Autorité
des marchés
financiers

Juillet 2026

Gestion des risques liés à la criminalité financière

Survol des bonnes pratiques observées dans les institutions financières

Table des matières

Dépôt légal – Bibliothèque et Archives nationales du Québec, 2026
ISBN 978-2-555-04350-3 (PDF)

Préambule

Dans l'exercice de leurs activités, les institutions financières évoluent dans un environnement où les risques liés à la criminalité financière sont en constante évolution. Ce type de criminalité se manifeste par des méthodes de plus en plus sophistiquées et diversifiées, nécessitant une adaptation continue des mécanismes de surveillance, de détection et de prévention mis en place par les institutions.

La criminalité financière englobe généralement trois grandes catégories de pratiques, qui peuvent avoir des impacts sur les clients :

- La fraude commise par une ressource interne à l'entité, comme un dirigeant, un administrateur ou un employé, en collusion ou non avec une personne à l'intérieur ou à l'extérieur de l'entité (par exemple un détournement de fonds par un employé);
- La fraude commise par un client ou par un tiers (par exemple une falsification de signature sur un chèque ou une réclamation d'assurance dont la valeur d'un bien réclamé a volontairement été surévaluée);
- Les pratiques associées au recyclage des produits de la criminalité (blanchiment d'argent) et au financement du terrorisme.

Bien que la surveillance et l'investigation de la criminalité financière relèvent en premier lieu d'organismes spécialisés, tels que le Centre d'analyse des opérations et déclarations financières du Canada (CANAFE) et les corps policiers, l'Autorité des marchés financiers (AMF) joue un rôle important en soutenant la résilience opérationnelle et financière du secteur ainsi qu'en assurant la protection et l'assistance des consommateurs de produits financiers et des utilisateurs de services financiers.

Dans le cadre de son mandat, l'AMF a mené, au cours de l'exercice 2025-2026, des travaux de surveillance transversale auprès d'un échantillon d'institutions financières autorisées à exercer au Québec. Ceux-ci s'inscrivent dans une démarche continue visant à mieux comprendre les pratiques de l'industrie et à évaluer la gestion des risques liés à la criminalité financière.

L'analyse s'est appuyée sur l'examen de documents ainsi que sur la tenue de rencontres statutaires ou d'entrevues auprès d'institutions de tailles et de types différents.

Assureurs de personnes	**Assureurs de dommages**
Institutions de dépôts	**Sociétés de fiducie et sociétés d'épargne**

Cette démarche visait à brosser un portrait des pratiques en matière de gestion des risques liés à la criminalité financière, incluant ceux associés à la fraude ayant un impact sur les clients.

Les constats et observations qui en découlent contribueront à la réflexion dans le cadre de la mise à jour de la *Ligne directrice sur la gestion des risques liés à la criminalité financière*. Par ailleurs, les pistes d'amélioration transmises de façon individualisée aux institutions, conformément au Cadre de surveillance des institutions financières et des agents d'évaluation du crédit, constituent également des intrants importants dans cette perspective.

Ces observations permettent également à l'AMF d'orienter et de prioriser les travaux visant le rehaussement des encadrements existants, en collaboration avec l'industrie, dans une optique d'optimisation de la charge de conformité.

Le présent document ne vise pas à présenter un état exhaustif des pratiques observées ni à établir de manière définitive les attentes de l'AMF. Il a plutôt pour objectif de partager certaines observations et bonnes pratiques afin de soutenir les institutions financières dans le renforcement de leurs dispositifs de gestion des risques liés à la criminalité financière et de favoriser une approche proactive et évolutive en la matière.

L'AMF espère que les bonnes pratiques dont ce rapport fait état permettront aux institutions de comparer leurs initiatives à celles de leurs pairs et qu'elles sauront les inspirer dans l'élaboration et le déploiement de leurs stratégies de gestion des risques liés à la criminalité financière.

Rappel des attentes de l'AMF

Les bonnes pratiques partagées ci-après sont mises en relation avec les attentes exprimées par l'AMF dans ses lignes directrices.

