2022–2024

Stratégie de cybersécurité

Réduire les risques et renforcer la résilience

BANQUE DU CANADA
BANK OF CANADA

MESSAGE DU CHEF DE L'EXPLOITATION

À titre de banque centrale du pays, la Banque du Canada a pour mandat en vertu de la loi de promouvoir la stabilité et la résilience opérationnelle de notre système financier. La Banque s'est engagée à permettre aux Canadiens d'avoir la confiance nécessaire pour saisir les opportunités pour :

- Favoriser la stabilité économique et financière;
- Affronter les changements incessants avec rigueur et intégrité;
- Contribuer à accroître la prospérité collective au Canada.

Notre leadership en matière de cybersécurité dans le secteur financier contribue à la réalisation de cette promesse. Un niveau de résilience élevé est essentiel à la sécurité de l'ensemble du système financier canadiens incluant celle de ses participants.

Les cyberattaques sont plus complexes, plus dommageables et plus difficiles à prévenir que jamais. Les résultats de l'enquête[1] de la Banque démontrent que les entreprises canadiennes considèrent les cyberincidents comme l'un des principaux risques pour les entreprises individuelles et le système financier.

Bien que le niveau de cybersécurité de la Banque se soit amélioré globalement, les cybermenaces ne disparaîtront jamais. La Banque doit continuer de développer ses initiatives internes et externes de cyberrésilience.

La stratégie de cybersécurité 2022-2024 nous donne un plan pour y parvenir. Cette stratégie est guidée par notre appétit pour le risque en matière de cybersécurité et par une vision stratégique claire : renforcer la cyberrésilience du système financier canadien face aux menaces en constante évolution.

Filipe Dinis, chef de l'exploitation

1 Les participants à l'enquête de la Banque sur le système financier du printemps 2021 identifient les cyberincidents comme l'un des trois principaux risques menaçant le système financier.

INTRODUCTION

La cyberrésilience est l'une des plus grandes priorités de la Banque du Canada. Une cyberattaque contre n'importe quelle composante du système financier pourrait potentiellement provoquer un événement systémique susceptible de perturber l'économie canadienne.

En 2019, la Banque a élaboré sa première stratégie de cybersécurité pour orienter ses activités internes et externes ainsi que ses priorités en matière de cybersécurité. Des progrès considérables ont été accomplis depuis.

La Banque a mis en place des programmes de base tels que les tests d'intrusion et la gestion des identités et des accès. Elle a attiré de nouveaux talents et développé l'expertise de son équipe chargée de la cybersécurité et a déployé de nouvelles cybertechnologies et de nouveaux systèmes. Ces mesures sont devenues des éléments essentiels des opérations de la Banque.

La résilience des opérations et de la cybersécurité de la Banque a fait partie intégrante de son succès dans sa réponse à la pandémie de la COVID-19 et dans la reprise qui a suivie.

Parallèlement, la Banque a établi des relations solides et fructueuses avec des partenaires externes au Canada et dans le monde entier. Elle collabore avec eux pour favoriser la résilience en matière de cybersécurité dans de nombreux pays.

Tous ces efforts ont contribué à des améliorations importantes du profil de cyberrisque global de la Banque entre 2019 et 2021.

La résilience des opérations et de la cybersécurité de la Banque a fait partie intégrante de son succès dans sa réponse à la pandémie de la COVID-19 et dans la reprise qui a suivie. En plus de sa résilience, sa souplesse a aussi permis aux employés de faire la transition vers le travail à distance en toute sécurité, avec peu ou pas de perturbation des opérations de la Banque.

La stratégie de cybersécurité 2022-2024 orientera la prochaine étape du travail des équipes chargées de la cybersécurité et de l'ensemble des fonctions de la Banque. Elle donnera également aux partenaires externes une idée claire sur les intentions de la Banque.

Un nouvel énoncé sur l'appétit pour le risque en matière de cybersécurité a été élaboré afin de fixer des limites stratégiques et de fournir une orientation générale pour la gestion des cyberrisques.

LES CYBERMENACES POUR LA BANQUE DU CANADA

La complexité des cybermenaces a continué d'évoluer au cours de la pandémie de la COVID-19. Bien que certains de ces vecteurs d'attaque ne soient pas nouveaux, les cyberattaques quant à elles sont de plus en plus fréquentes et sophistiquées.

