DEUXIÈME ÉDITION DU FORUM SUR L'INTELLIGENCE ARTIFICIELLE DANS LE SECTEUR DES SERVICES FINANCIERS :

UNE APPROCHE COLLABORATIVE À L'ÉGARD DES MENACES, POSSIBILITÉS ET PRATIQUES EXEMPLAIRES LIÉES À L'IA

ATELIER 1 – SÉCURITÉ ET CYBERSÉCURITÉ

JUILLET 2025

INSTITUT DU RISQUE MONDIAL

Gouvernement du Canada | Government of Canada

« Le Forum qui se tient aujourd'hui nous offre une formidable occasion de mieux comprendre l'IA et son rôle dans le secteur financier, et de réfléchir à la manière d'envisager les risques liés à la sécurité et à la cybersécurité. Mieux comprendre ces questions, c'est dissiper des craintes non fondées, et ainsi nous permettre de nous concentrer sur les vrais problèmes et de trouver des solutions adaptées. »

Suzy McDonald, sous-ministre déléguée, ministère des Finances, mai 2025

AVANT-PROPOS

Ces dernières années, il est devenu de plus en plus important de comprendre, d'intégrer et de gérer de façon responsable l'utilisation qui est faite de l'intelligence artificielle (IA) dans le secteur financier. Il est aujourd'hui urgent de travailler en collaboration et d'élaborer des pratiques exemplaires dans ce domaine.

Dans le but d'alimenter la réflexion et le dialogue sur cette question cruciale, le Bureau du surintendant des institutions financières (BSIF) et l'Institut du risque mondial (GRI) ont organisé en 2022 la première édition du Forum sur l'intelligence artificielle dans le secteur des services financiers (FIASSF) pour promouvoir l'utilisation responsable de l'IA dans le secteur financier canadien. Cette initiative a permis de réunir des experts de l'IA issus du secteur financier ainsi que des décideurs politiques, des organismes de réglementation, des universitaires et des instituts de recherche.

Le rapport produit à la suite de cette première édition du Forum, Une perspective canadienne sur l'IA responsable, souligne la nécessité pour les institutions financières d'adopter des stratégies globales de gestion du risque afin de faire face aux problèmes singuliers que pose l'IA. Le rapport met en évidence 4 principes jugés essentiels pour assurer une utilisation responsable de l'IA : les principes EDGE (explicabilité, données, gouvernance et éthique).

L'évolution rapide des outils d'IA et la plus grande conscientisation des risques s'y rapportant font ressortir la nécessité d'élargir la portée de ces discussions et constituent la raison d'être de la deuxième édition du FIASSF : Une approche collaborative à l'égard des menaces, possibilités et pratiques exemplaires liées à l'IA. Cette deuxième édition s'articulera autour de 4 ateliers[i] qui porteront sur des problèmes pressants liés à l'IA auxquels est confronté le secteur

i Les ateliers sont organisés par le BSIF, le ministère des Finances (Finances Canada), l'Agence de la consommation en matière financière du Canada (ACFC), le Centre d'analyse des opérations et déclarations financières du Canada (CANAFE) et le GRI.

financier canadien : la sécurité et la cybersécurité; la criminalité financière; la protection des consommateurs; et la stabilité financière. Chaque atelier donnera lieu à un rapport intermédiaire, comme celui-ci, et un rapport final sera produit pour présenter les thèmes clés, les enseignements, les pratiques exemplaires et les recommandations en lien avec l'ensemble des sujets abordés.

Le premier atelier, qui a eu lieu le 28 mai 2025, était organisé par le BSIF, Finances Canada et le GRI. Il a réuni 56 experts de l'IA canadiens et étrangers de tous horizons : banques, assureurs, gestionnaires d'actifs, universitaires, fournisseurs de technologie, mais aussi décideurs politiques et organismes de réglementation et de surveillance fédéraux et provinciaux.

