BANQUE DU CANADA
BANK OF CANADA

Ligne directrice provisoire – Contexte

La *Loi sur les activités associées aux paiements de détail* et le *Règlement sur les activités associées aux paiements de détail* obligent les fournisseurs de services de paiement à respecter certaines exigences en matière de gestion des risques et de déclaration. La *Loi* confère aussi à la Banque du Canada le pouvoir de publier des lignes directrices pour établir ses attentes quant à l'application de ce cadre législatif.

Dans ses lignes directrices, la Banque présente les normes et les pratiques que les fournisseurs de services de paiement devraient incorporer dans leurs activités opérationnelles en vue de se conformer à la *Loi* et au *Règlement*.

En février 2024, nous avons amorcé une période de consultation de 90 jours auprès d'acteurs du secteur et d'autres parties prenantes pour recevoir leurs commentaires sur cette ligne directrice.

La consultation est maintenant terminée. La Banque en remercie les participants pour leurs commentaires, qui seront pris en compte dans la version définitive des lignes directrices.

La version définitive sera publiée durant la seconde moitié de 2024 avec un résumé anonymisé des commentaires reçus pendant la consultation.

Les fournisseurs de services de paiement peuvent continuer de se référer à cette version de la ligne directrice pour se préparer aux exigences de conformité.

Pour voir l'ensemble des politiques et des lignes directrices, rendez-vous à l'adresse https://www.banqueducanada.ca/SPD/#ressources.

BANQUE DU CANADA
BANK OF CANADA

Le risque opérationnel et la réponse aux incidents

Type de publication : Projet de ligne directrice pour consultation

Table des matières

Introduction 3

1. Documentation et disponibilité du cadre 6

2. Rôles et responsabilités 7

3. Ressources humaines et financières 9

4. Objectifs 12

5. Recenser 15

6. Protéger 19

7. Déceler 21

8. Réponse et rétablissement 24

9. Examen interne 28

10. Mises à l'essai 30

11. Examen indépendant 34

12. Tiers fournisseurs de services 36

13. Mandataires 43

Annexe A : Glossaire 47

Annexe B : Documentation du cadre 51

Annexe C : Objectifs, cibles de fiabilité et indicateurs 52

Annexe D : Éléments de protection concernant les technologies de l'information et la cybersécurité 54

Annexe E : Relation entre le contrôle continu, la détection des incidents et les plans de réponse et de rétablissement 59

Annexe F : Contrôles concernant les technologies de l'information et la cybersécurité 60

Annexe G : Examen interne 61

Annexe H : Mises à l'essai 62

Annexe I : Tiers fournisseurs de services 64

Annexe J : Mandataires 67

Introduction

La présente ligne directrice vise à aider les fournisseurs de services de paiement (FSP) assujettis à la *Loi sur les activités associées aux paiements de détail* (LAAPD) à remplir leurs obligations de gestion des risques opérationnels et de réponse aux incidents.

Résultats

- Le FSP établit, met en œuvre et maintient un cadre de gestion des risques et de réponse aux incidents en vue d'identifier et d'atténuer les risques opérationnels et de répondre aux incidents.
- Le FSP adapte son cadre à sa propre situation et veille à ce que ce cadre convienne à l'importance des risques auxquels il est exposé. Dans ce contexte, le cadre est proportionnel aux répercussions que pourraient avoir une entrave, une perturbation ou une interruption de ses activités associées aux paiements de détail sur les utilisateurs finaux et les autres FSP.

Indications

Exigences de gestion des risques opérationnels et de réponse aux incidents

Le paragraphe 17(1) de la LAAPD exige que « le fournisseur de services de paiement qui exécute une activité associée aux paiements de détail est tenu en vue d'identifier et d'atténuer les risques opérationnels et de répondre aux incidents, d'établir, de mettre en œuvre et de maintenir, conformément aux règlements, un cadre de gestion des risques et de réponse aux incidents qui remplit les exigences prévues par règlement ».