Pendant la pandémie[2], le secteur financier a été une cible attrayante pour les cyberopérateurs malveillants. Lorsque les employés et les consultants de la Banque ont commencé à travailler à distance en utilisant des réseaux domestiques moins sécurisés l'exposition aux cyberattaques et le profil de risque de la Banque, comme ceux des autres institutions, ont augmenté.

Les nouvelles cybermenaces sont également liées à l'évolution des activités et des processus de banque centrale, comme les systèmes de paiement actualisés, la monnaie numérique, la technologie de chaîne de blocs et la numérisation. La Banque continue de s'inquiéter d'une recrudescence éventuelle des activités d'espionnage et de sabotage, qui pourraient se traduire par un risque accru de vol de propriété intellectuelle et de renseignements exclusifs liés à ses activités ou pourraient paralyser ou perturber les systèmes financiers essentiels.

Les cybermenaces d'États-nations et de groupes parrainés par un État demeurent élevées et constituent une menace stratégique pour le Canada. Les États-nations ont été à l'origine de cyberattaques agressives dans le monde entier, utilisant les cyberopérations pour des gains financiers ou pour promouvoir leurs intérêts nationaux.

À l'échelle mondiale, les institutions financières et les gouvernements constatent également une augmentation du nombre et de la complexité des attaques par rançongiciel[3], avec par exemple des demandes de paiement de rançons plus importantes et des tactiques d'attaque à multiples facettes.

Des incidents internationaux majeurs en 2020 et 2021 ont attiré l'attention sur les conséquences potentiellement dévastatrices de cyberattaques sur les infrastructures essentielles et sur la nécessité pour les organisations de gérer les cyberrisques liés aux tiers.

2 I. Aldasoro, J. Frost, L. Gambacorta et D. Whyte (2021), « COVID-19 and Cyber Risk in the Financial Sector », BIS Bulletin, Banque des règlements internationaux, no 37, janvier.

3 S. Lyngaas (2021), « US Financial Institutions Report Major Increase in Ransomware Payments to Cybercriminals », CNN Politics, 15 octobre

ÉVOLUTION DE LA CYBERSÉCURITÉ À LA BANQUE DU CANADA

Ces dernières années, la Banque a établi une base solide en matière de cybersécurité pour répondre aux besoins existants et émergents dans ce domaine. Depuis la publication de sa stratégie de cybersécurité en 2019, la Banque a continué à renforcer sa posture de cybersécurité.

À l'interne, la Banque a étendu ses capacités de cybersécurité dans les cinq fonctions du cadre de cybersécurité[4] du National Institute of Standards and Technology (NIST) des États-Unis.

La Banque a :

- Adopté une approche de la gestion des risques axée sur les principaux actifs de la Banque et des scénarios de cyberattaques préoccupants;
- Appliqué un modèle de lignes de défense avec une deuxième ligne de défense plus robuste;
- Donné la priorité à la formation et au perfectionnement du personnel dans un marché du travail très concurrentiel pour la cybersécurité;
- Renforcé les systèmes de protection et de détection pour répondre à l'évolution des techniques de cyberattaque;
- Mis en place un programme spécialisé de gestion des identités et des accès pour renforcer les contrôles et réduire la probabilité d'exploitation des comptes avec privilèges;
- Réalisé des investissements stratégiques dans de nouveaux outils et de nouveaux systèmes de surveillance qui ont facilité l'accès à distance aux données et les vidéoconférences pour les employés travaillant à distance;
- Renforcé la sensibilisation à la cybersécurité en organisant régulièrement des formations et des exercices sur l'hameçonnage et le harponnage à l'échelle de la Banque.

4 Le Cadre de cybersécurité du NIST est un cadre volontaire utilisé à l'échelle internationale par les entreprises, les administrations publiques et le milieu universitaire pour gérer les cyberrisques.

À l'externe, la Banque a collaboré avec des partenaires canadiens et internationaux des secteurs public et privé pour renforcer la cybersécurité des systèmes financiers nationaux et mondiaux.

