BANQUE DU CANADA
BANK OF CANADA

La Banque du Canada recueille de l'information auprès du secteur et de parties prenantes afin de mieux comprendre l'écosystème des services de paiement de détail. Le présent document et les scénarios, diagrammes et questions qu'il renferme sont destinés à améliorer la compréhension de la Banque du Canada et ne doivent pas être interprétés comme une indication d'éventuelles options législatives ou réglementaires.

Comité consultatif sur les paiements de détail

Risque opérationnel

29 et 30 juillet 2020

La présente note a pour but d'aider les participants à se préparer à la réunion de juillet 2020 du Comité consultatif sur les paiements de détail (le « Comité »). À cette réunion, les membres seront appelés à :

1. s'inspirer du modèle de gestion du risque opérationnel présenté dans le document de consultation de 2017 (ci-après) pour tracer les grandes lignes de l'approche en matière de gestion du risque opérationnel envisagée par la Banque du Canada (la « Banque »);
2. parvenir à une conception commune des principes généraux de l'approche proposée en vue de discussions approfondies sur des sujets particuliers aux prochaines réunions du Comité;
3. aider la Banque à mieux comprendre les pratiques actuelles de gestion des risques posés par des tiers, du risque opérationnel dans les cas où les fournisseurs de services de paiement (FSP) assurent des services auprès d'utilisateurs finaux dans divers territoires, et des risques liés à l'information et à la cybersécurité;
4. décider des sujets de discussion pour la prochaine réunion (ci-dessous).

Les questions qui suivent visent à faciliter la préparation à la réunion et ne sont pas obligatoires. Elles ne constituent pas une liste exhaustive et se veulent des pistes de discussion destinées à aider la Banque à recueillir de l'information sur la manière dont les FSP gèrent le risque opérationnel.

Ce qui ressortira de la réunion aidera à orienter de prochains échanges avec le Comité, et à plus grande échelle avec le secteur des services de paiement, en ce qui concerne la gestion du risque opérationnel.

Objectifs et portée

Le risque opérationnel a trait aux processus ou aux systèmes internes inadéquats ou défaillants, à l'erreur humaine ou aux événements externes qui pourraient interrompre ou compromettre les services de paiement. Ce type de risque peut nuire à la disponibilité, à la fiabilité et à la sécurité des services de paiement ainsi que des données et des fonds qui transitent par ces services.

Dans son document de consultation *Un nouveau cadre de surveillance des paiements de détail* publié en 2017 (le « document de consultation de 2017 »), le ministère des Finances du Canada postule qu'un cadre de surveillance destiné aux FSP devrait comprendre des mesures proportionnelles aux risques qu'ils représentent pour l'économie et qu'en conséquence, l'accent serait mis sur la protection des utilisateurs finaux.

Les exigences de gestion du risque opérationnel envers les FSP devraient se rattacher à trois objectifs :

- **Intégrité :** Assurer l'exactitude des données et l'intégrité des systèmes.
- **Confidentialité :** Protéger les données pendant qu'elles sont stockées, utilisées ou transmises.
- **Disponibilité :** Maintenir un niveau raisonnable de fiabilité des services.

Il reviendra aux FSP de déterminer et d'atténuer tous les risques opérationnels pouvant nuire à leurs activités de paiements de détail, en accordant une attention particulière aux objectifs ci-dessus.

Comme pour d'autres cadres similaires, le cadre de surveillance des paiements de détail proposé devra englober les activités des **mandataires et des fournisseurs de services externes**[1]. De ce fait, les FSP seront responsables de gérer le risque opérationnel émanant de façon directe ou indirecte de leur relation avec ces personnes de la même manière que s'ils offraient le service ou assuraient la fonction en question eux-mêmes.