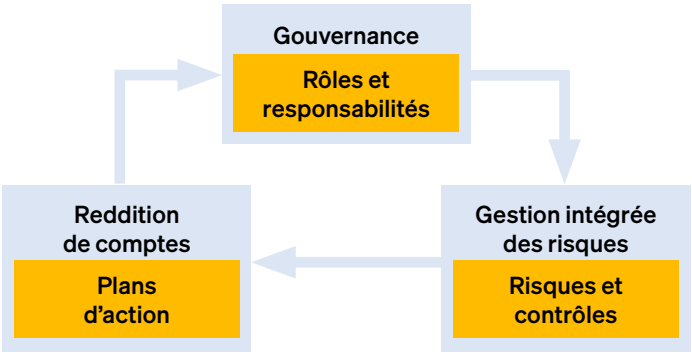
Encadrement des pratiques : qu'entend-on par attentes?

L'AMF préconise une approche prudentielle fondée principalement sur des principes et de bonnes pratiques, plutôt que sur l'édiction de règles prescriptives détaillées. À cette fin, conformément aux pouvoirs que lui confèrent les lois qu'elle administre, l'AMF établit des lignes directrices visant à informer les institutions financières des mesures qui, de son avis, leur permettent de satisfaire à leurs obligations, en fonction de leurs activités autorisées.

Il incombe à chaque institution de s'approprier les principes et les attentes énoncés dans les lignes directrices et d'en assurer une mise en œuvre appropriée, en tenant compte du principe de proportionnalité, soit en fonction de la nature, de la taille et de la complexité de ses activités ainsi que de son profil de risque.

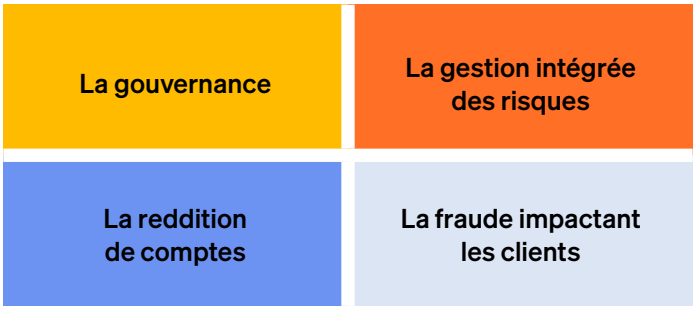
De façon générale, l'AMF s'attend à ce que la gestion des risques liés à la criminalité financière par les institutions financières :

- soit soutenue par une **gouvernance** efficace ainsi que par des rôles et responsabilités clairement établis;
- fasse partie intégrante de la **gestion intégrée des risques**;
- inclue un cadre formel de **reddition de comptes**.



La mise en œuvre de pratiques de gestion conformes à ces attentes permet aux institutions financières de prévenir et de détecter les activités associées à la criminalité financière et d'en mitiger les risques, tant pour l'institution que pour sa clientèle.

Les bonnes pratiques de gestion identifiées sont présentées sous quatre grandes thématiques.



Thème 1 : la gouvernance

Comme fondement d'une saine gestion, la majorité des institutions financières consultées se dotent d'une **structure de gouvernance** comprenant :

- l'identification des acteurs clés à leur bon fonctionnement;
- l'adoption d'une **politique globale**, adaptée à leur réalité, qui encadre la gestion de ces risques en précisant notamment :
  - les rôles et responsabilités des intervenants,
  - les interrelations avec le cadre de gestion des risques,
  - les mécanismes de gestion et de signalement des incidents de sécurité de l'information, incluant les fraudes,
  - la reddition de comptes requise,
  - les attentes,
  - la culture,
  - les conséquences pour les employés ou les tiers fautifs,
  - un organigramme illustrant la structure de gouvernance;
- l'adoption de **politiques spécifiques** traitant, entre autres, du blanchiment d'argent ainsi que de la fraude externe et interne;
- le développement d'**outils** permettant de considérer et de prendre en charge les situations auxquelles elles sont confrontées ainsi que de s'assurer que tous les secteurs sont adéquatement sensibilisés aux risques liés à la criminalité financière. Ces outils peuvent notamment prendre la forme de guides, d'aide-mémoire, de communautés de pratique, de rencontres de partage, d'établissements de tendances, d'analyses des causes racines ou de mécanismes de coordination organisationnelle.