Les participants s'étaient donné 2 grands objectifs :

- Mieux comprendre comment les technologies d'IA redéfinissent les menaces et les possibilités au chapitre de la sécurité et de la cybersécurité
- Réfléchir à des pratiques exemplaires et à des stratégies efficaces de gestion des risques liés à l'IA, et apprendre à renforcer la résilience des organisations et des cadres de sécurité

Par « sécurité », on entend ici le fait que les institutions financières doivent se protéger contre les menaces internes et externes pesant sur leurs actifs physiques, leurs infrastructures, leur personnel, leurs technologies et leurs données. En ce sens, la sécurité ne se limite donc pas à la solidité des institutions, mais a des implications sur le plan de la sécurité nationale. Les capacités croissantes de l'IA amplifient la portée, l'ampleur et la rapidité de propagation des risques existants en matière de sécurité, et plus particulièrement dans le domaine de la cybersécurité, sachant que le cyberrisque est déjà l'un des risques les plus importants auxquels est confronté le système financier canadien. Pour faire face à ces risques, l'ensemble des parties prenantes doivent faire preuve de vigilance et prendre des mesures en amont.

Pour le système financier, l'IA est source à la fois de possibilités et de risques, et les organisateurs tiennent à remercier sincèrement tous les participants à l'atelier pour leur contribution et leur collaboration lors de ces discussions.

L'Institut du risque mondial (GRI)	Bureau du surintendant des institutions financières	Ministère des Finances Canada

SÉCURITÉ, CYBERSÉCURITÉ ET IA : ÉCLAIRAGES SUR LES MENACES, LES RISQUES ET LES MESURES D'ATTÉNUATION

> « Selon les estimations, les coûts directs et indirects associés aux cyberincidents oscillent entre 1 % et 10 % du PIB mondial. Le nombre d'attaques par hypertrucage est 20 fois plus élevé aujourd'hui qu'il y a 3 ans. »
>
> Michael Barr, Conseil des gouverneurs, Réserve fédérale, avril 2025

L'IA est une arme à double tranchant. De fait, si les acteurs du secteur financier adoptent des solutions d'IA qui permettent par exemple d'améliorer le service à la clientèle, de faciliter la détection des fraudes ou d'automatiser le règlement des demandes d'indemnisation, il existe aussi des outils d'IA similaires qui créent des risques ou les amplifient, et donnent ainsi les moyens aux auteurs de menaces d'adopter rapidement l'IA pour renforcer l'efficacité de leurs activités malveillantes.

Optique du secteur financier au sujet de l'adoption de l'IA

Lorsqu'on a demandé aux participants à l'atelier de nommer les 3 principaux obstacles internes auxquels sont confrontées les institutions financières au chapitre de la gestion des risques de sécurité liés à l'IA, 60 % ont indiqué que le frein le plus important tenait au fait que l'IA progresse plus rapidement que les pratiques de gestion du risque ne s'adaptent. Le deuxième obstacle le plus cité, juste derrière, est le contrôle de sécurité des fournisseurs tiers.

Les experts de l'IA du secteur financier ont insisté sur le fait que les risques liés à l'IA doivent être pleinement intégrés aux cadres de gouvernance et de gestion du risque des institutions. Pour ce faire, dans de nombreux cas, il est possible qu'une actualisation des cadres soit nécessaire compte tenu de l'ampleur et du rythme de l'évolution de l'IA, ce qui peut comprendre l'établissement d'une fonction de supervision de l'IA par la direction. Cet exercice passe par la consolidation des politiques et des mécanismes de contrôle

Figure 1 : Questionnaire des participants, 28 mai 2025

existants. Les participants ont par ailleurs rappelé qu'une hygiène technologique de base est essentielle et que « parfois, des mécanismes de contrôle élémentaires tout simples jouent un rôle essentiel dans la gestion de ces risques importants liés à l'IA, par exemple dans le cas des tiers ».