La Banque a :

- Fait la promotion de la cybersécurité relative aux systèmes de paiement du Canada dans le cadre de sa surveillance des infrastructures des marchés financiers (IMF) désignées;
- Publié de nouvelles lignes directrices dans le document Cyberrésilience : attentes à l'égard des infrastructures de marchés financiers (IMF);
- Poursuivi son rôle de premier plan au sein du Groupe sur la résilience du secteur financier canadien - un forum pour les institutions financières canadiennes d'importance systémique et les organismes de réglementation afin de coordonner les réponses aux problèmes opérationnels systémiques dans le secteur financier, y compris les cyberincidents;
- Continué son travail sur le Programme de résilience du système de paiement de gros – une collaboration avec les six plus grandes banques du Canada et Paiements Canada pour partager des informations et renforcer la cyberrésilience du système de paiement de gros du Canada.

La Stratégie de cybersécurité 2022-2024 *représente le plan de la Banque visant à s'appuyer sur cette base et à continuer de renforcer la cybersécurité dans les années à venir.*

Regarder vers l'avenir

BUTS STRATÉGIQUES POUR 2022-2024

La Banque maintient la vision et la mission en matière de cybersécurité qu'elle a formulées en 2019.

Vision

Renforcer la cyberrésilience du système financier canadien face aux menaces en constante évolution.

Mission

Favoriser l'efficience et la stabilité du système financier canadien grâce à de solides connaissances et capacités en matière de cybersécurité, à des efforts de collaboration et de mise en commun de l'information et à un vaste processus de surveillance.

Les buts stratégiques, les résultats et les mesures à prendre ont été mis à jour pour correspondre à l'évolution des besoins de la Banque dans les mois et les années à venir.

Buts

1. Continuer à incorporer la cyberrésilience dans toutes les opérations courantes de la Banque du Canada, à mesure que celle-ci évolue.
2. Accroître la résilience du secteur financier en misant sur la collaboration et sur des partenariats.
3. Faire en sorte que le système financier inspire confiance grâce à des lignes directrices en matière de cybersécurité claires qui s'inscrivent dans le mandat de la Banque.

Appétit pour le risque en matière de cybersécurité :

La stratégie de cybersécurité cadre avec l'appétit pour le risque en matière de cybersécurité de la Banque. Les quatre éléments suivants orienteront l'évaluation du risque en matière de cybersécurité dans le cadre de l'atteinte des objectifs opérationnels de la Banque.

Compte tenu du rôle important de la Banque du Canada dans le système financier canadien et de l'impossibilité de prévenir tout cyberincident :

1. Tous nos employés comprennent leur rôle dans la protection des systèmes et des renseignements de la Banque, assument leurs responsabilités à cet égard et en exigent autant des partenaires et des fournisseurs;
2. Nos spécialistes en cybersécurité et notre système de cybersécurité, d'intervention et de reprise des opérations sont équivalents ou supérieurs à ceux de nos pairs;
3. Notre exposition aux cyberattaques est réévaluée stratégiquement pour équilibrer le ratio risques/occasions;
4. Nous collaborons avec des partenaires certifiés et prenons des risques calculés pour optimiser la cybersécurité de la Banque et celle du système financier canadien.

Les sections ci-dessous présentent les priorités internes et externes de la Banque en matière de cybersécurité qui contribueront à l'atteinte de ces buts au cours des trois prochaines années.

Priorités internes

Les capacités de résilience actuelles de la Banque constitueront une base solide pour la gestion des cyberrisques sur la période 2022-2024. La cybersécurité demeurera un élément essentiel de la gestion des nouvelles technologies et des plateformes numériques qui soutiendront les grandes fonctions de la Banque dans les années à venir.

Avec la complexité accrue des besoins commerciaux, des technologies et des menaces, les unités fonctionnelles deviendront des partenaires pleinement intégrés dans la gestion des cyberrisques.

La Banque mettra davantage l'accent sur le modèle « confiance zéro[5] » pour la cyberdéfense, qui part du principe que tous les appareils connectés comportent un certain risque, même au sein de réseaux sécurisés. La Banque travaillera également avec des partenaires des secteurs public et privé pour se préparer à la nouvelle ère de l'informatique quantique.

Répondre au marché concurrentiel des talents en cybersécurité demeure une priorité. Outre les stratégies visant à identifier et à recruter de nouvelles personnes, la Banque s'efforcera de conserver ses employés expérimentés. L'accent sera mis sur la diversité et l'inclusion, la formation et le perfectionnement des compétences.