À titre d'information, voici quelques exemples d'éléments relevés dans les différents mécanismes et politiques consultés, lesquels peuvent varier selon l'institution, sa taille et la complexité de ses activités.

Afin de préserver la pertinence de l'ensemble de leurs politiques en vigueur, de demeurer conformes aux attentes des autorités, de s'adapter aux nouveaux risques et d'améliorer leurs pratiques, plusieurs institutions effectuent des **mises à jour** :

- à intervalle régulier et préalablement établi, par exemple tous les deux ans;
- ponctuellement, au besoin, par exemple lorsque des faiblesses sont constatées dans les politiques, procédures et contrôles, lors de l'apparition de nouveaux stratagèmes, lors du lancement de nouveaux produits, lors du développement d'un nouveau type de clientèle ou lors d'un changement dans le modèle de distribution, dans la réglementation ou dans l'encadrement prudentiel.

Politique globale de gestion des risques

Exemples d'éléments considérés :

- Cadre de gouvernance et de gestion des risques (incluant un énoncé d'appétit pour le risque)
- Mandats ou chartes des comités
- Audits internes et externes
- Reddition, tableaux de bord et escalade

Encadrements ou mécanismes spécifiques de gestion des risques liés à la criminalité financière

Exemples d'éléments considérés :

- Sécurité de l'information
- Gestion des accès
- Gestion et registre des incidents
- Gestion des tiers et impartition
- Plan de continuité des affaires
- Utilisation de l'intelligence artificielle
- Prévention des pertes et des fraudes
- Gestion des cas et mesures de prévention
- Contrôle et vérification des fraudes et enjeux potentiels
- Taxonomie
- Indicateurs et stratagèmes
- Guide de conformité
- Bien connaitre son client
- Filtrage et traitement
- Classification et vérification
- Déclaration des opérations douteuses
- Formations obligatoires et en continu
- Communications
- Etc.

Politique spécifique liée à l'éthique ou à la conduite

Exemples d'éléments considérés :

- Codes pour les employés, les administrateurs et dirigeants et pour les fournisseurs
- Lutte à la corruption et à la collusion
- Déclaration de conflits d'intérêts
- Ligne éthique
- Ligne de signalement (dénonciation)
- Gestion des cas détectés/signalés
- Identification des sanctions et mesures disciplinaires
- Etc.

Thème 2 : la gestion intégrée des risques

En plus du cadre de gouvernance, l'AMF a constaté qu'en fonction de sa taille, l'institution dédie parfois une équipe spécialisée en gestion des risques **spécifiquement à la lutte contre la criminalité financière et la fraude**. Dans tous les cas, ces responsabilités relèvent d'un niveau hiérarchique élevé (par exemple la deuxième ligne de défense) et sont exercées de manière indépendante des opérations supervisées. Le responsable désigné dispose alors d'un accès direct au conseil d'administration ou à l'un de ses comités.

Outre la gestion des risques, la **contribution ou la collaboration d'autres secteurs** est aussi constatée pour assurer une saine gestion de ces risques, notamment les secteurs suivants :

- Affaires juridiques;
- Ressources humaines (par exemple en cas de sanctions ou de mesures disciplinaires envers un employé);
- Conformité;
- Approvisionnement (par exemple la gestion des contrats ou des tiers);
- Chef de la sécurité de l'information;
- Chef des technologies de l'information;
- Responsable de la protection des renseignements personnels;
- Chef des données;
- Responsable de la lutte contre la fraude;
- Audit interne.