Les participants au Forum ont aussi souligné qu'il était important que l'adoption de l'IA soit fondée sur une analyse de cas d'utilisation ou sur une analyse de rentabilité. Autrement dit, il ne faut pas envisager l'IA comme le dernier « gadget à la mode » qu'il faut absolument se procurer, mais plutôt s'assurer que l'adoption de l'IA produit des résultats tangibles pour les actionnaires ou les parties prenantes.

Lors de l'atelier, les participants ont cerné les 4 menaces ou risques suivants associés à l'IA dans le contexte du secteur financier, de pair avec des mesures d'atténuation.

1. Piratage psychologique et fraude à l'identité synthétique

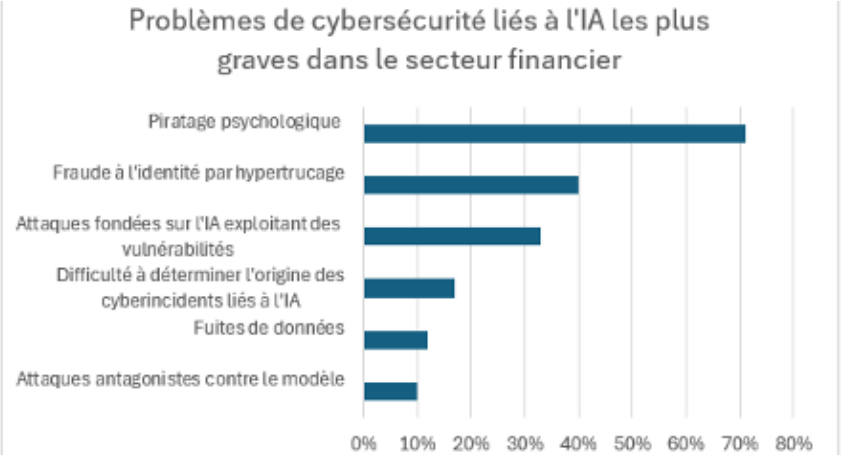
Nature du risque

L'IA donne un coup de fouet aux attaques par hameçonnage et par fraude à l'identité synthétique grâce à des méthodes de piratage psychologique qui sont convaincantes et peuvent évoluer et s'adapter, ce qui accentue les risques pour l'intégrité financière et la sécurité nationale. Les pratiques d'intégration virtuelle permettent aux auteurs de menaces d'utiliser des hypertrucages et d'autres outils d'IA pour s'infiltrer au sein des entreprises.

Aujourd'hui, il suffit à l'IA de quelques secondes d'enregistrement audio pour imiter la voix d'une personne. Par conséquent, il est possible de créer des hypertrucages capables de tromper des employés et de les amener à commettre des actes préjudiciables. Le contenu accessible sur les médias sociaux peut être utilisé pour créer des attaques par hameçonnage convaincantes et hyperpersonnalisées, qui peuvent ensuite être menées rapidement et à grande échelle, et qui sont donc bien plus susceptibles de réussir.

Au total, 71 % des participants à l'atelier ont indiqué que le piratage psychologique dopé à l'IA constituait le problème de cybersécurité lié à l'IA le plus grave dans le secteur financier. Le deuxième problème le plus grave, cité par 40 % des participants, est la fraude à l'identité par hypertrucage.

Figure 2 : Questionnaire des participants, 28 mai 2025



Dorénavant, les entreprises doivent être plus attentives aux risques de piratage psychologique et de fraude à l'identité, car ils accentuent les possibilités d'infiltration, notamment dans le cadre du processus d'embauche. Citons un exemple récent pour illustrer ce risque : des identités synthétiques générées par l'IA ont permis à des agents nord-coréens de décrocher un emploi en télétravail dans des entreprises nord-américaines. Une fois embauchés, ces agents ont eu accès aux systèmes internes des entreprises, exposant ainsi des données exclusives et des informations sur les clients à une possible exfiltration[ii].

Conséquences sur le plan de la gestion du risque

Pour contrer les menaces liées au piratage psychologique dopé à l'IA, les institutions renforcent les procédures de vérification de l'identité et actualisent la formation des employés.