Cependant, le cadre **ne couvrira pas** les aspects suivants :

- La réglementation d'**autres activités opérationnelles** menées par les FSP – Conformément à l'approche fonctionnelle adoptée pour l'élaboration du cadre, les exigences en matière de risque opérationnel devraient être axées sur les risques opérationnels pouvant nuire aux activités de paiement des FSP. Cela dit, bien que les autres branches d'activité des FSP ne soient pas visées par le cadre, ceux-ci devront veiller à ce que leurs activités de paiement soient adéquatement protégées contre les risques opérationnels qui en découlent.
- L'atténuation, par les FSP, du **risque de recyclage des produits de la criminalité et de financement des activités terroristes** – Les FSP devront se conformer à la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* (LRPCFAT) et, pour ce faire, ceux qui offrent des services monétaires devront s'inscrire auprès du Centre d'analyse des opérations et déclarations financières du Canada (CANAFE).
- **La responsabilité en cas de fraude et les conventions d'indemnisation** – De manière générale, la fraude est une source de risque opérationnel pour les FSP. Même si l'établissement de la responsabilité ou de conventions d'indemnisation en cas de fraude ne sera pas du ressort du cadre, les exigences en matière de risque opérationnel, notamment celles visant la sûreté des systèmes informatiques, devraient prévoir que les FSP mettent en place des contrôles pour atténuer le risque de fraude.

Le **champ d'application géographique** du cadre proposé n'est pas explicitement soulevé dans le document de consultation de 2017.

- L'une des options examinées par le Comité consultatif du ministère des Finances sur le système de paiement consiste à suivre une approche semblable à celle qui a été établie dans la récente modification de la LRPCFAT.
- Aux fins du cadre de surveillance des paiements de détail, une telle approche assujettirait aux exigences du cadre même les FSP sans présence physique au Canada et qui assurent des fonctions de paiement à l'étranger, mais qui dirigent ou fournissent des services de paiement destinés à des utilisateurs finaux au Canada. Les FSP ayant une présence physique au Canada seraient tenus de se conformer aux exigences du cadre dans leurs activités avec leurs clients tant canadiens qu'étrangers. Le tableau ci-dessous résume les implications de cette approche potentielle.

---

[1] Un mandataire est une personne ou une entreprise qui représente un FSP (le mandant) et agit en son nom en vertu d'un contrat ou d'un mandat l'autorisant à exécuter des tâches précises (p. ex., l'exécution de fonctions de paiement au nom du FSP). Il n'est pas un employé du FSP. Un fournisseur de services externe est une personne ou une entité qui, en vertu d'un contrat, fournit au FSP un service lié à une fonction de paiement. Par exemple, un FSP peut sous-traiter une partie de ses activités à un fournisseur de services externe.

Emplacement du FSP	Emplacement de l'utilisateur final	Le FSP serait-il assujetti aux exigences du cadre?
Au Canada	Au Canada	Oui
Au Canada	À l'extérieur du Canada	Oui
À l'extérieur du Canada	Au Canada	Oui
À l'extérieur du Canada	À l'extérieur du Canada	Non

- Selon cette approche, les FSP à l'extérieur du Canada seraient assujettis aux exigences du cadre proposé (y compris les exigences de gestion du risque opérationnel) uniquement pour les services de paiement qu'ils offrent à des utilisateurs finaux au Canada. Quant aux FSP au Canada, ils seraient tenus de se conformer aux exigences dans toutes leurs activités de paiement.

1. **À l'heure actuelle, quelles sont vos pratiques de gestion et d'atténuation des risques liés à l'intégrité, à la confidentialité et à la disponibilité dans les cas où vos services sont fournis par :**
   a. **des mandataires;**
   b. **des fournisseurs de services externes (sous-traitance).**
2. **Avez-vous connaissance de difficultés actuelles ou potentielles quant au respect des exigences en matière de risque opérationnel dans les cas où vos services de paiement sont offerts à des utilisateurs finaux de plusieurs territoires? Le cas échéant, quelles sont-elles?**
   a. **Comment les FSP composent-ils avec ces difficultés en ce moment?**

Attentes

La présente section porte sur les **concepts** pouvant s'inscrire dans les attentes envers les FSP quant au risque opérationnel. **Ces concepts ne constituent pas un avant-goût du libellé, ou de la structure d'une loi, d'un règlement ou d'une ligne directrice à venir.**