Dans les meilleures pratiques, l'identification des risques liés à la criminalité financière se fait en tenant compte des **autres risques** auxquels l'institution est exposée (par exemple les risques opérationnels, les risques liés aux technologies de l'information et des communications (TIC) ainsi que les risques de non-conformité) et de sa vulnérabilité aux **facteurs internes et externes**.

Exemples de facteurs considérés lors de l'identification des risques

Facteurs internes à l'entité	Facteurs externes à l'entité
• Nature des activités • Caractéristiques des produits • Développement de nouveaux produits • Modèle de distribution • Profil de risque des clients • Relations d'affaires externes • Systèmes de technologies de l'information utilisés • Emplacement géographique • Expérience des employés • Etc.	• Contexte économique et social • Contexte géopolitique • Évolution des technologies et de la règlementation • Méthodes utilisées pour commettre des actes associés à la criminalité financière • Historique des incidents externes • Etc.

Les institutions financières consultées effectuent une **revue des risques et de l'environnement** auxquels elles sont exposées :

- sur une base périodique, en respectant une fréquence prédéfinie (par exemple tous les deux à trois ans) ou en réalisant une revue ponctuelle lorsque la situation l'exige;
- trimestriellement pour les institutions opérant dans un environnement à risque et en constante évolution;
- en ciblant des activités ou des produits spécifiques lorsque requis;
- en considérant les **activités réalisées par les tiers** avec lesquels elles font affaire.
- en fonction d'une **taxonomie des risques** qui leur est propre afin de s'assurer que tous les types de risques sont répertoriés. Ceux-ci varient selon le secteur d'activité de l'institution, sa taille et son contexte d'affaires.

Une illustration des risques TIC et des contrôles associés à certains scénarios est présentée à l'Annexe 1 afin de préciser les enjeux et les moyens mis en place par les institutions pour ce type de risques.

Certaines institutions regroupent les risques en familles de risques. Cela permet de faciliter l'identification de causes semblables pour ensuite mettre en place un éventail de mesures, dont certaines sont communes à un ensemble de risques, notamment des contrôles.

Les **moyens déployés pour contrer les risques** liés à la criminalité financière incluent, entre autres, des contrôles efficaces, l'utilisation de données pour détecter les menaces ainsi que le recours à des technologies permettant une intervention efficace.

En matière de **cybersécurité**, l'adoption d'une approche de sécurité à paliers multiples permet de garantir que, lorsqu'un contrôle est compromis, un autre puisse prendre le relais afin d'assurer la protection de l'information.

Voici quelques exemples de contrôles et de moyens plus spécifiques appliqués par les institutions financières.

Exemples de contrôles

Séparation des tâches	Seuils de transactions par niveau d'employés
Double approbation de transactions importantes/sensibles	Croisement d'information
Analyse de données	Vérification des antécédents (employés, partenaires d'affaires, fournisseurs)
Authentification multifacteurs	**Autres moyens**
Contrôles d'accès et encadrement des privilèges dans les systèmes	Code d'éthique et de déontologie
Journalisation des accès	Formations obligatoires, à l'embauche et récurrentes, sur la fraude et l'éthique

Thème 3 : la reddition de comptes

L'une des étapes importantes d'une saine gouvernance est la divulgation de l'information aux instances de gouvernance appropriées. L'AMF a constaté que les responsables de la gestion des risques liés à la criminalité financière rendent compte **au conseil d'administration ou à l'un de ses comités**, par exemple au comité d'audit ou au comité de gestion des risques, lequel inclut les risques TIC, afin de leur permettre :

- d'obtenir un portrait global de la situation de l'institution en matière de gestion des risques liés à la criminalité financière et ainsi de s'assurer de sa conformité aux lois, règlements et lignes directrices;
- d'identifier les contrôles à corriger ou à mettre en place;
- de suivre les tendances;
- d'être informé d'un évènement exceptionnel pouvant augmenter certains risques et d'en évaluer l'ampleur;
- de suivre l'évolution des risques.