Le cadre de gestion des risques et de réponse aux incidents (le « cadre ») comprend tous les arrangements pris par le FSP relativement à la gestion des risques opérationnels et à la réponse aux incidents. Il s'agit notamment des systèmes, des politiques, des procédures, des processus, des plans, des contrôles, des objectifs, des ressources et des rôles et responsabilités liés à l'identification des risques opérationnels, à leur atténuation et à la réponse aux incidents.

Le cadre doit être conçu pour préserver l'intégrité, la confidentialité et la disponibilité des activités du FSP associées aux paiements de détail ainsi que des systèmes, données et renseignements liés à l'exercice de ces activités. Pour ce faire, le FSP doit :

- recenser les risques opérationnels auxquels il s'expose possiblement en exerçant des activités associées aux paiements de détail
- se protéger contre ces risques opérationnels
- déceler les incidents, les anomalies et les défaillances dans la mise en œuvre du cadre
- répondre aux incidents et s'en rétablir (quelle que soit leur importance)
- examiner et mettre à l'essai son cadre

Si le FSP a recours à des tiers fournisseurs de services ou à des mandataires, il doit également prendre ses précautions en les soumettant à des évaluations régulières. Le recours à des tiers fournisseurs de services peut offrir au FSP des gains d'efficacité et d'autres avantages dans le cadre de ses activités associées aux paiements de détail et de sa gestion des risques opérationnels. Toutefois, ces relations peuvent aussi présenter des risques additionnels. C'est pourquoi elles sont associées à des exigences supplémentaires concernant la gestion des risques opérationnels.

Comme le prévoit le paragraphe 17(1) de la LAAPD, le FSP est tenu d'établir, de mettre en œuvre et de maintenir tous les éléments décrits, définis ou exigés dans son cadre. La Banque s'attend à ce que les FSP interprètent largement les termes « établir », « mettre en œuvre » et « maintenir ». Par exemple, « établir » engloberait la conception et l'élaboration du cadre et de ses éléments, « mettre en œuvre » engloberait sa mise en vigueur, et « maintenir » engloberait sa surveillance et sa mise à jour par la suite.

Le FSP doit être capable de démontrer en permanence qu'il se conforme aux exigences de la LAAPD, notamment en conservant des documents à l'appui de cette conformité.

Champ d'application des attentes en matière de risque opérationnel

Tous les FSP assujettis à la LAAPD doivent satisfaire aux exigences concernant le risque opérationnel et la réponse aux incidents établies dans la LAAPD et le *Règlement sur les activités associées aux paiements de détail* (le « *Règlement* ») qui sont décrites dans la présente ligne directrice. Cette obligation s'applique quels que soient l'emplacement de leurs systèmes, données, renseignements ou actifs ou le lieu d'exercice de leurs activités.

Selon la LAAPD, la supervision qu'exerce la Banque sur les arrangements pris par le FSP pour la gestion des risques opérationnels et la réponse aux incidents vise toutes les activités associées aux paiements de détail du FSP. Ces activités comprennent les actifs (p. ex., systèmes, données, renseignements et tout autre actif) et les processus opérationnels associés ou contribuant à l'exercice de ces activités par le FSP. La section 5 aux présentes (« Recenser ») précise le champ d'application du cadre en ce qui a trait aux actifs et aux processus.

La conformité aux exigences de gestion des risques opérationnels et de réponse aux incidents s'applique également à toutes les activités associées aux paiements de détail, ou aux processus ou opérations connexes, qu'un employé, un tiers fournisseur de services ou un mandataire exerce pour le FSP. Comme l'indique l'article 87 de la LAAPD, le FSP ou toute autre personne ou entité soumise à une exigence en vertu de la LAAPD reste responsable d'une violation commise par un de ses employés, tiers fournisseurs de services ou mandataires.