La Banque regroupera à nouveau ses objectifs internes, ses résultats et ses mesures stratégiques selon les cinq **catégories NIST :** identifier et gérer, protéger, détecter, intervenir et rétablir. Les investissements dans les catégories identifier, protéger et détecter se poursuivront, mais, comme les cyberattaques ne peuvent pas être complètement évitées, la nouvelle stratégie met davantage l'accent sur les initiatives d'intervention et de rétablissement.

IDENTIFIER ET GÉRER | **PROTÉGER** | **DÉTECTER** | **INTERVENIR** | **RÉTABLIR**

5 « Confiance zéro » est le terme utilisé pour désigner un ensemble de paradigmes de cybersécurité en constante évolution, qui font passer les défenses des périmètres statiques basés sur les réseaux aux utilisateurs, aux actifs et aux ressources. SP 800-207, Zero Trust Architecture | CSRC (nist.gov)

Catégorie 1 **IDENTIFIER ET GÉRER**

Intégrer la cybersécurité aux activités de la Banque du Canada

La Banque veillera à ce que ses employés, son infrastructure et ses actifs atteignent les objectifs conformément à l'énoncé sur l'appétit pour le risque en matière de cybersécurité.

Résultats

- Les processus de gestion des cyberrisques sont bien définis, appliqués et évalués pour une prise de décisions efficace basé sur les risques;
- La Banque attire, fidélise et développe des talents dans le domaine de la cybersécurité, dans une optique de diversité et d'inclusion;
- La Banque dispose d'un plan défini pour parvenir à la résilience quantique.

Mesures

- Faire progresser la mise au point de processus et d'outils de gestion des cyberrisques;
- Mettre en œuvre la nouvelle stratégie relative aux employés;
- Mettre à l'épreuve le cadre de préparation en matière d'informatique quantique et évaluer la résilience des systèmes.

Catégorie 2 **PROTÉGER**

Assurer une posture proactive contre les cyberattaques

La Banque utilisera efficacement ses systèmes, ses outils et ses politiques de cybersécurité pour sécuriser ses informations et ses actifs numériques. L'accent sera mis sur l'adoption d'une architecture « confiance zéro ».

Résultats

- Les identités avec privilèges sont rigoureusement protégées et automatisées grâce au cycle de vie des identités;
- Le programme de sensibilisation à la cybersécurité prend en compte les menaces émergentes;
- Le programme de mise à l'épreuve de la cybersécurité permet de maintenir une excellente cyberhygiène;
- Des contrôles de prévention des pertes de données et de sécurité des applications sont mis en œuvre d'après des scénarios de risque précis.

Mesures

- Continuer d'améliorer les contrôles de gestion des identités et des accès;
- Augmenter les initiatives de la sensibilisation à la cybersécurité;
- Continuer de faire évoluer le Programme des tests de cybersécurité;
- Faire progresser les mesures de prévention des pertes de données et de sécurité des applications.

Catégorie 3 **DÉTECTER**

Renforcer les systèmes pour détecter et identifier les cyberincidents

La Banque fera progresser l'intégration de la collecte de renseignements sur les menaces, les outils de détection et la surveillance de la cybersécurité.

Résultats

- L'analytique de détection évoluée est exploitée, notamment pour les cybermenaces hautement prioritaires;
- La collecte de renseignements sur les menaces, les outils de détection et les processus de surveillance sont en place à l'échelle de la Banque.

Mesures

- Faire évoluer, automatiser et intégrer la surveillance de la cybersécurité;
- Préciser le cadre de renseignements sur les cybermenaces;
- Recourir davantage à l'analytique des données servant à la détection des menaces.

Catégorie 4 **INTERVENIR**

Renforcer les mesures pour limiter l'incidence d'un cyberincident potentiel

La Banque améliorera sa capacité à évaluer et à trier les cyberévénements et les cyberincidents et à intervenir le cas échéant.

Résultats

- Les interventions et processus en cas de cyberincidents sont bien établis et régulièrement mis à l'épreuve;
- Les décideurs et les intervenants ont accès aux données en temps opportun lors de cyberincidents.

Mesures

- Réaliser régulièrement des exercices à tous les niveaux de l'organisation pour tester les cyberdéfenses, les interventions et la prise de décision;
- Valider continuellement les stratégies d'intervention en cas d'incident;
- Développer des outils d'analytique évoluée pour faciliter la détection et l'intervention précoces.

Catégorie 5 **RÉTABLIR**

Améliorer la résilience opérationnelle pour assurer la reprise des activités après un cyberincident

La Banque améliorera sa capacité à rétablir les opérations clés en réponse aux cyberattaques.