Ces redditions de comptes portent, entre autres, sur :

- la vigie des risques émergents;
- certains cas survenus présentant des risques plus importants. Ceux-ci font également l'objet de communications spécifiques et directes au conseil d'administration ou aux comités d'audit et de gestion des risques, soit dans le cadre de ces rapports, soit à une fréquence plus rapprochée, au besoin;
- les tendances;
- les causes principales;
- les vérifications effectuées pour les enjeux présentant des risques plus importants;
- les remédiations en cours ou les actions demandées pour les risques plus importants.

Des informations plus détaillées sont aussi partagées, en les adaptant, à différents paliers hiérarchiques au moyen de tableaux de bord liés aux risques opérationnels, par exemple sous forme de ratios ou de tendances.

La figure suivante présente des **indicateurs spécifiques à la fraude** suivis par les institutions, lesquels peuvent être inclus dans ce type de reddition.

Les redditions présentent également l'information relative aux activités de prévention, notamment le nombre de formations données, les tests effectués sur différents contrôles ainsi que les encadrements en cours de mise à jour.

Indicateurs spécifiques à la fraude
Nombre de cas de fraudes, par trimestre, par produit et par secteur d'activité
Montant des fraudes (en moyenne et par minimum-maximum), ratios/tendances
Montant total des pertes liées à la fraude, globalement, par secteur et par type de fraude, ratios/tendances
Efficacité des contrôles en place
Comparabilité avec les autres institutions de même taille du même secteur
Taux d'identification des causes racines par type de fraude

Thème 4 : la fraude impactant les clients

Outre les travaux ayant mené à l'identification des pratiques en termes de gouvernance et de gestion des risques, des travaux portant spécifiquement sur la fraude impactant les clients ont également été effectués lors de la surveillance transversale. Dans le cadre de ce mandat, des rencontres ont été tenues avec une sélection d'institutions financières afin d'identifier les bonnes pratiques en place en matière de prévention, d'accompagnement des clients victimes de fraude, ainsi que de protection des clientèles vulnérables.

Pour ce qui est des bonnes pratiques liées à la **prévention**, l'AMF a constaté que des institutions financières :

- participent activement à des **communautés de partage** dont les objectifs sont de tenir leurs membres informés des dernières tendances en matière de fraude, de partager des informations liées aux modes opératoires utilisés par certains fraudeurs et de renforcer la vigilance collective de l'industrie. Ces communautés peuvent être constituées de groupes internes à une organisation, de différentes entités d'un même groupe financier ou de plusieurs institutions financières à l'échelle provinciale, nationale ou internationale.
- disposent également d'un **programme de formation** destiné à leurs équipes, aux dirigeants et aux tiers, comprenant certaines formations obligatoires. Ce programme vise notamment à outiller les intervenants de première ligne pour leur permettre de reconnaître différents stratagèmes de fraude ayant un impact sur la clientèle et ainsi d'agir rapidement pour limiter les risques pour les clients. Ces formations sont dispensées lors de l'embauche puis de façon continue, par exemple annuellement ou lorsque de nouvelles situations le justifient.
- ont mis en place des **lignes de signalement** anonyme à titre de mécanismes permettant aux clients et aux employés de signaler toute situation pouvant être associée à une tentative de fraude. Ces lignes de signalement contribuent ainsi à instaurer un environnement plus sécuritaire et à favoriser la détection proactive des comportements suspects. Les signalements sont traités de façon confidentielle et anonyme par un service indépendant, comme l'audit interne ou une firme externe spécialisée. Lorsque les situations le justifient, les rapports relatifs à ces signalements sont transmis à un comité, par exemple le comité de conformité et d'éthique, afin que les actions appropriées soient prises.

Plusieurs institutions ont établi une définition de la **notion de personne vulnérable**. Cette bonne pratique s'inspire, de manière générale, de la définition proposée par l'AMF dans son guide *Protéger un client en situation de vulnérabilité : Guide pratique pour l'industrie des services financiers*.

