BANQUE DU CANADA
BANK OF CANADA

Date de publication : Juin 2021
Non-Sensitive - Non Délicat

Lignes directrices concernant le signalement des cyberincidents et des incidents liés aux technologies de l'information

Contexte

Les infrastructures de marchés financiers (IMF) jouent un rôle important dans la stabilité du système financier canadien. Leurs services sont essentiels aux particuliers et aux entreprises, car ils leur permettent d'acheter des biens et des services, d'investir dans des actifs financiers et de gérer les risques financiers de façon sûre et efficace. Compte tenu de leur rôle central, les IMF doivent adopter de solides pratiques de gestion des risques et être résilientes aux chocs.

La *Loi sur la compensation et le règlement des paiements* (la Loi) confie à la Banque du Canada la surveillance réglementaire des systèmes de compensation et de règlement (aussi connus sous le nom d'IMF[1]). La surveillance exercée par la Banque a pour objectifs de faire en sorte que les IMF désignées[2] fonctionnent en contrôlant adéquatement les risques, et d'accroître l'efficience et la stabilité du système financier canadien. Les IMF sont tenues de mettre en œuvre des pratiques de gestion des risques appropriées et 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 (PIMF)[3]. Le principe 17 des PIMF donne des directives aux IMF pour gérer le risque opérationnel, soit 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.

---

1 Dans les présentes lignes directrices, « IMF » désigne tant le système de compensation et de règlement que sa chambre de compensation, au sens de la Loi. Dans une optique de simplicité, on utilise ici le terme « opérateur » pour désigner la chambre de compensation de l'IMF.

2 La Loi 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. Pour obtenir 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 du Canada conformément à la *Loi sur la compensation et le règlement des paiements* ».

3 Les PIMF sont des normes internationales applicables aux IMF d'importance systémique, qui ont été publiées en 2021 par le Comité sur les paiements et les infrastructures de marché (CPIM), de concert avec l'Organisation internationale des commissions de valeurs (OICV). Les normes de la Banque relatives à la gestion des risques des systèmes de paiement importants (SPI) reposent sur les PIMF, mais sont formulées en fonction du niveau de risque présent dans un SPI, qui est relativement moins élevé que dans les IMF d'importance systémique.

Parmi les éléments importants à prendre en compte dans le cadre de gestion du risque opérationnel d'une IMF figurent les cyberrisques – la probabilité qu'un cyberincident se matérialise ainsi que ses conséquences. Au cours de la dernière décennie, le nombre de cyberincidents qui ont entraîné ou auraient pu entraîner des pertes financières substantielles a augmenté de façon soutenue [4]. Ces incidents sont plus courants et plus coûteux dans le secteur financier, et susceptibles de perturber les opérations essentielles d'une IMF. Un cyberincident pourrait aussi avoir des conséquences systémiques dans certains scénarios, par exemple, si une cyberattaque perturbait les opérations essentielles d'une IMF pendant une période prolongée.

Des incidents opérationnels liés à des défaillances des systèmes de technologie de l'information (TI) pourraient avoir des conséquences similaires. À titre d'exemple, les erreurs de mise en place et de traitement TI surviennent peu souvent, mais les pertes qu'elles occasionnent sont élevées par rapport à celles engendrées par les cyberincidents, et certains incidents ont causé une panne prolongée des systèmes[5]. C'est pourquoi la Banque exige que les IMF désignées établissent un cadre de gestion des cyberrisques et des risques opérationnels, conformément aux normes de la Banque en matière de gestion des risques[6]. Les IMF doivent prendre les mesures qui s'imposent pour accroître leur cyberrésilience et leur résilience opérationnelle globale, et aviser sans délai la Banque de tout cyberincident ou de tout incident TI important.

Objet

Les présentes lignes directrices décrivent les exigences de la Banque à l'égard des IMF désignées concernant le signalement des cyberincidents et des incidents TI. Sachant que les IMF sont actuellement tenues de signaler tout type d'incident opérationnel, les présentes lignes directrices apportent des éclaircissements supplémentaires quant au signalement des cyberincidents et des incidents TI. Aux fins des présentes lignes directrices, un cyberincident est défini comme suit :

> *Un événement qui compromet la cybersécurité (soit la confidentialité, l'intégrité ou l'accessibilité) d'un système ou l'information que le système traite, stocke ou transmet; ou qui constitue une violation ou une menace imminente de violation des politiques de sécurité, des procédures de sécurité ou des politiques sur les usages approuvés*[7].

4 Banque du Canada (2019). *Revue du système financier*.

5 N. Chande et D. Yanchus (2019), *Cyberincidents : état des lieux*, note analytique du personnel nº 2019-32, Banque du Canada.

6 Outre les PIMF, la Banque exige des IMF qu'elles respectent les directives énoncées dans le document intitulé *Guidance on Cyber Resilience for Financial Market Infrastructures*, qui a été rédigé par le CPIM et l'OICV pour compléter les PIMF, compte tenu des risques croissants que les cybermenaces font peser sur la stabilité financière.

7 Adaptation de la définition de « computer security incident » (incident de sécurité informatique) du National Institute of Standards and Technology (NIST), consultable à l'adresse https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf (en anglais seulement). Voir également le Règlement 24-102 sur les obligations relatives aux chambres de compensation et l'Instruction générale connexe.

Cette définition vise à englober la divulgation, la modification, la perte ou l'utilisation abusive d'informations (quelle qu'en soit l'origine, y compris les initiés) ainsi que les perturbations ou les pannes survenant au sein de l'IMF.