Le document de consultation de 2017 indique que les attentes envers les FSP quant à la gestion du risque opérationnel seraient fondées sur le principe 17, *Risque opérationnel*, des *Principes pour les infrastructures de marchés financiers* (PIMF) publiés conjointement par le Comité sur les paiements et les infrastructures de marché (CPIM) et l'Organisation internationale des commissions de valeurs (OICV). Il énonce également que les PIMF sont des normes internationales conçues pour les institutions d'importance systémique. Dans ce même document, on propose des modifications aux exigences des PIMF pour qu'elles s'appliquent aux FSP :

- Un FSP devrait établir un cadre rigoureux de gestion des risques opérationnels comportant des systèmes, des politiques, des procédures et des contrôles appropriés pour déterminer, surveiller et gérer les risques opérationnels.
- La direction d'un FSP devrait définir clairement les rôles et les responsabilités liés au traitement du risque opérationnel et devrait appuyer le cadre de gestion des risques opérationnels du FSP. Les systèmes, les politiques opérationnelles, les procédures et les contrôles devraient être examinés, audités et testés périodiquement, ainsi qu'après des changements importants.
- Un FSP devrait définir clairement ses objectifs de fiabilité opérationnelle et devrait avoir des politiques en place visant à réaliser ces objectifs.

- Le système d'un FSP devrait comporter des politiques exhaustives sur la sécurité physique et des renseignements qui refléteraient toutes les vulnérabilités et menaces importantes possibles.
- Un FSP devrait avoir un plan de continuité des activités qui prend en compte les événements représentant un risque important d'interruption des activités. Le plan devrait être conçu de manière à protéger les renseignements et les données de paiement des utilisateurs finaux et à permettre la récupération de données exactes à la suite d'un incident. Le plan devrait viser également à atténuer l'incidence d'une interruption sur les utilisateurs finaux en ayant un plan de retour aux activités normales.
- Un FSP devrait déterminer, surveiller et gérer les risques que les utilisateurs finaux, les participants, autres FSP et fournisseurs de service (publics ou non) pourraient représenter pour ses activités. De plus, un FSP devrait identifier, surveiller et gérer les risques que ses activités pourraient représenter pour d'autres.

Les normes proposées dans le document de consultation de 2017 peuvent également être envisagées d'un **point de vue fonctionnel**. De façon générale, il est prévu que les FSP devront :

- se doter d'un cadre de gestion du risque opérationnel qui leur permettra :
  - de déterminer les risques opérationnels;
  - de protéger leurs activités de paiement contre ces risques (par des contrôles de protection);
  - de détecter les incidents opérationnels (par des contrôles de détection);
  - d'intervenir en cas d'incident, puis de reprendre leurs activités (par des mécanismes d'intervention).
- évaluer et tester leur cadre, ainsi que les politiques, procédures et contrôles connexes, et tirer des leçons de ces tests pour renforcer leurs capacités de gestion du risque opérationnel.

Par souci de clarté, le risque opérationnel serait divisé en sous-catégories (cybersécurité, sécurité de l'information, sécurité informatique, etc.). La pièce jointe n° 1 donne des précisions sur les concepts pouvant être couverts par une loi, un règlement ou une ligne directrice.

En faisant concorder les attentes envers les FSP en matière de risque opérationnel avec celles des PIMF (adaptées aux particularités du secteur des paiements de détail), on obtient **une approche qui cadre avec celle d'autres régimes de réglementation**, particulièrement les normes internationales pour les systèmes de paiement d'importance systémique et les exigences réglementaires canadiennes visant les systèmes de paiement importants[2].

Il est entendu que les FSP pourraient suivre d'autres normes (publiques ou sectorielles, par exemple) ou se conformer à des exigences d'autres territoires. Pour limiter les cas où des exigences réglementaires seraient en conflit, les attentes envers les FSP en matière de risque opérationnel cadreront avec ces autres normes et exigences dans la mesure du possible et selon la nature des risques posés par les FSP. Dans ses démarches avec le ministère des Finances, la Banque entend tenir compte des normes suivantes :

- Orientations de l'Autorité bancaire européenne sur la gestion des risques liés aux TIC et à la sécurité[3]

---

[2] De plus amples renseignements sur les systèmes de paiement importants et les systèmes d'importance systémique, de même que sur les exigences réglementaires pertinentes (fondées sur les PIMF), se trouvent sur le site Web de la Banque.