Ce guide a également inspiré d'autres bonnes pratiques en matière de **protection des clientèles vulnérables, notamment** :

- La désignation d'une personne de confiance dès l'ouverture ou lors de la mise à jour du dossier;
- L'obtention d'un consentement écrit et documenté, précisant les situations où la communication est permise et la nature des informations pouvant être partagées;
- La définition d'indices de vulnérabilité et de maltraitance financière à surveiller, par exemple des transactions inhabituelles, des changements soudains de comportement ou l'ingérence d'un proche;
- L'offre au client d'être accompagné par une personne de confiance s'il le souhaite;
- La mise en place d'un processus d'intervention graduelle en cas de soupçon de maltraitance;
- La désignation d'une personne-ressource interne pour les situations liées à la vulnérabilité et à la maltraitance;
- La formation des employés et des représentants sur l'identification des situations à risque, le rôle des personnes de confiance et la documentation attendue au dossier.

Certaines institutions financières ont exprimé des réserves quant aux **limites opérationnelles** auxquelles elles font face. En effet, bien que des mises en garde soient adressées au client, ce dernier demeure libre d'effectuer les transactions qu'il souhaite. Cette réalité crée un écart entre l'objectif de protection poursuivi et la capacité réelle d'éviter certaines situations, notamment lorsque le client exerce pleinement son autonomie décisionnelle malgré les risques identifiés ou portés à son attention par l'institution.

En matière d'**accompagnement des clients victimes de fraude**, les institutions ont indiqué que, lorsqu'un incident survient, elles mettent généralement en œuvre les bonnes pratiques suivantes :

- La désignation d'une personne-contact afin d'assurer un suivi en continu de la situation;
- L'élaboration de critères pour déterminer les causes de la fraude et appuyer la prise de décision quant à un éventuel dédommagement du client.

Autres outils et accompagnement offerts par l'AMF

Afin d'outiller les intervenants des institutions financières, l'AMF rend disponibles plusieurs contenus sur son site Web, notamment :

- Protection des données et des renseignements personnels
- Lutte contre le terrorisme
- Gestion des incidents de sécurité de l'information

D'autres contenus sont aussi disponibles afin de sensibiliser les clients et de les outiller face à différents stratagèmes et types de fraude.

Les clients et les intervenants du domaine financier peuvent également communiquer avec le centre d'information de l'AMF afin d'obtenir de l'information ou de l'assistance : 1 877 525-0337.

Les attentes de l'AMF sont exprimées, entre autres, dans les lignes directrices et encadrement suivants :

- *Ligne directrice sur la gestion des risques liés à la criminalité financière*
- *Ligne directrice sur la gouvernance*
- *Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications*
- *Règlement sur la gestion et le signalement des incidents de sécurité de l'information de certaines institutions financières et des agents d'évaluation du crédit*

Conclusion

Les travaux ayant servi de fondement au présent rapport ont permis de constater que les institutions sont sensibles à l'accroissement des risques relatifs à la criminalité financière, notamment en lien avec les technologies de l'information et des communications, ainsi que des conséquences que la criminalité financière peut avoir sur leurs activités.

Les analyses ont par ailleurs permis de dégager certaines pistes d'amélioration et de mettre en évidence des besoins de clarification. À titre d'exemple, l'AMF a constaté la nécessité de formaliser davantage ses attentes à l'égard de l'accompagnement offert par les institutions financières aux clients victimes de fraude. À cet égard, elle examinera les différentes avenues à sa disposition afin de soutenir l'industrie.

Tel qu'indiqué dans l'*Énoncé annuel des priorités 2026-2027* de l'AMF, l'évolution des encadrements nationaux et internationaux confirme la nécessité d'actualiser la *Ligne directrice sur la gestion des risques liés à la criminalité financière*. L'AMF entreprendra ainsi, au cours de 2026-2027, des travaux en ce sens, en s'appuyant sur les constats du présent exercice, dans le but notamment de renforcer le traitement équitable des clients en situation de fraude.