Si le FSP fait partie d'un groupe, y compris d'un groupe international, il doit tout de même se conformer aux exigences de la LAAPD et démontrer cette conformité à la Banque. Il peut s'appuyer sur les arrangements pris par une entité liée pour la gestion des risques opérationnels et la réponse aux incidents (y compris ses ressources, systèmes, politiques, procédures, processus ou contrôles). Par exemple, le FSP peut adopter tout ou partie d'un cadre établi par une société mère. Toutefois, s'il en résulte une situation non conforme aux exigences de la LAAPD, le FSP doit modifier ce cadre ou prendre des arrangements supplémentaires pour assurer cette conformité.

Approche fondée sur les risques et proportionnalité

La Banque reconnaît que les FSP ont des pratiques différentes en matière de risque opérationnel, selon la nature et la complexité de leurs activités, leur structure organisationnelle, leurs technologies et d'autres facteurs pertinents. Le FSP doit adapter son cadre à sa situation, en tenant compte de ces facteurs et de la nature des risques auxquels il est exposé.

Selon le paragraphe 5(2) du *Règlement*, le FSP est tenu de s'assurer que « tous les aspects du cadre de gestion des risques et de réponse aux incidents, notamment les objectifs, cibles, systèmes, politiques, procédures, processus et contrôles, doivent être proportionnels aux répercussions que pourraient avoir une entrave, perturbation ou interruption de ses activités associées aux paiements de détail sur les utilisateurs finaux et les autres fournisseurs

de services de paiement ». Le même paragraphe exige aussi que le FSP tienne compte notamment de son ubiquité et interconnexion pour déterminer les répercussions d'une telle entrave, perturbation ou interruption[1].

Ce paragraphe signifie que plus l'ubiquité et l'interconnexion d'un FSP sont grandes, plus son approche de la gestion des risques opérationnels et de la réponse aux incidents doit être rigoureuse (c'est ce qu'on appelle ci-après la « proportionnalité »). La présente ligne directrice contient des exemples de situations où la Banque s'attend à une approche plus rigoureuse, bien que ces exemples ne soient pas exhaustifs.

---

1 Voici les informations qu'utiliserait la Banque pour établir l'ubiquité et l'interconnexion d'un FSP :
- le nombre d'utilisateurs finaux auxquels le FSP fournit des activités associées aux paiements de détail
- la valeur des fonds détenus pour des utilisateurs finaux par le FSP
- la valeur des transferts électroniques de fonds en lien avec lesquels le FSP a exercé une activité associée aux paiements de détail
- le nombre de transferts électroniques de fonds en lien avec lesquels le FSP a exercé une activité associée aux paiements de détail
- le nombre de FSP auxquels le FSP fournit des activités associées aux paiements de détail

1. Documentation et disponibilité du cadre

Cette section fournit des orientations sur le paragraphe 5(1) et l'article 6 du *Règlement*.

Résultat

- Le cadre de gestion des risques et de réponse aux incidents du FSP est documenté et mis à la disposition de tous ceux qui jouent un rôle dans sa mise en œuvre ou son maintien.

Indications

Documentation

1.1 Le paragraphe 5(1) du *Règlement* indique que le cadre du FSP doit être écrit.

1.2 Toutefois, il n'y a pas de structure universelle pour le cadre ou la manière dont il doit être documenté. Le FSP doit documenter son cadre d'une façon qui favorise l'atténuation de son risque opérationnel, sa réponse aux incidents et son rétablissement après un incident. Sa documentation doit être :

1.2.1 suffisamment complète pour véhiculer toute l'information nécessaire à l'atteinte de l'objectif visé (p. ex., toutes les étapes du processus doivent être indiquées dans une procédure écrite)

1.2.2 facilement compréhensible et convenable aux parties qui l'utilisent (p. ex., les employés ou d'autres ressources humaines du FSP ou, le cas échéant, ses mandataires)

1.2.3 tenue à jour et exacte

1.3 L'annexe B donne des exemples de types de documents que le FSP doit envisager lorsqu'il établit, met en œuvre et maintient son cadre.

1.4 En vertu de l'article 40 du *Règlement*, la documentation du FSP doit également étayer sa conformité générale aux exigences de tenue de documents établies dans la LAAPD. Le FSP doit conserver les documents qui démontrent et justifient sa conformité à la LAAPD, y compris la manière dont il a établi, mis en œuvre et maintenu son cadre.