[3] Ces orientations entrent en vigueur en juin 2020 et remplacent les *Orientations relatives aux mesures de sécurité pour les risques opérationnels et de sécurité dans le cadre de la directive (UE) 2015/2366 (DSP2)*.

- Ligne directrice E-21 – Gestion du risque opérationnel du Bureau du surintendant des institutions financières
- Cadre de cybersécurité du National Institute of Standards and Technology
- Norme de sécurité des données de l'industrie des cartes de paiement
- COBIT 5 de l'ISACA
- Critical Security Controls for Effective Cyber Defense du Center for Internet Security
- ISO/IEC 27001 – Management de la sécurité de l'information
- ISO 31000 – Management du risque

En ce qui concerne la surveillance, une **approche fondée sur les risques** est également envisagée dans le document de consultation de 2017. Selon cette approche, tous les FSP devraient remplir les objectifs réglementaires visant la gestion du risque opérationnel, mais la façon d'y parvenir pourrait dépendre des caractéristiques uniques de chaque FSP. La Banque pourrait aussi soumettre certains FSP à un examen de conformité plus pointu ou plus fréquent que d'autres.

3. **Les risques liés à la sécurité de l'information et à la cybersécurité seront pris en compte dans les attentes envers les FSP en matière de risque opérationnel. Vos processus et politiques de gestion du risque opérationnel touchent-ils à ces risques ou ceux-ci sont-ils traités à part?**
4. **Les membres ont-ils des préoccupations quant aux normes qui pourraient être prises en considération dans l'élaboration des exigences en matière de risque opérationnel? Y a-t-il d'autres normes dont il faudrait tenir compte?**

Sujets à approfondir

À la prochaine réunion, la Banque demandera aux membres du Comité de se prononcer sur des points plus précis entourant les mesures de gestion du risque opérationnel qui seront intégrées dans le cadre de surveillance des paiements de détail. De pair avec le ministère des Finances, elle sollicitera aussi des avis quant aux mesures de gestion du risque opérationnel, notamment par le processus de consultation publique du gouvernement du Canada pour l'élaboration de règlements (*Gazette du Canada*) et une de ses propres consultations publiques.

Voici les points que la Banque tient à approfondir à la prochaine réunion :

- les objectifs de fiabilité opérationnelle;
- la détermination des risques opérationnels, dont ceux posés par des tiers (fournisseurs de services externes et mandataires);
- la protection contre le risque opérationnel (y compris les risques liés à la sécurité de l'information et à la cybersécurité) et la détection d'incidents potentiels;
- l'intervention en cas d'incident et la planification de la continuité des opérations;
- l'évaluation et les tests;
- les rôles et responsabilités;
- les ressources humaines et financières dont disposent les FSP pour gérer le risque opérationnel.

Certains éléments de la pièce jointe nº 1 seront également abordés pendant les discussions.

5. **Y a-t-il d'autres sujets touchant au risque opérationnel ou à tout autre élément de la liste ci-dessus dont la Banque devrait discuter avec les acteurs du secteur des paiements de détail?**

Pièce jointe n^{o} 1 – Concepts relatifs au risque opérationnel

La présente pièce jointe donne des précisions sur les concepts auxquels pourraient renvoyer des exigences en matière de risque opérationnel envers les FSP, que ce soit dans une loi, un règlement ou une ligne directrice. On y trouve aussi quelques exemples d'autres normes que la Banque et le ministère des Finances pourraient prendre en considération dans la définition de ces concepts. Les concepts présentés ci-dessous ne constituent pas un avant-goût du libellé, du niveau de détail ou de la structure d'une loi, d'un règlement ou d'une ligne directrice à venir. Les listes de concepts et d'exemples de normes ci-dessous ne sont pas exhaustives.