D'ici la mise à jour de cette ligne directrice, l'AMF invite les institutions financières à tirer parti des bonnes pratiques recensées dans ce document et à les intégrer de manière proportionnée à leurs activités, en fonction de leur profil de risque.

Annexe 1 - Gestion des risques liés aux technologies de l'information et des communications

Gestion des accès

Exemple de scénario fictif[1]

Un employé transféré dans un autre secteur de l'institution continue de détenir des accès obtenus dans le cadre de ses anciennes fonctions (rôle), notamment des autorisations transactionnelles lui permettant de modifier ou d'approuver certains dossiers clients.

Risques encourus

Cette situation peut générer plusieurs risques, dont :

- Risque d'erreur ou de manipulation de données, intentionnelle ou non;
- Risque de fraude interne, lorsque des accès transactionnels subsistent inutilement;
- Risque de conflit d'intérêts, en raison du changement de rôle;
- Risque de non-conformité et de bris de la séparation des tâches;
- Risque d'atteinte à l'intégrité de l'information, si des actions non détectées sont effectuées.

Exemples de mesures d'atténuation et bonnes pratiques identifiées

Une gestion rigoureuse du cycle de vie des accès est essentielle. Celle-ci peut prévoir les processus suivants :

- Retrait des droits et privilèges;
- Revue régulière ou certification des accès (mécanismes formels assurant que tout changement de fonction entraîne, en temps opportun, une révision et un retrait des droits et des privilèges qui ne sont plus requis);
- Application du principe du moindre privilège (alignement sur les responsabilités actuelles des employés et revue périodique, notamment les accès à privilèges élevés);
- Alignement entre le rôle réel d'un employé et les autorisations associées à ce rôle;
- Ségrégation des fonctions/tâches entre les fonctions opérationnelles et les fonctions de surveillance, telles que la conformité et la gestion des risques, afin de prévenir les conflits d'intérêts et de réduire les risques de fraude interne;
- Journalisation, traçabilité et surveillance des activités.

1 Les scénarios présentés dans cette annexe ont été élaborés pour illustrer les risques potentiels et partager les bonnes pratiques mises en place pour les mitiger. Il ne s'agit pas de cas réels.

Hameçonnage

Exemple de scénario fictif

Un employé reçoit un courriel semblant provenir de l'équipe de sécurité informatique de l'institution, indiquant qu'une mise à jour urgente du système d'authentification est requise à l'aide d'un lien menant à une page qui imite le portail interne de connexion.

Lorsque l'employé clique sur le lien, il y saisit ses identifiants, qui sont récupérés par les fraudeurs pour tenter d'accéder aux systèmes internes de l'institution.

Risques encourus

Cette situation peut générer plusieurs risques, dont :

- Risque de bris de confidentialité (critique), d'abus et de fraude :
  - — données personnelles, confidentielles et financières potentiellement exposées;
  - — fraude, usurpation d'identité, hameçonnage (phishing) ciblé;
  - — rançongiciel possible;
  - — bris d'intégrité;
  - — systèmes compromis/mouvement latéral;
- Risque réglementaire (p. ex. obligation de divulgation);
- Risque d'atteinte à la réputation.

Exemples de mesures d'atténuation et bonnes pratiques identifiées

Parmi les exemples de bonnes pratiques, on retrouve notamment :

- La formation et la sensibilisation à la sécurité de l'information pour tous les utilisateurs;
- Les tests d'hameçonnage auprès de tous les employés, incluant la haute direction et le conseil d'administration;
- La détection et la validation des courriels d'hameçonnage;
- La validation des accès Internet afin de filtrer les sites malicieux;
- Le déploiement d'un système de sécurité sur les points terminaux pour assurer une détection et une réponse rapides en cas de compromission;
- L'inclusion d'une bannière lors de la réception de courriels provenant de l'externe;
- L'authentification multifacteurs (MFA) ou l'utilisation de clés d'accès pour tout accès externe à l'institution.