Résultats

- Les protocoles de cybersécurité, de reprise des opérations et de récupération des données sont bien définis et régulièrement mis à l'épreuve;
- Les outils améliorés de récupération des données sont intégrés aux opérations de la Banque.

Mesures

- Augmenter la fréquence des exercices de mise à exécution du plan antisinistre lié aux cyberincidents;
- Continuer de perfectionner les outils, les guides et les plans de reprise;
- Augmenter la capacité de récupération des données afin d'inclure des cyberscénarios complexes.

Priorités internes

	IDENTIFIER ET GÉRER	PROTÉGER	DÉTECTER	INTERVENIR	RÉTABLIR
RÉSULTATS	Les processus de gestion des cyberrisques sont bien définis, appliqués et évalués pour une prise de décisions efficace basé sur les risques. La Banque attire, fidélise et développe des talents dans le domaine de la cybersécurité, dans une optique de diversité et d'inclusion. La Banque dispose d'un plan défini pour parvenir à la résilience quantique.	Les identités avec privilèges sont rigoureusement protégées et automatisées grâce au cycle de vie de l'identité. Le programme de sensibilisation à la cybersécurité prend en compte les menaces émergentes. Le programme de mise à l'épreuve de la cybersécurité permet de maintenir une excellente cyberhygiène. Des contrôles de prévention des pertes de données et de sécurité des applications sont mis en œuvre d'après des scénarios de risque précis.	L'analytique de détection évoluée est exploitée, notamment pour les cybermenaces hautement prioritaires. La collecte de renseignements sur les menaces, les outils de détection et les processus de surveillance sont en place à l'échelle de la Banque.	Les interventions et processus en cas de cyberincidents sont bien établis et régulièrement mis à l'épreuve. Les décideurs et les intervenants ont accès aux données en temps opportun lors de cyberincidents.	Les protocoles de cybersécurité, de reprise des opérations et de récupération des données sont bien définis et régulièrement mis à l'épreuve. Les outils améliorés de récupération des données sont intégrés aux opérations de la Banque.
MESURES	Faire progresser la mise au point de processus et d'outils de gestion des cyberrisques	Continuer d'améliorer les contrôles de gestion des identités et des accès	Faire évoluer, automatiser et intégrer la surveillance de la cybersécurité	Réaliser régulièrement des exercices à tous les niveaux de l'organisation pour tester les cyberdéfenses, les interventions et la prise de décision	Augmenter la fréquence des exercices de mise à exécution du plan antisinistre lié aux cyberincidents
	Mettre en œuvre la nouvelle stratégie relative aux employés	Augmenter les initiatives de la sensibilisation à la cybersécurité	Préciser le cadre de renseignements sur les cybermenaces	Valider continuellement les stratégies d'intervention en cas d'incident	Continuer de perfectionner les outils, les guides et les plans de reprise
	Mettre à l'épreuve le cadre de préparation en matière d'informatique quantique et évaluer la résilience des systèmes	Continuer de faire évoluer le Programme des tests de cybersécurité; Faire progresser les mesures de prévention des pertes de données et de sécurité des applications	Recourir davantage à l'analytique des données servant à la détection des menaces	Développer des outils d'analytique évoluée pour faciliter la détection et l'intervention précoces	Augmenter la capacité de récupération des données afin d'inclure des cyberscénarios complexes

Priorités externes

Les activités de cybersécurité internes et externes de la Banque sont de plus en plus interreliées, particulièrement dans le cas des systèmes déterminants et essentiels, comme les systèmes de compensation et de règlement des paiements, d'adjudication des titres et de gestion des réserves de change.

La coordination entre les secteurs public et privé au Canada et à l'étranger, est essentielle. Le partage de l'information aide toutes les parties à définir et à gérer les cybervulnérabilités et les cyberrisques liés au système financier et à se préparer conjointement à intervenir en cas de cyberattaques qui pourraient toucher des partenaires individuels ou des systèmes plus vastes ainsi qu'à rétablir les activités.

À l'échelle nationale, la Banque collabore avec des partenaires fédéraux du secteur financier, d'autres organismes de sécurité du secteur public, le secteur financier et les commissions provinciales des valeurs mobilières dont les responsabilités comportent des cyberrisques. À l'échelle internationale, elle participe aux travaux liés à la cybersécurité effectués par le G7 et le Comité sur les paiements et les infrastructures de marché, entre autres.