Les mesures préventives peuvent aussi consister à promouvoir une culture de vigilance et à encourager le personnel à remettre en question les demandes inattendues, en particulier celles qui ont trait à des données sensibles ou à des opérations financières. Parallèlement, certaines institutions adoptent des outils de surveillance fondés sur l'IA pour détecter les scénarios de communication inhabituels et repérer les intrusions en temps réel.

2. Cyberattaques assistées par l'IA

Nature du risque

Les auteurs de menaces instrumentalisent l'IA pour automatiser, accélérer et personnaliser leurs cyberattaques. Parallèlement, le fait que les institutions financières utilisent de plus en plus l'IA a pour effet d'élargir le périmètre d'attaque global et d'accroître la vulnérabilité des institutions aux attaques.

D'une part, les progrès de l'IA font que les auteurs de menaces ont moins d'obstacles à contourner pour s'introduire dans les systèmes et, d'autre part, ils permettent de créer des outils très élaborés qui réduisent l'efficacité des mesures de sécurité traditionnelles. Les outils dopés à l'IA, comme les maliciels capables de s'adapter, permettent aux auteurs de menaces d'agir vite et de causer des dommages importants à leurs cibles, mais aussi de repérer plus rapidement et avec plus de précision les vulnérabilités de sécurité des institutions financières.

Les modèles d'IA internes utilisés par les institutions financières traitent souvent des données sensibles, et les menaces comme les empoisonnements de données, les extractions de modèles et les manipulations antagonistes présentent des risques importants. Les fuites de données peuvent entraîner l'exposition de données sensibles, une vulnérabilité accrue aux attaques antagonistes (ou adverses) et la perte de propriété intellectuelle, et minent donc l'intégrité opérationnelle et la confiance des clients.

ii Office of Public Affairs | Fourteen North Korean Nationals Indicted for Carrying Out Multi-Year Fraudulent Information Technology Worker Scheme and Related Extortions | Département de la Justice des États-Unis (en anglais seulement)

Lors de l'atelier, l'un des intervenants a souligné que les cyberattaques ont évolué; elles sont passées de la phase dite de « possibilité », où un auteur de menace donné peut lancer une seule attaque malveillante, à la phase dite d'« automatisation », où un auteur de menace peut générer des millions d'incidents simultanés à l'aide d'outils dopés à l'IA.

Les participants à l'atelier se sont également dits préoccupés par le fait que les campagnes de « désinformation » sur les médias sociaux pourraient amplifier les cyberattaques assistées par l'IA. Les perturbations du marché sont perçues comme étant une menace bien réelle, surtout en cas d'attaques multiformes ciblant une institution en particulier, des groupes d'institutions ou d'autres composantes essentielles de l'infrastructure financière du Canada.

Il a également été question du fait que les organismes gouvernementaux sont eux aussi exposés au risque de cyberattaque, car ils sont les dépositaires de quantités importantes de données exclusives et sensibles des institutions financières. L'intégrité des données repose donc sur les efforts de sécurité et de cybersécurité de tous les membres de l'écosystème.

Conséquences sur le plan de la gestion du risque

Les participants ont suggéré d'adopter différentes tactiques préventives pour se défendre contre les cybermenaces fondées sur l'IA qui sont de plus en plus complexes, et pour remédier à ces vulnérabilités :

1. Adopter des outils de sécurité assistés par l'IA
   - Adopter des outils de sécurité qui existent déjà et qui sont capables de détecter les anomalies et les activités inhabituelles en temps réel
   - Mettre en œuvre des normes de sécurité reposant sur le principe de vérification systématique, de manière que chaque demande d'accès à des données soit validée
2. Établir des normes d'intégrité en matière de modèles d'IA
   - Effectuer des tests de résistance aux attaques antagonistes et offrir de la formation pour renforcer la résilience
   - Établir des procédures de surveillance des requêtes et utiliser des outils de limite d'accès pour détecter et bloquer les scénarios d'accès atypiques
3. Parfaire la formation des employés
   - Créer des outils de formation à l'intention des employés pour qu'ils soient capables de repérer et de signaler les comportements suspects
4. Améliorer les protocoles d'échange d'informations
   - Tirer parti des échanges d'informations entre l'ensemble des parties prenantes pour constituer une base de renseignements communs sur les menaces

