au risque** plutôt que par la taille des organisations, ce qui en fait un **levier encore sous-exploité** pour passer d'une posture réactive à proactive.



Les organisations ont réalisé davantage de progrès en matière **de contrôle des accès privilégiés** qu'en matière de **surveillance continue des comportements à risque préalablement définis**, ce qui met en évidence un écart persistant entre les capacités de prévention et de détection.

Comparaison sectorielle

Financier

Leader en maturité... mais plus exposé à la menace interne



3,7/5

Score moyen de maturité **le plus élevé** en matière de **gestion de la menace interne**

87%

ayant subi ≥ 1 **incident** dans les 12 derniers mois (le plus élevé)

Priorité stratégique

Renforcer le dépistage continu et les programmes de sensibilisation des employés



54%

des organisations du **secteur Finance** ayant déclaré au moins un incident de menace interne ont subi de la **fraude**, ce qui en fait la menace la plus répandue.

Gouvernement

Approche plus équilibrée, malgré une maturité globale inférieure



2,8/5

Score moyen de maturité en matière de formalisation des politiques et des cadres

2,6/5

Score moyen de maturité pour le groupe de travail multifonctionnel

Priorité stratégique

Renforcer la gouvernance et la sensibilisation



18%

Les **incidents d'ingérence étrangère et d'extrémisme violent** sont quasi exclusivement rapportés par les entités gouvernementales (18% des organisations respectivement).



63%

Près du tiers des organisations ayant signalé des incidents de violence et de harcèlement au travail proviennent respectivement des secteurs **Gouvernement et Énergie** (31 % chacun).

Énergie et services publics

Forte exposition aux incidents malgré une priorisation exécutive plus faible



2,8/5

Score moyen de priorisation de la menace interne par les exécutifs (le + faible)

46%

ayant subi ≥ 1 incident dans les 12 derniers mois (le + élevé)

Priorité stratégique

Investir dans la sensibilisation et la détection



75%

Le **Sabotage TI** est concentré dans le secteur Énergie et services publics, représentant 75% des organisations ayant déclaré avoir subi ce type d'incident.

Conclusion

Posture Proactive



La modernisation de la détection ne doit pas se faire au détriment des contrôles fondamentaux. Alors que l'adoption de capacités avancées progresse, plusieurs mécanismes éprouvés du cycle de vie de l'employé s'érodent. Ce déséquilibre expose les organisations à bâtir des capacités sophistiquées sur des fondations qui se fragilisent, précisément aux transitions les plus sensibles : accès, mobilité et départ.

Diagnostic de maturité des capacités

Prévention		Détection		Réponse	
2025	2026	2025	2026	2025	2026
2,7/5	2,7/5	2,8/5	2,8/5	3,2/5	3/5
▲ +0,0		▲ +0,0		▼ -0,2	



Les organisations canadiennes ont franchi le cap de la reconnaissance : la menace interne est désormais traitée comme un **risque d'entreprise**. Cette prise de conscience ne s'est toutefois pas encore traduite en programmes structurés – **à peine 5 % disposent de politiques et de cadres robustes** – laissant un écart important entre l'intention et l'exécution.



Le profil de risque varie selon les secteurs, mais la **hausse des incidents de harcèlement et de violence en milieu de travail**, combinée à la prédominance persistante des incidents liés à la négligence, souligne la **nécessité d'accorder autant d'importance au facteur humain qu'aux contrôles techniques**.



Le prochain cap est celui de la proactivité. Aucun secteur n'atteint encore le seuil de 3/5 en posture proactive, et la prévention marque même un léger recul. Faire progresser la maturité d'ici la prochaine édition supposera une gouvernance intégrée, une surveillance continue mieux outillée et une coordination interfonctionnelle renforcée, pour passer d'une posture réactive à une gestion anticipée du risque.