Principes	Concepts susceptibles de figurer dans une loi, un règlement ou une ligne directrice	Exemples d'autres normes pertinentes
1. Un FSP devrait établir un cadre rigoureux de gestion des risques opérationnels comportant des systèmes, des politiques, des procédures et des contrôles appropriés pour déterminer, surveiller et gérer les risques opérationnels.	Exemples d'éléments d'un bon cadre de gestion du risque opérationnel : • Procédures et systèmes nécessaires pour déterminer, mesurer, surveiller et gérer les multiples risques qui découlent des activités de paiement du FSP et ceux auxquels le FSP est exposé. Il faut, au minimum, un plan d'intervention et un plan de continuité des opérations, ainsi que des politiques de sécurité physique, de sécurité de l'information et de cybersécurité; • Principes généraux de gestion du risque opérationnel à l'échelle de l'organisation. Exemples d'objectifs pour le cadre : • Adopter une vue d'ensemble des risques (erreur humaine, cyberattaques, erreurs techniques, catastrophes naturelles, etc.); • Prendre en compte les liens d'interdépendance, c'est-à-dire les interactions entre les éléments du cadre et la cohérence interne du cadre (p. ex., façon dont les contrôles de prévention se conjuguent aux contrôles d'intervention). Ressources nécessaires pour instaurer et maintenir le cadre : • Accès à des ressources humaines et financières suffisantes pour déterminer, surveiller et gérer les risques opérationnels, ainsi qu'atteindre les objectifs de fiabilité et exécuter les plans de continuité des opérations.	Principe 17.1 des PIMF Ligne directrice E21 – Gestion du risque opérationnel du BSIF ISO 31000 – Management du risque

Principes	Concepts susceptibles de figurer dans une loi, un règlement ou une ligne directrice	Exemples d'autres normes pertinentes
	Il est recommandé au FSP de prendre en compte les facteurs suivants au moment de déterminer les risques : • Vulnérabilités et menaces plausibles (compte tenu de ses activités, de ses technologies, de sa présence physique au Canada ou à l'étranger, etc.); • Différentes sources potentielles (p. ex., erreur humaine, catastrophes naturelles, lacunes dans les systèmes, cybermenaces, risques associés aux autres activités du FSP); • Prise en compte des risques que comporte le recours aux services d'un mandataire ou d'un fournisseur de services externe. Exigences pratiques : • Le FSP a l'obligation d'établir un processus pour revoir et mettre à jour le cadre et les politiques, procédures et systèmes connexes. Le cadre doit être appliqué en permanence, y compris lorsque les activités du FSP changent.	
2. La direction d'un FSP devrait définir clairement les rôles et les responsabilités liés au traitement du risque opérationnel et devrait appuyer le cadre de gestion des risques opérationnels du FSP.	Exemples de rôles à définir : • Rôles et responsabilités divers : haute direction formulant et communiquant des orientations stratégiques, personnel de première ligne connaissant ses rôles et responsabilités en ce qui a trait au risque opérationnel (p. ex., mesures de contrôle des risques, responsabilités de signalement des événements), fonction d'analyse critique (sous une forme ou une autre) établie en interne; • Définition et attribution des rôles et responsabilités clés et des voies hiérarchiques nécessaires pour faire appliquer les mesures de sécurité et gérer la sécurité et les risques opérationnels, aussi bien en temps normal qu'en cas d'incident; • Rôles et responsabilités liés aux fournisseurs de services externes et aux mandataires. Les rôles précis à attribuer varieront selon le modèle d'affaires et les risques du FSP. • Par exemple, un FSP de grande taille ou aux activités complexes pourra envisager une séparation officielle des responsabilités et une structure à trois lignes de défense, tandis qu'un FSP aux activités simples n'aura peut-être pas besoin de définir autant de rôles.	Principe 17.2 des PIMF Orientations de l'ABE sur la gestion des risques liés aux TIC et à la sécurité