3. Vulnérabilités aux systèmes d'IA des tiers et de la chaîne d'approvisionnement

Nature du risque

Le fait que les institutions financières ont recours à des infrastructures et à des modèles d'IA de tiers qui sont opaques les expose à des risques en cascade. Cela s'explique par des réseaux de dépendances grandissants provenant de sources multiples au sein de la chaîne d'approvisionnement, ce qui crée de nouveaux points faibles potentiels et ouvre la voie à de possibles attaques.

Le secteur financier canadien dépend fortement de fournisseurs de services tiers, en particulier dans le domaine de l'IA. L'adoption de l'IA accroît donc les dépendances envers les tiers pour ce qui est de la conception des modèles, des services de données et de l'infrastructure informatique. Les petites et moyennes institutions financières font souvent davantage appel à des fournisseurs externes, ce qui élargit le périmètre des risques auxquels elles sont exposées et accroît les risques liés aux tiers associés à l'IA.

Les institutions dépendent de plus en plus de fournisseurs de quatrième, cinquième et nième niveau au sein des « chaînes d'approvisionnement » en IA, ce qui accentue le risque que la perturbation ou la faillite d'un seul fournisseur engendre des répercussions importantes. Les petits fournisseurs d'IA peuvent mettre en péril les chaînes d'approvisionnement s'ils ne disposent pas des mécanismes nécessaires pour contrôler la résilience.

A contrario, le risque de concentration augmente lui aussi, car les grands fournisseurs de services infonuagiques fondés sur l'IA et les concepteurs de modèles de base sont peu nombreux, et la faillite de l'un d'entre eux pourrait avoir des effets perturbateurs en cascade dans le secteur financier.

Un autre risque courant lié aux tiers fournisseurs de services d'IA est le manque de transparence – que ce soit au niveau des données, de la conception des modèles ou des algorithmes – qui fragilise l'intégrité des données et complique la validation des modèles. Même les modèles entièrement libres fonctionnent souvent comme des boîtes noires, moyennant des milliards de paramètres appris automatiquement dont l'interprétation est extrêmement difficile, voire carrément impossible.

Conséquences sur le plan de la gestion du risque

Les dépendances croissantes envers les tiers fournisseurs de services d'IA et les vulnérabilités des chaînes d'approvisionnement font qu'il est nécessaire d'actualiser les protocoles de vérification préalable et d'établir clairement les responsabilités des fournisseurs, de manière à assurer l'application de normes de sécurité et de résilience opérationnelle uniformes et renforcées.

Les participants ont évoqué différentes mesures pour améliorer la résilience à l'égard des tiers, notamment les suivantes :

1. Normaliser les obligations contractuelles
   - Normaliser un libellé de contrat qui peut être utilisé par des institutions de toutes tailles
   - Établir des cadres de responsabilisation et des droits d'audit clairs

2. Établir des normes de sécurité uniformes

- Exiger que les modèles externes fassent l'objet de tests de sécurité indépendants
- Imposer le respect des normes ISO ou d'autres normes internationales par les tiers fournisseurs de services d'IA

3. Établir des exigences de communication uniformes

- Exiger la transparence des données et des modèles
- Établir des protocoles de communication des dépendances à l'égard de la chaîne d'approvisionnement des tiers
- Introduire des exigences en matière de consignation des informations par écrit

4. Renforcer la surveillance des tiers

- Étudier des moyens de resserrer la surveillance des principaux tiers fournisseurs de services d'IA par les organismes de réglementation
- Dresser une liste de fournisseurs de services d'IA agréés qui serait approuvée et utilisée par les professionnels du milieu et les organismes de réglementation

5. Mobiliser par la collaboration

- Mettre sur pied une tribune d'échange d'informations réunissant des institutions financières, des organismes de réglementation et des organismes de surveillance pour favoriser la gestion des risques liés aux tiers associés à l'IA

4. Vulnérabilités des données attribuables à l'IA

Nature du risque

Non seulement les systèmes d'IA augmentent le risque de corruption et de fuite de données, mais ils transforment aussi les données sensibles de grande valeur des institutions et des clients en cibles de plus en plus vulnérables pour les auteurs de menaces.