Vol/Fraude interne

Exemple de scénario fictif

Un employé malveillant de l'institution a profité de ses accès privilégiés pour manipuler discrètement les données de plusieurs dossiers de réclamations afin de rediriger les paiements vers des comptes frauduleux qu'il contrôle.

Risques encourus

Cette situation peut générer plusieurs risques, dont :

- Risque d'abus et de fraude :
  - — données volées utilisées pour tenter d'accéder à des comptes ou pour effectuer des transactions financières frauduleuses;
  - — pertes financières;
  - — atteinte à la réputation.

Exemples de mesures d'atténuation et bonnes pratiques identifiées

Parmi les exemples de bonnes pratiques, on retrouve notamment :

- Le renforcement de la surveillance des accès privilégiés (modifications des champs plus sensibles, telles les coordonnées des clients et les informations bancaires) et de l'utilisation des accès privilégiés;
- La gestion des identités et des accès (GIA) :
  - — ségrégation des tâches et application du principe du moindre privilège;
  - — système de tickets pour autoriser les accès privilégiés;
  - — voûte accordant des mots de passe à usage unique pour ces types d'accès, lesquels sont journalisés;
- La surveillance active de la fraude : règles renforcées, vérifications accrues au centre de contact, détection comportementale, envoi d'une confirmation ou d'un avertissement par courriel lors des changements aux coordonnées des clients;
- La réalisation d'enquêtes préembauche.

Tiers

Exemple de scénario fictif

Un fournisseur externe ou un fournisseur de services infonuagiques responsable de la gestion des dossiers clients d'une institution financière subit une intrusion informatique ciblée, permettant à des acteurs malveillants d'exfiltrer un lot de données comprenant des renseignements personnels et des informations financières sensibles.

Risques encourus

Cette situation peut générer plusieurs risques, dont :

- Risque de bris de confidentialité (critique) :
  - de données personnelles et financières exposées;
- Risque accru : fraude, usurpation d'identité, hameçonnage (*phishing*) ciblé;
- Risque réglementaire (p. ex. obligation de divulgation, risques de sanctions ou de non-conformité);
- Risque d'atteinte à la réputation;
- Risque opérationnel entraînant :
  - une activation de la réponse aux incidents : analyses, communication, coordination juridique;
  - une perturbation des opérations si le fournisseur est indisponible;
- Risques liés aux tiers résultant :
  - des failles dans les contrôles du fournisseur;
  - des clauses contractuelles potentiellement insuffisantes (notification, audits et responsabilités).

Exemples de mesures d'atténuation et bonnes pratiques identifiées

Parmi les exemples de bonnes pratiques, on retrouve notamment :

- L'évaluation du risque des tiers en amont et l'exigence qu'ils se conforment aux pratiques de sécurité et/ou détiennent une certification en sécurité, comme SOC 2 Type 2 ou certification spécifique au domaine d'affaires;
- Le renforcement des accès associés au fournisseur (rotation immédiate des clés, jetons, comptes et authentification multifacteurs);
- La surveillance active de la fraude : règles renforcées, vérifications accrues au centre de contact, détection comportementale;
- La limitation des flux et des permissions du fournisseur (segmentation, accès minimaux, suspension des échanges non essentiels);
- La notification en temps opportun (gestionnaires/dirigeants et instances de l'institution, Commission d'accès à l'information, AMF et clients) et l'activation d'un plan de communication clair et transparent pour réduire le risque réputationnel;
- L'exigence, envers le fournisseur, d'un plan de remédiation et d'amélioration des contrôles, l'obtention d'une preuve de correction et la réalisation d'une revue contractuelle (prévoir des droits d'audit et des délais de notification).

Sans frais 1 877 525-0337
lautorite.qc.ca

Québec
418 525-0337
Place de la Cité, tour PwC
2640, boulevard Laurier, bureau 400
Québec (Québec) G1V 5C1

Montréal
514 395-0337
800, rue du Square-Victoria, bureau 2200
Montréal (Québec) H3C 0B4