Contacts clés



Pierre-Luc Pomerleau
Ph.D.
Associé, Crimes Financiers
E : ppomerleau@deloitte.ca



Victor Munro
Ph.D.
Président-directeur général, CInRM CoE
E : victor.munro@cinrmcoe-cdecgrinc.ca

Secrétaire général, APRI
E : victor.munro@irpa.org

Contributeurs



Isabelle Fraser
Directrice



Mélissa Bourgie
Directrice



Sébastien Bodart
Analyste



Sabrina Marleny Cruz Jimenez
Analyste

À propos de Deloitte Canada

Chez Deloitte, notre raison d'être est d'avoir une influence marquante. Nous existons pour inspirer et aider nos gens, nos organisations, nos collectivités et nos pays à prospérer. Notre travail soutient une société prospère où les gens peuvent s'épanouir et saisir des occasions. Il renforce la confiance des consommateurs et des entreprises, aide les organisations à trouver des moyens créatifs de déployer des capitaux, habilite des institutions sociales et économiques justes, fiables et efficaces, et permet à nos amis, à nos familles et à nos collectivités de profiter de la qualité de vie qui accompagne un avenir durable. Étant le plus grand cabinet de services professionnels détenu et exploité par des Canadiens dans notre pays, nous sommes fiers de travailler aux côtés de nos clients pour avoir une influence positive sur tous les Canadiens.

Deloitte offre des services de premier plan dans les domaines de la consultation, de la fiscalité et des services juridiques, des conseils financiers, de l'audit et de la certification ainsi que des conseils en gestion des risques à près de 90 % des sociétés du palmarès Fortune Global 500^{MD} et à des milliers de sociétés fermées. Nous réunissons des compétences, des perspectives et des services de classe mondiale pour aborder les enjeux d'affaires les plus complexes de nos clients.

Deloitte S.E.N.C.R.L./s.r.l., société à responsabilité limitée constituée en vertu des lois de l'Ontario, est le cabinet membre canadien de Deloitte Touche Tohmatsu Limited. Deloitte désigne une ou plusieurs entités parmi Deloitte Touche Tohmatsu Limited, société fermée à responsabilité limitée par garanties du Royaume-Uni, ainsi que son réseau de cabinets membres dont chacun constitue une entité juridique distincte et indépendante. Pour obtenir une description détaillée de la structure juridique de Deloitte S.E.N.C.R.L./s.r.l. et de ses filiales, veuillez consulter www.deloitte.com/ca/apropos.

Pour en apprendre plus sur Deloitte Canada, veuillez nous suivre sur [LinkedIn](#), [X](#), [Instagram](#) ou [Facebook](#).

© 2026 Deloitte S.E.N.C.R.L./s.r.l. et ses sociétés affiliées.

À propos du Centre d'excellence canadien en gestion des risques liés aux menaces internes (CInRM CoE)

Fondé en 2022, le Centre d'excellence canadien en gestion des risques liés aux menaces internes (CInRM CoE) est un organisme sans but lucratif constitué en vertu de la Loi canadienne sur les organisations à but non lucratif. Établi à la Norman Paterson School of International Affairs (NPSIA) de l'Université Carleton, il agit comme organisme de service public voué à l'avancement des pratiques de gestion des risques liés aux menaces internes au Canada.

Le CInRM CoE favorise les partenariats entre les milieux universitaire, public et privé afin de soutenir la recherche, la formation, le partage des connaissances et le développement des capacités visant à atténuer les menaces internes au sein des organisations canadiennes et des infrastructures essentielles. Ses services sont offerts aux organisations fédérales, provinciales, territoriales et autochtones du Canada, avec un accent particulier sur le renforcement de la résilience des infrastructures essentielles.

Le Centre adopte une approche interdisciplinaire de la gestion des risques liés aux menaces internes afin de promouvoir les pratiques exemplaires et l'innovation dans un contexte de menaces en constante évolution. Financé par des contributions de l'industrie et des subventions de recherche, il offre une expertise nationale centralisée en matière de risques liés aux menaces internes. Ses activités comprennent la recherche et l'analyse, l'animation d'ateliers et d'événements de partage des connaissances, la production de leçons apprises, la formation en milieu de travail ainsi que la promotion d'initiatives visant à renforcer la résilience collective du Canada face aux menaces internes. Ces travaux reposent sur une solide culture de partage de l'information au sein d'une communauté de confiance composée de professionnels de la sécurité, du renseignement et de la défense.

© 2026 Centre d'excellence canadien en gestion des risques liés aux menaces internes (CInRM CoE).