BANQUE DU CANADA
BANK OF CANADA

Date de publication: 1 mars 2024

Non Délicat – Non-Sensitive

Lignes directrices visant les infrastructures de marchés financiers désignées : Déclaration des cyberincidents et des incidents liés aux technologies

Contexte

Aux termes de la *Loi sur la compensation et le règlement des paiements*, la Banque du Canada (la Banque) est responsable de la surveillance réglementaire des infrastructures de marchés financiers (IMF) susceptibles d'engendrer un risque systémique ou un risque pour le système de paiement au Canada[1].

Dans son rôle de surveillance, la Banque s'assure que les IMF désignées[2] mettent en œuvre des pratiques de gestion des risques appropriées. Ces pratiques doivent être conformes aux normes de gestion des risques de la Banque du Canada, lesquelles respectent les normes internationales énoncées dans les *Principes pour les infrastructures de marchés financiers* et les attentes de la Banque quant à la cyberrésilience des infrastructures de marchés financiers.

Le principe 17 des *Principes pour les infrastructures de marchés financiers* et la norme 12 des critères et normes de la Banque en matière de gestion des risques applicables aux systèmes de paiement importants donnent des directives de gestion du risque opérationnel pour les IMF susceptibles d'engendrer un risque systémique ou un risque pour le système de paiement, respectivement. Le risque opérationnel est le risque que des dysfonctionnements des systèmes d'information, des processus internes, des erreurs humaines ou des perturbations découlant d'événements extérieurs aboutissent à la réduction, à la détérioration ou à l'interruption des services fournis par une IMF. Les IMF doivent déterminer les sources plausibles de risque opérationnel, tant internes qu'externes, et atténuer leur impact en recourant à des systèmes, politiques,

[1] Dans les présentes lignes directrices, « IMF » désigne tant le système de compensation et de règlement que sa chambre de compensation (l'entité qui exploite l'IMF). Ces deux termes sont définis dans la *Loi sur la compensation et le règlement des paiements*.

[2] La *Loi sur la compensation et le règlement des paiements* confère au gouverneur de la Banque le pouvoir de désigner une IMF si elle est jugée susceptible d'engendrer un risque systémique ou un risque pour le système de paiement au Canada, et le ministre des Finances doit être d'avis qu'une telle désignation sert l'intérêt public. Pour la définition du risque systémique et du risque pour le système de paiement, consulter les lignes directrices concernant les activités de surveillance menées par la Banque.

procédures et contrôles appropriés.

Étant donné la dépendance accrue des IMF à l'égard des technologies, les risques technologiques et les cyberrisques peuvent avoir une incidence sur la disponibilité, la confidentialité et l'intégrité de leurs systèmes. Une défaillance technologique ou un cyberincident pourrait aussi entraîner des conséquences systémiques, par exemple si une cyberattaque perturbait les opérations essentielles d'une IMF pendant une période prolongée.

C'est pourquoi la Banque exige que les IMF désignées établissent un cadre de gestion du risque opérationnel, y compris les risques technologiques et les cyberrisques, conformément aux normes de la Banque en matière de gestion des risques. Les IMF doivent prendre les mesures qui s'imposent pour accroître leur résilience opérationnelle globale, et aviser sans délai la Banque de tout cyberincident ou incident lié aux technologies important.

Objet

Les IMF doivent signaler tout type d'incident opérationnel. Cependant, les présentes lignes directrices décrivent les exigences particulières de la Banque concernant la déclaration des cyberincidents et des incidents liés aux technologies.

Aux fins des présentes lignes directrices, un cyberincident ou incident lié aux technologies est défini comme suit :

- Un incident qui entraîne ou pourrait entraîner des répercussions sur les opérations d'une IMF, y compris sur la confidentialité, l'intégrité ou la disponibilité de ses systèmes et renseignements.

Critères de déclaration

La Banque s'attend à ce que les IMF signalent tous les cyberincidents et incidents liés aux technologies qui sont importants pour les IMF (IMF s'entend d'un système de compensation et de règlement ou de sa chambre de compensation).