Les modèles et systèmes d'IA utilisent de très grands volumes de données exclusives ou de données sensibles sur les clients. Du fait de la rapidité avec laquelle ces modèles et systèmes ont été élaborés, le risque de perte de données commerciales ou financières exclusives et de données sensibles sur les clients a considérablement augmenté. L'adoption de systèmes d'IA par l'ensemble des fonctions opérationnelles accroît également la vulnérabilité des données. Le fait que ces données pourraient être corrompues peut entraîner des erreurs dans l'évaluation du risque, la valorisation des actifs ou le processus automatisé de prise de décisions, erreurs qui pourraient se traduire par une érosion de la confiance, une atteinte à la réputation ou des pertes opérationnelles.

Enfin, les données dont l'accessibilité était auparavant restreinte selon le principe du « besoin de savoir » sont désormais accessibles à un plus grand nombre de personnes ayant besoin d'y accéder pour qu'il soit possible de tirer les avantages attendus de l'IA. Ce phénomène accentue le risque de perte de données ou de violation de la confidentialité des données.

Conséquences sur le plan de la gestion du risque

Les participants ont évoqué différentes mesures pour atténuer les vulnérabilités des données attribuables à l'IA, notamment les suivantes :

1. S'engager à respecter les principes fondamentaux
   - Accorder la priorité aux mesures fondamentales d'hygiène informatique liées à la sécurité, notamment la sécurité des réseaux
   - Encourager l'adoption de procédures d'authentification multifactorielle
2. Définir clairement le « besoin de savoir »
   - Améliorer les mécanismes de contrôle de la gestion de l'identité et de l'accès (GIA) pour pouvoir distinguer les différents types d'accès aux données sensibles (pour mener les activités ou pour développer l'IA)
3. Établir de nouvelles normes régissant l'exportation des données
   - Élargir la portée des lignes directrices sur la gouvernance et la gestion du risque pour y inclure l'exportation de données exclusives et de données sensibles sur les clients
4. Adopter de nouveaux outils dopés à l'IA
   - Investir dans l'élaboration et la mise en service d'outils de surveillance de la sécurité dopés à l'IA pour analyser l'accès aux données, la confidentialité et les vulnérabilités des réseaux, et pour fournir le soutien requis
5. Renforcer les plans de reprise des activités
   - Renforcer les plans de reprise des activités pour couvrir des éventualités comme la diffusion involontaire de données commerciales et institutionnelles exclusives

Possibilités liées à l'IA dans le secteur financier canadien

Menaces, risques et échanges d'informations en temps utile

Selon les participants, il existe une réelle possibilité de renforcer les dispositifs de sécurité dans le secteur financier en améliorant les échanges d'informations entre les gouvernements et les institutions, principalement au moyen de renseignements opportuns, anonymisés et exploitables. Ils estiment également qu'une plus grande collaboration, que ce soit au sein des entités, entre les secteurs ou entre les entreprises de toutes tailles, est un facteur essentiel pour assurer une bonne gestion des cyberrisques liés à l'IA et une intervention efficace en cas d'incidents de sécurité.

Identification et vérification numériques

Selon certains participants, au vu de la forte augmentation des cas de piratage psychologique, d'hypertrucage et de fraude à l'identité synthétique dopés à l'IA, il est devenu évident qu'il faut se doter de procédures d'identification et d'authentification numériques sécurisées. Un solide cadre d'identification numérique pourrait aider à s'assurer que seules les personnes ayant fait l'objet d'une vérification appropriée ont accès aux systèmes et aux données sensibles.