Principes	Concepts susceptibles de figurer dans une loi, un règlement ou une ligne directrice	Exemples d'autres normes pertinentes
3. Un FSP devrait définir clairement ses objectifs de fiabilité opérationnelle et devrait avoir des politiques en place visant à réaliser ces objectifs.	Au nombre des objectifs de fiabilité figurent idéalement la préservation de la confidentialité et de l'intégrité et le maintien de niveaux adéquats de disponibilité. Exemples d'objectifs plus précis : • Un délai de reprise visé, une mesure de la perte de disponibilité acceptable; • Un point de reprise visé, une mesure de la perte de données acceptable; • Un taux de disponibilité (pourcentage du temps où les activités sont possibles). Facteurs à prendre en compte au moment d'établir les objectifs de fiabilité en fonction des risques et des besoins opérationnels du FSP, comme l'incidence des activités du FSP sur les utilisateurs finaux et les tiers (p. ex., autres FSP, infrastructures de marchés financiers [IMF]). Il convient que les politiques et les procédures (p. ex., atténuation, continuité des opérations) soient conçues pour atteindre ces objectifs et que le FSP s'interroge sur son recours à des fournisseurs de services externes ou à des mandataires.	Principe 17.3 des PIMF Orientations de l'ABE sur la gestion des risques liés aux TIC et à la sécurité
4. Un FSP devrait déterminer, surveiller et gérer les risques que les utilisateurs finaux, les participants, autres FSP et fournisseurs de service (publics ou non) pourraient représenter pour ses activités. De plus, un FSP devrait identifier, surveiller et gérer les risques que ses activités pourraient représenter pour d'autres.	Dans la détermination des risques opérationnels (point 1 du tableau), le FSP doit envisager les risques auxquels d'autres peuvent l'exposer et, au besoin, les atténuer adéquatement. Il doit penser, entre autres, aux liens d'interdépendance suivants : • Utilisateurs finaux; • Autres FSP (parmi ses clients ou ses propres fournisseurs); • IMF (auxquelles il participe ou fournit des services); • Fournisseurs de services externes; • Mandataires. Le FSP doit réfléchir aux risques qu'il représente pour d'autres et en tenir compte au moment d'établir ses objectifs de fiabilité et de dresser ses plans d'intervention en cas d'incident et de continuité des opérations.	Principe 17.7 des PIMF Éléments de la ligne directrice E21 – Gestion du risque opérationnel du BSIF, principe 4

Principes	Concepts susceptibles de figurer dans une loi, un règlement ou une ligne directrice	Exemples d'autres normes pertinentes
5. Le système d'un FSP devrait comporter des politiques exhaustives sur la sécurité physique et des renseignements qui refléteraient toutes les vulnérabilités et menaces importantes possibles.	Il convient de protéger les données contre les pertes et les fuites, l'accès non autorisé et d'autres risques liés au traitement, tels que la mauvaise tenue de dossiers. Le FSP doit définir des contrôles de protection (prévention) et de détection ainsi que des mécanismes d'intervention pour chacun des risques déterminés : • Établir des normes de confidentialité, d'intégrité, d'authentification, d'autorisation, de non-répudiation, de disponibilité et d'auditabilité (reddition de comptes). • Disposer de politiques, de normes, de pratiques et de contrôles judicieux et robustes concernant la sécurité de l'information, de manière à ce que toutes les parties prenantes conservent un niveau de confiance approprié dans le FSP. • Disposer de politiques efficaces lui permettant d'évaluer et d'atténuer la vulnérabilité de ses sites physiques en cas d'attaques, d'intrusions et de catastrophes naturelles. Il ne faut pas non plus négliger les cyberrisques et les risques pour la sécurité de l'information : • Méthodes permettant d'établir quels types d'actifs informatiques, de données et de renseignements doivent être protégés contre les cyberattaques; • Évaluation de la nature et de la gravité du risque que représentent les cyberattaques pour les utilisateurs finaux et les autres entités interconnectées; • Faculté de détecter les cyberattaques et les intrusions, fructueuses ou infructueuses; • Procédures et politiques permettant d'intervenir en cas de cyberattaque ou d'intrusion et de reprendre les activités de manière à atteindre les objectifs de fiabilité tout en continuant de fournir des services de paiement sûrs et fiables.	Principe 17.5 des PIMF Cadre de cybersécurité du NIST Norme de sécurité des données de l'industrie des cartes de paiement COBIT 5 de l'ISACA Critical Security Controls for Effective Cyber Defense du Center for Internet Security ISO/IEC 27001 – Management de la sécurité de l'information
6. Les systèmes, les politiques opérationnelles, les procédures et les contrôles devraient être examinés, audités et testés périodiquement, ainsi	Conditions dans lesquelles un examen, un audit ou un test doit avoir lieu, et nature précise de chacun de ces processus. Façons d'appliquer les leçons tirées des tests ou des audits et de remédier aux lacunes ou aux vulnérabilités.	Principe 17.2 des PIMF Orientations de l'ABE sur la gestion des