Le degré d'importance d'un incident est défini en fonction de ses conséquences pour l'IMF, qu'elles soient directes ou indirectes. Les incidents classés parmi les deux niveaux de gravité les plus élevés du cadre d'intervention en cas d'incident de l'IMF sont réputés importants et doivent être signalés à la Banque. Si un incident a été signalé à une autre autorité de surveillance ou de réglementation, à une autorité policière ou à une autorité connexe, il doit également être signalé à la Banque.

Dans certains cas, une IMF pourrait avoir besoin de temps pour évaluer la nature et la gravité de l'incident et déterminer s'il est doit être considéré comme important. Pour évaluer le degré d'importance d'un cyberincident ou d'un incident lié aux technologies, l'IMF est invitée à s'appuyer sur son analyse des répercussions sur les opérations et son cadre interne d'intervention en cas d'incident de ce type. L'IMF doit aviser la Banque de tout incident susceptible d'être important avant même que toutes ses répercussions soient connues.

Portée des déclarations

Un incident important peut provenir de l'IMF ou d'une entité qui a des liens avec elle (IMF liée, fournisseur de services, participant, membre ou entité affiliée)[3]. Un incident qui touche une entité interconnectée pourrait être transmis à l'IMF elle-même, ou perturber les services essentiels que l'entité lui fournit à l'IMF. Par exemple, de nombreuses IMF s'appuient sur des technologies fournies par un tiers fournisseur de services. Par conséquent, un incident survenant chez un tel fournisseur pourrait entraîner des répercussions importantes pour l'IMF elle-même.

Le **tableau 1** présente la portée des déclarations.

- La colonne 1 définit trois catégories de conséquences que la Banque demande aux IMF de prendre en compte pour évaluer si un incident est important et doit être signalé.
- La colonne 2 donne une liste non exhaustive d'exemples d'incidents qui seraient considérés comme importants.

Tableau 1 : Portée des déclarations d'incidents

Domaines touchés	Exemples de répercussions importantes
1. Les services essentiels : • de paiement • de compensation centrale • de règlement de titres • de dépôt de titres Cela comprend les fonctions ou les technologies à l'appui de ces services, qu'ils soient fournis par l'IMF elle-même (le système de compensation et de règlement ou la chambre de compensation) ou confiés à une autre entité.	▪ Les systèmes essentiels de l'IMF ou les composantes principales de ceux-ci sont inaccessibles. ▪ Les systèmes d'entreprise de l'IMF sont compromis, et certaines fonctions sont désactivées. ▪ L'IMF ou ses participants ne sont pas en mesure d'honorer leurs obligations de règlement. ▪ Les membres compensateurs ne peuvent pas remplir les exigences de marge et de garanties. ▪ Les participants ne sont pas en mesure d'échanger des messages de paiement ou de les soumettre pour les opérations de compensation et de règlement. ▪ Les participants ne peuvent pas s'échanger des titres entre eux. ▪ Un fournisseur externe de technologies requises pour la prestation des services essentiels de l'IMF subit une panne. ▪ Un incident survenant dans un centre de données utilisé par l'IMF met celui-ci hors service, ce qui nuit aux opérations de l'IMF.

[3] Un fournisseur de services peut être une entité affiliée ou non affiliée.

2. Une entité affiliée qui exerce des activités indispensables aux services essentiels : • de paiement • de compensation centrale • de règlement de titres • de dépôt de titres	▪ L'IMF, une entité affiliée ou un tiers fournisseur de services subit un cyberincident ou un incident lié aux technologies qui entraîne : o un accès non autorisé aux systèmes ou une incapacité de ceux-ci à fournir les services essentiels de l'IMF o une perte financière o une atteinte à la réputation
3. La confidentialité, l'intégrité ou la disponibilité de l'information que l'IMF ou sa chambre de compensation traite, stocke ou transmet.	▪ L'IMF publie par inadvertance des renseignements de nature délicate (p. ex., les positions des membres compensateurs). ▪ Un cyberincident compromet l'intégrité des données essentielles de l'IMF (p. ex., transactions opérationnelles, données de référence, modèles de risque). ▪ L'IMF ne peut pas accéder à ses données essentielles.