Disponibilité

1.5 Le FSP doit « veille[r] à ce que son cadre de gestion des risques et de réponse aux incidents demeure disponible à toute personne participant à sa mise en œuvre et à son maintien et prend[re] toutes les précautions raisonnables pour prévenir sa suppression, destruction ou modification non autorisées », comme l'indique l'article 6 du *Règlement*.

1.5.1 Le cadre et la documentation doivent être à la disposition du personnel concerné et des autres intéressés au besoin. Par exemple, le FSP doit veiller à ce que les plans et les procédures de réponse aux incidents et de rétablissement soient accessibles en cas d'incident.

1.5.2 Le FSP doit établir, mettre en œuvre et maintenir des procédures et d'autres moyens permettant de garantir la disponibilité et d'empêcher la suppression, la destruction ou la modification non autorisées de sa documentation. Il peut s'agir, entre autres, de contrôles d'accès, de contrôles de versions et d'arrangements relatifs au stockage et à la conservation des documents.

2. Rôles et responsabilités

Cette section fournit des indications sur l'alinéa 5(1)d) et les paragraphes 5(5) et 5(6) du *Règlement*.

Résultats

- Le FSP établit, met en œuvre et maintient des rôles et des responsabilités pour tous les aspects entourant la gestion des risques opérationnels, la réponse aux incidents et le rétablissement après un incident, ce qui comprend la surveillance et l'examen critique.
- Le FSP surveille les rôles et responsabilités confiés à des tiers.

Indications

2.1 Selon l'alinéa 5(1)d) du *Règlement*, le cadre de gestion des risques et de réponse aux incidents doit « réparti[r] les rôles et les responsabilités à l'égard de sa mise en œuvre et de son maintien – tant dans le cours normal des affaires que lors de la détection d'incidents, de la réponse à ceux-ci et du rétablissement après un incident ». La définition des rôles et des responsabilités instaure une structure d'imputabilité et de responsabilité chez le FSP pour ce qui est de la gestion des risques opérationnels et de la réponse aux incidents.

2.2 Le FSP doit adapter à sa situation les rôles et les responsabilités nécessaires à l'établissement, à la mise en œuvre et au maintien de son cadre, notamment selon la nature et la complexité de ses activités, y compris sa structure de propriété et d'organisation, ses technologies et les autres facteurs pertinents.

2.2.1 Si le FSP fait partie d'un groupe élargi (y compris un groupe international), il peut attribuer des rôles et des responsabilités liés au cadre en dehors de l'entité réglementée. Néanmoins, c'est le FSP qui reste responsable de sa conformité à la LAAPD.

2.3 À moins que le FSP soit une personne physique, la répartition des rôles et des responsabilités doit :

- inclure toutes les parties responsables de l'établissement, de la mise en œuvre et du maintien du cadre, lesquelles dépendront de la nature et des arrangements précis du FSP, mais devraient inclure le cadre dirigeant, le conseil d'administration (s'il y en a un), la direction, le personnel et, s'il y a lieu, les tiers fournisseurs de services, les mandataires, les entités affiliées ou d'autres tiers
- être effectuée pour chaque étape de l'établissement, de la mise en œuvre et du maintien du cadre
- viser des postes précis (il peut s'agir d'équipes ou d'unités opérationnelles précises ou de postes attribués à des personnes)
- inclure un rôle d'examen critique et de surveillance relativement à l'exercice des rôles et responsabilités répartis, conformément au sous-alinéa 5(1)d)(i) du *Règlement*, laquelle peut être attribuée par exemple aux cadres dirigeants, à la direction ou à une fonction indépendante
- respecter la séparation des tâches, au besoin, afin qu'une personne ne contrôle pas un processus du début à la fin
- prévoir des liens hiérarchiques formels et, au besoin, des voies clairement définies pour la transmission des problèmes aux échelons supérieurs

2.4 Le FSP doit s'assurer qu'il dispose des ressources adéquates pour assumer chaque rôle et chaque responsabilité (voir Ressources humaines et financières).