Adoption universelle de l'authentification multifactorielle

Des participants ont fait valoir qu'il est essentiel d'adopter l'authentification multifactorielle (AMF) pour pouvoir contrer les attaques faisant appel à l'IA. De fait, l'ajout d'une deuxième couche, ou étape, de vérification permet de protéger les systèmes, les données et les comptes clients contre les compromissions, faisant ainsi de l'AMF un pilier essentiel de la sécurité des institutions et des clients. Comme l'a fait remarquer un participant, « les consommateurs exigent rapidité et convivialité, mais il faut tout de même trouver un juste équilibre entre redondances et risque ».

Refonte de la formation des employés au regard du piratage psychologique

Les participants à l'atelier ont plaidé en faveur d'une « refonte » de la formation des employés au regard des tentatives d'hameçonnage hyperpersonnalisé, en trouvant un juste équilibre entre réalisme et préoccupations en matière d'éthique et de protection de la vie privée. Au lieu d'avoir recours à des simulations trompeuses, les institutions pourraient opter pour des approches d'apprentissage reposant sur des scénarios et sur l'acquisition d'habitudes pour préparer le personnel à contrer des menaces très élaborées, qui permettent de préserver la confiance.

Prochaines étapes

Les participants retiendront de l'atelier que les services financiers sont particulièrement bien placés pour tirer parti du développement et de l'adoption des systèmes d'IA, du fait que ce secteur repose essentiellement sur les données. L'IA offre des perspectives prometteuses pour ce qui est de relever certains des problèmes de productivité qui persistent depuis de nombreuses années au Canada. Notre secteur financier se trouve donc dans une position particulièrement favorable pour jouer un rôle moteur dans l'adoption responsable de l'IA.

> « Il est judicieux de recourir à des tribunes réunissant des acteurs des secteurs public et privé pour apprendre ensemble et trouver des moyens de tirer parti des avantages que peut apporter l'utilisation de l'IA en conjonction avec des pratiques de gestion du risque et des mécanismes de contrôle adaptés. »
>
> Angie Radiskovic, surintendante adjointe, Bureau du surintendant des institutions financières, mai 2025

Les institutions financières, les organismes de réglementation, les organismes de surveillance et les universitaires se sont tous montrés très enclins à poursuivre la conversation sur ces questions et sur d'autres sujets liés à l'IA dans le but de faire progresser les politiques et les pratiques exemplaires de gestion du risque, et d'accélérer l'innovation responsable dans le domaine de l'IA. Les organisateurs continueront d'alimenter ces discussions en vue de parvenir à un juste équilibre entre gestion du risque et innovation.

En outre, il sera possible d'approfondir les sujets abordés dans ce rapport intermédiaire lors des 3 autres ateliers prévus dans le cadre de la deuxième édition du FIASSF. Plusieurs des discussions qui se sont tenues durant ce premier atelier ont d'ailleurs porté sur des sujets directement liés aux ateliers à venir sur la criminalité financière, la protection des consommateurs et la stabilité financière, notamment :

i. les tactiques de piratage psychologique et la fraude à l'identité synthétique, qui sont principalement utilisées pour commettre des crimes financiers classiques et des tentatives de blanchiment d'argent (deuxième atelier);

ii. l'importance de communiquer avec les clients concernant l'utilisation de leurs données et les risques auxquels ils pourraient être exposés (troisième atelier);

iii. en quoi la désinformation et les campagnes de mésinformation amplifiées par l'IA représentent une menace émergente pour la stabilité financière, du fait qu'elles peuvent éroder la confiance du public et perturber les marchés (quatrième atelier).

Des rapports intermédiaires seront publiés après chaque atelier. Une fois tous les ateliers terminés, un rapport final détaillé suivra pour présenter les principaux enseignements et les pratiques exemplaires.

© Sa Majesté le Roi du Chef du Canada, 2025

IN4-35/2025F-PDF
ISBN 978-0-660-77977-5