Les incidents opérationnels liés à des défaillances des systèmes TI qui ne relèvent pas de la cybersécurité peuvent également entraîner des pannes ou des perturbations ainsi que des pertes d'information. Étant donné qu'il peut être difficile pour l'IMF de faire initialement la distinction entre un cyberincident et un incident TI, les présentes lignes directrices s'appliquent au signalement de ces deux types d'incidents.

Portée des signalements

La Banque s'attend à ce que les IMF signalent tous les cyberincidents et incidents TI (ci-après dénommés des incidents) qui sont importants pour les IMF (IMF s'entend d'un système de compensation et de règlement ou de son opérateur). Le degré d'importance d'un incident est défini en fonction de ses conséquences pour l'IMF, qu'elles soient directes ou indirectes. Un incident important peut provenir de l'IMF elle-même ou d'une entité qui a des liens avec celle-ci (IMF liées, prestataires de services[8], participants ou membres, fournisseurs ou entités apparentées). Un incident qui touche une entité interconnectée pourrait être transmis à l'IMF elle-même, ou perturber les services essentiels que l'entité interconnectée fournit à l'IMF. Par exemple, de nombreuses IMF s'appuient sur des TI fournies par un prestataire de services externe. Par conséquent, un incident survenant chez le prestataire de services TI pourrait avoir des répercussions importantes pour l'IMF elle-même.

La portée des signalements est décrite dans le tableau ci-dessous. Dans la première colonne sont définies 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 seconde colonne contient des exemples de types de conséquences négatives qui entraîneraient la classification d'un incident comme étant important. Cette liste d'exemples n'est pas exhaustive.

Portée des signalements d'incident	
Catégorie de conséquences	**Exemple de conséquence négative**
Un incident est important s'il a ou pourrait avoir des conséquences négatives sur :	Exemples de conséquences négatives qui déclencheraient un signalement :
1. Les services essentiels de paiement, de compensation centrale ou de règlement et de dépôt de titres de l'IMF, y compris les fonctions ou les technologies à l'appui de ces services, qu'ils soient fournis par l'IMF elle-même ou confiés à une autre entité	▪ L'IMF pourrait ne pas être en mesure de respecter le délai de deux heures visé pour la reprise des opérations essentielles. ▪ L'IMF ou ses participants n'honoreront pas leurs obligations de règlement. ▪ Les membres compensateurs ne peuvent pas soumettre leurs dépôts de garantie. ▪ 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 titres ne peuvent être transférés entre les participants.

8 Un prestataire de services peut être une entité non liée ou apparentée.

	▪ Le fournisseur externe des TI pour les 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 pendant une longue période.
2. L'opérateur de l'IMF ou une entité apparentée effectuant des activités indispensables aux services essentiels de paiement, de compensation centrale ou de règlement et de dépôt de titres	▪ Les systèmes d'entreprise de l'IMF sont compromis, et certaines fonctions sont désactivées. ▪ Une entité apparentée a subi une attaque qui pourrait se traduire par une perte financière importante ou une atteinte à la réputation. ▪ Un incident qui se produit dans une entité apparentée pourrait compromettre sa capacité à fournir des services indispensables aux services essentiels de l'IMF. ▪ Un incident chez un prestataire de services externe constitue une menace réelle ou crédible pour l'image de marque, la réputation, les objectifs stratégiques de l'IMF ou la confiance qu'elle inspire.
3. La confidentialité, l'intégrité ou la disponibilité de l'information que le système ou l'opérateur de l'IMF traite, stocke ou transmet[9]	▪ 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 professionnelles, données de référence, modèles de risque). ▪ L'IMF ne peut accéder à ses données essentielles.

Il incombe à chaque IMF de déterminer quels incidents sont importants et doivent donc être signalés à la Banque. Pour évaluer le degré d'importance d'un cyberincident, l'IMF est invitée à s'appuyer sur son analyse des répercussions sur les opérations et son cadre interne d'intervention en cas de cyberincident et d'incident IT. 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.

Procédures de signalement

Dès qu'un incident important est détecté, les IMF sont tenues d'aviser sans délai le directeur responsable de la surveillance des IMF [10]. Les détails de l'incident doivent être envoyés par écrit et une copie doit être adressée au directeur principal, Surveillance, de la Banque ainsi qu'à toute autre personne-ressource spécifiée par la Banque. L'IMF concernée doit fournir de nouvelles informations si le statut de l'incident évolue, notamment et obligatoirement lors de la reprise des services et une fois que

9 Le principe 17 (3.17.12) des PIMF exige des IMF qu'elles disposent de politiques, de normes, de pratiques et de contrôles solides et robustes concernant la sécurité de l'information, de manière à ce que toutes les parties prenantes conservent un niveau de confiance approprié dans l'IMF. De plus, les objectifs et politiques d'une IMF relativement à la sécurité de l'information devraient respecter des normes raisonnables de confidentialité, d'intégrité et de disponibilité, entre autres.

10 Pour alléger son fardeau réglementaire, l'IMF peut répondre à cette attente en informant simultanément la Banque et les autres instances de réglementation, le cas échéant.

l’incident a été entièrement résolu. Les IMF doivent utiliser le modèle de rapport d’incident opérationnel de la Banque pour communiquer les détails de l’incident en mettant ledit rapport à jour tel qu’exigé à des moments précis au cours du cyberincident.

Conservation des dossiers

Les IMF sont tenues de garder à jour un registre de tous les cyberincidents, 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 et afin d’évaluer si les seuils d’importance relative fixés par les IMF permettent de recenser efficacement les types de cyberincidents qui intéressent la Banque. La Banque demande aux IMF de conserver ces dossiers pendant au moins trois ans.