Les travaux visant à améliorer la cyberrésilience des IMF sont continus. La Banque surveille les IMF désignées dont les responsabilités de compensation et de règlement des paiements jouent un rôle important dans la stabilité du système financier.

La Banque se préparera à jouer un nouveau rôle de gestion du cadre de supervision des paiements de détail qui entrera en vigueur vers 2024. La Banque supervisera la gestion des risques opérationnels effectuée par les fournisseurs de services de paiement et veillera au respect des exigences obligatoires, le cas échéant.

La Banque réagira également à l'évolution rapide du contexte des menaces externes et des tendances en matière de technologie de l'information et de numérisation. Cela comprend des initiatives potentielles telles que l'introduction d'une monnaie numérique de banque centrale (MNBC) et la planification à long terme du chiffrement de sécurité des ordinateurs quantiques.

RENFORCER **AMÉLIORER** **FAIRE PROGRESSER** **FAIRE ÉVOLUER**

Catégorie 1 **RENFORCER**

Renforcer la résilience du système financier

La Banque favorisera la stabilité du système financier canadien en élaborant et en mettant en œuvre des mesures de collaboration visant à accroître la résilience en matière de cybersécurité.

Résultats

- Collaboration fructueuse avec les institutions financières d'importance systémique pour augmenter la résilience du système financier;
- Compréhension, analyse et documentation des cyberrisques auxquels le système financier canadien est exposé;
- Parties prenantes du système financier en mesure d'intervenir en cas de cyberincident touchant l'ensemble du système.

Mesures

- Concevoir un cadre de tests d'intrusion axés sur les menaces pour les principales institutions du secteur financier;
- Évaluer les cyberrisques auxquels les systèmes financiers sont exposés à l'aide de données sur les incidents, de modèles et de recherches;
- Participer aux exercices du Groupe sur la résilience du secteur financier canadien pour renforcer la coordination des interventions en cas d'incident.

Catégorie 2 **AMÉLIORER**

Améliorer la collaboration et les partenariats

La collaboration au sein de la Banque et avec les partenaires externes permettra de s'assurer que les risques en matière de cybersécurité pour les institutions financières canadiennes sont bien compris, communiqués et gérés.

Résultats

- Collaboration efficace avec les partenaires pour élaborer des stratégies de cybersécurité, des politiques et des initiatives réglementaires;
- Bon échange d'information relative au secteur financier avec les partenaires à l'échelle nationale et internationale.

Mesures

- Collaborer avec les partenaires du Programme de résilience du système de paiement de gros pour s'attaquer aux plus grands scénarios de cybersécurité auxquels le secteur financier canadien est confronté;
- Se servir des partenariats avec le Groupe sur la résilience du secteur financier canadien pour repérer et combler tout manque de coordination lors d'interventions sectorielles en cas d'incident opérationnel systémique;
- Contribuer aux travaux du groupe d'experts du G7 sur la cybersécurité visant à renforcer la cybersécurité à l'échelle mondiale.

Catégorie 3 **FAIRE PROGRESSER**

Faire progresser les pratiques de cybersécurité des infrastructures de marchés financiers (IMF)

La Banque continuera de remplir le mandat qui lui a été confié par la loi, qui consiste à favoriser la stabilité du système financier par la surveillance des IMF. Cela signifie notamment renforcer et améliorer les pratiques de cyberrésilience pour les IMF.

Résultats

- Attentes de la Banque en ce qui a trait à la cyberrésilience des IMF désignées[6], notamment pour les plans d'intervention et de reprise des opérations, satisfaites ou dépassées par les IMF;
- Lignes directrices concernant le signalement à la Banque des cyberincidents comprises et respectées par les exploitants d'IMF.

Mesures

- Utiliser les lignes directrices sur les attentes en matière de cyberrésilience pour les prochains examens d'assurance de base des IMF désignées;
- Collaborer avec les IMF désignées pour améliorer les interventions et la reprise des opérations en cas d'attaque par rançongiciel ou de compromission des données;
- Poursuivre la mise en œuvre des lignes directrices pour le signalement des cyberincidents par les IMF.