Procédures de déclaration

La déclaration des incidents par les IMF se fait en trois étapes :

1. **Avis immédiat** – Lorsqu'une IMF repère un incident important ou potentiellement important, elle doit aviser immédiatement l'équipe de surveillance de la Banque par courriel.

2. **Déclaration initiale** – Dans les 24 heures (ou avant, si possible), l'IMF doit fournir à l'équipe de surveillance de la Banque une mise à jour concernant l'incident, en incluant les détails indiqués dans la section « Exigences de déclaration initiale » ci-dessous.

3. **Déclaration subséquente** – Dans les 20 jours ouvrables, l'IMF doit fournir des précisions sur l'incident, y compris une analyse de la cause fondamentale, en incluant les détails indiqués dans la section « Exigences de déclaration subséquente » ci-dessous. La déclaration doit être envoyée par courriel à l'équipe de surveillance de la Banque.

De plus, l'IMF doit fournir des mises à jour lorsque l'incident change d'état, au minimum lorsque :

- le service est rétabli
- l'incident a été entièrement résolu

Exigences de déclaration initiale

- Courte description de l'incident
- État actuel de l'incident
- Date et heure auxquelles l'incident s'est produit
- Date et heure auxquelles l'incident a été découvert ou repéré
- Date et heure auxquelles l'avis immédiat a été transmis à la Banque

- Description de la solution de contournement
- Délai de rétablissement estimé
- État de l'avis :
    - aux participants au système (Ont-ils été avisés? Si oui : indiquer le moment de l'avis et le nom de l'incident.)
    - à la direction générale de l'IMF
    - au conseil d'administration de l'IMF
    - aux groupes internes et externes de gestion des incidents (p. ex., le Groupe sur la résilience du secteur financier canadien)
    - aux autres autorités de réglementation ou de supervision
- Personnes-ressources de l'IMF :
    - nom
    - adresse courriel
    - numéro de téléphone
    - poste
- Date de l'incident
- Classification interne de l'incident
- Type et catégorie de l'incident
- Systèmes désignés [touchés ou visés par la déclaration]
- Indiquer si la direction générale de l'IMF a été avisée de l'incident
- Indiquer si le conseil d'administration de l'IMF a été avisé de l'incident
- Liens connus entre l'incident et tout incident déjà signalé

Exigences de déclaration subséquente

- Heure de début et de fin de l'incident et durée totale
- Description détaillée et exhaustive du problème, chronologie de l'incident et mesures prises
- Répercussions sur les services essentiels de l'IMF (p. ex., échéances de paiement non respectées)
- Manière dont l'incident a été découvert
- Mesures d'urgence prises durant l'incident, le cas échéant, et état actuel de ces mesures, y compris les échéanciers applicables
- Services essentiels de l'IMF touchés par l'incident
- Résultats de l'enquête
- Cause fondamentale
    - Si la cause fondamentale est connue : mesures prises pour la trouver
    - Si la cause fondamentale est inconnue : détails de l'enquête en cours et durée prévue
- Plan d'action pour éviter que ce type d'incident ne se reproduise (p. ex., surveillance améliorée, délais de réaction plus rapides, contrôles supplémentaires ou nouvelle technologie):
    - Mesures prises et dates d'achèvement

  - Mesures en cours et dates d'achèvement visées
- Si l'incident a été causé par une attaque malveillante : détails sur l'auteur de la menace, si connu
- Relation de l'incident avec un changement, s'il y a lieu
- Répercussions de l'incident sur d'autres parties prenantes (clients, fournisseurs, actionnaires, gouvernement, organismes de réglementation, etc.)
- Actifs touchés par l'incident, le cas échéant
- Lieux touchés par l'incident, le cas échéant

Tenue de documents

Les IMF sont tenues de garder à jour un registre de tous les cyberincidents et incidents liés aux technologies, qu'ils soient importants ou non, et de mettre cette information à la disposition de la Banque, si elle en fait la demande. La Banque peut demander à avoir accès à ces dossiers pour :

- mener ses examens d'assurance de base
- évaluer si les seuils d'importance relative fixés par les IMF permettent de recenser efficacement les types de cyberincidents et d'incidents liés aux technologies qui intéressent la Banque

La Banque exige que les IMF conservent ces dossiers pendant au moins trois ans.