Principes	Concepts susceptibles de figurer dans une loi, un règlement ou une ligne directrice	Exemples d'autres normes pertinentes
qu'après des changements importants[4].	Éléments de la gestion du risque opérationnel qu'il faut évaluer et tester (p. ex., plan de continuité des opérations, contrôles de cybersécurité, autres politiques, tests et évaluations des contrôles de protection et de détection ainsi que mécanismes d'intervention). Méthodes de conception et d'exécution des tests. Fréquence des tests, des audits et des examens : • Si certains processus doivent être testés tous les ans (p. ex., plan de continuité des opérations; possibilité de tester chaque année des parties différentes du plan), d'autres peuvent l'être moins souvent. • Les éléments du cadre de gestion du risque opérationnel peuvent être audités sur une période fixe. • Le cadre de gestion du risque opérationnel doit être examiné tous les ans. Le FSP doit choisir entre procéder lui-même aux tests, audits et examens ou les confier à un tiers.	risques liés aux TIC et à la sécurité
7. Un FSP devrait avoir un plan de continuité des activités qui prend en compte les événements représentant un risque important d'interruption des activités. Le plan devrait être conçu de manière à protéger les renseignements et les données de paiement des utilisateurs finaux et à	Le FSP doit surveiller et détecter les incidents opérationnels. But d'un plan de continuité des opérations : • Servir de plan structuré et clair pour réagir aux éventuels incidents, y compris ceux qui portent lourdement atteinte à la confidentialité, à l'intégrité ou à la disponibilité des activités de paiement de détail du FSP ou des systèmes informatiques, des données ou des renseignements facilitant ses fonctions de paiement.	Principe 17.6 des PIMF Orientations de l'ABE sur la gestion des risques liés aux TIC et à la sécurité

[4] Dans le document de consultation de 2017, ce principe faisait partie de l'attente selon laquelle les FSP devraient définir les rôles et responsabilités en ce qui a trait au risque opérationnel.

Principes	Concepts susceptibles de figurer dans une loi, un règlement ou une ligne directrice	Exemples d'autres normes pertinentes
permettre la récupération de données exactes à la suite d'un incident. Le plan devrait viser également à atténuer l'incidence d'une interruption sur les utilisateurs finaux en ayant un plan de retour aux activités normales.	Gouvernance d'un plan de continuité des opérations : • Il convient que le FSP assigne explicitement les responsabilités de la planification de la continuité des opérations et de la gestion des incidents et affecte des ressources adéquates à cette planification. Contenu d'un plan de continuité des opérations : • Le plan de continuité des opérations doit prévoir des étapes claires pour atteindre les objectifs du FSP quant à l'intervention en cas d'incident et à la reprise des activités d'une manière sûre et fiable. • Il doit nommer les événements qui risquent de grandement perturber les activités et tenir compte de l'impact sur le fonctionnement des infrastructures et des services essentiels. • Il doit permettre au FSP de maintenir les niveaux de service dans l'éventualité d'un événement de ce type et de continuer de fournir des services de paiement sûrs et fiables.	