Catégorie 4 **FAIRE ÉVOLUER**

Faire évoluer les programmes de cybersécurité en fonction des tendances externes

La Banque réagira à l'évolution rapide du contexte des menaces externes et des tendances en matière de technologie de l'information et de numérisation. Pour ce faire, elle devra collaborer avec des organismes partenaires du gouvernement du Canada et du secteur privé.

Résultats

- Cybersécurité intégrée dans la conception du système de paiement de détail et à une éventuelle monnaie numérique de banque centrale;
- Contribution de la Banque à la préparation à long terme du Canada à l'arrivée de l'informatique quantique;
- Échange transfrontalier approprié d'information liée à la cybersécurité au sein du secteur financier facilité par la Banque.

Mesures

- Inclure la cybersécurité dans le nouveau mandat de la Banque pour la surveillance des paiements de détail;
- Intégrer la cybersécurité aux plans d'instauration d'une monnaie numérique de banque centrale;
- Contribuer aux recherches et à la planification relativement aux nouvelles technologies de chiffrement par l'entremise de la stratégie quantique nationale et du groupe de travail Quantum du gouvernement fédéral;
- Se pencher sur le rôle du Canada dans l'échange transfrontalier d'information au sein du secteur financier.

6 Le document Cyberrésilience : attentes à l'égard des infrastructures de marchés financiers, publié en octobre 2021, oriente la mise en œuvre des dispositions du document d'information du CPIM et de l'OICV pour les infrastructures de marchés financiers (IMF) au Canada.

External priorities

	RENFORCER	AMÉLIORER	FAIRE PROGRESSER	FAIRE ÉVOLUER
RÉSULTATS	Collaboration fructueuse avec les institutions financières d'importance systémique pour augmenter la résilience du système financier. Compréhension, analyse et documentation des cyberrisques auxquels le système financier canadien est exposé. Parties prenantes du système financier en mesure d'intervenir en cas de cyberincident touchant l'ensemble du système.	Collaboration efficace avec les partenaires pour élaborer des stratégies de cybersécurité, des politiques et des initiatives réglementaires. Bon échange d'information relative au secteur financier avec les partenaires à l'échelle nationale et internationale.	Attentes de la Banque en ce qui a trait à la cyberrésilience des IMF désignées , notamment pour les plans d'intervention et de reprise des opérations, satisfaites ou dépassées par les IMF. Lignes directrices concernant le signalement à la Banque des cyberincidents comprises et respectées par les exploitants d'IMF.	Cybersécurité intégrée dans la conception du système de paiement de détail et à une éventuelle monnaie numérique de banque centrale. Contribution de la Banque à la préparation à long terme du Canada à l'arrivée de l'informatique quantique. Échange transfrontalier approprié d'information liée à la cybersécurité au sein du secteur financier facilité par la Banque.
MESURES	Concevoir un cadre de tests d'intrusion axés sur les menaces pour les principales institutions du secteur financier	Bon échange d'information relative au secteur financier avec les partenaires à l'échelle nationale et internationale	Utiliser les lignes directrices sur les attentes en matière de cyberrésilience pour les prochains examens d'assurance de base des IMF désignées	Inclure la cybersécurité dans le nouveau mandat de la Banque pour la surveillance des paiements de détail
	Évaluer les cyberrisques auxquels les systèmes financiers sont exposés à l'aide de données sur les incidents, de modèles et de recherches	Se servir des partenariats avec le Groupe sur la résilience du secteur financier canadien pour repérer et combler tout manque de coordination lors d'interventions sectorielles en cas d'incident opérationnel systémique	Collaborer avec les IMF désignées pour améliorer les interventions et la reprise des opérations en cas d'attaque par rançongiciel ou de compromission des données	Intégrer la cybersécurité aux plans d'instauration d'une monnaie numérique de banque centrale
	Participer aux exercices du Groupe sur la résilience du secteur financier canadien pour renforcer la coordination des interventions en cas d'incident	Contribuer aux travaux du groupe d'experts du G7 sur la cybersécurité visant à renforcer la cybersécurité à l'échelle mondiale	Poursuivre la mise en œuvre des lignes directrices pour le signalement des cyberincidents par les IMF	Contribuer aux recherches et à la planification relativement aux nouvelles technologies de chiffrement par l'entremise de la stratégie quantique nationale et du groupe de travail Quantum du gouvernement fédéral
				Se pencher sur le rôle du Canada dans l'échange transfrontalier d'information au sein du secteur financier