2.5 En vertu du principe de proportionnalité, la Banque s'attend à ce que les FSP ayant une ubiquité et une interconnexion relativement grande mettent en œuvre un modèle à trois lignes de défense.

Cadre dirigeant, conseil d'administration et approbation du cadre

2.6 En vertu du sous-alinéa 5(1)d)(ii) du *Règlement*, à moins que le FSP soit une personne physique, son cadre doit attribuer à un cadre dirigeant la responsabilité de surveiller :

- la conformité avec le paragraphe 17(1), l'article 18 et le paragraphe 19(3) de la LAAPD ainsi que les articles 6 à 10 du *Règlement*;
- les décisions importantes relatives à l'identification des risques opérationnels et des incidents, à leur atténuation et aux mesures prises en réponse à ces risques et incidents.

2.7 Quel que soit son emplacement, le cadre dirigeant doit être à l'emploi du FSP, occuper un poste défini au sein du FSP ou relever directement de certaines personnes au sein du FSP (voir l'article 1 du *Règlement*).

2.8 Selon le paragraphe 5(6) du *Règlement*, le cadre doit être approuvé :

- par le cadre dirigeant et le conseil d'administration du FSP (s'il y en a un) au moins une fois par année
- par le cadre dirigeant après chaque modification importante

2.9 Il appartient au FSP d'établir si une modification est importante. Cela dit, les changements importants (voir la ligne directrice *Les avis de changement important ou d'activité nouvelle*) doivent aussi être considérés comme des modifications importantes, de même que tout changement majeur qui n'est pas de nature administrative et qui concerne la façon dont le FSP gère le risque opérationnel.

2.10 Le FSP doit également fournir au cadre dirigeant :

- les conclusions issues des examens du cadre, pour approbation (paragraphe 8(4) du *Règlement*)
- les résultats des essais (paragraphe 9(3) du *Règlement*)
- les examens indépendants du cadre (paragraphe 10(3) du *Règlement*)
- les renseignements sur les incidents (sous-alinéa 5(1)i)(vi) du *Règlement*)

Surveillance des tiers

2.11 Conformément au paragraphe 5(5) du *Règlement*, si le cadre attribue des rôles et responsabilités à un tiers, notamment à un tiers fournisseur de services ou à un mandataire du FSP, il doit comprendre des systèmes, politiques, procédures, processus, contrôles ou autres moyens pour surveiller la réalisation de ses rôles et l'accomplissement de ses responsabilités. Les responsabilités suivantes doivent en faire partie :

- réaliser des évaluations par précaution
- assurer un suivi de la prestation des services et de l'exercice des rôles et responsabilités

3. Ressources humaines et financières

Cette section fournit des indications sur l'alinéa 5(1)c), l'article 7 et l'alinéa 8(2)c) du *Règlement*.

Résultats

- Le FSP dispose d'un accès rapide et fiable aux ressources humaines et financières pour établir, mettre en œuvre et maintenir son cadre de gestion des risques et de réponse aux incidents, y compris pour répondre aux incidents.
- Les ressources humaines disposent des compétences, des informations et de la formation nécessaires pour remplir leur rôle.

Indications

3.1 Selon alinéa 5(1)c) du *Règlement,* le cadre du FSP doit « recense[r] les ressources humaines et financières du fournisseur de services de paiement nécessaires pour la mise en œuvre et le maintien du cadre, ce qui comprend, à l'égard des ressources humaines, leurs compétence et formation et les mesures à prendre par le fournisseur de services de paiement pour assurer l'accès fiable et opportun à ces ressources, qu'elles soient internes ou externes ».

Quantité, rapidité et disponibilité

3.2 Le FSP doit adapter à sa situation les ressources humaines et financières nécessaires à la mise en œuvre et au maintien du cadre. Il faut notamment tenir compte de la nature et de la complexité des activités, de la propriété, des structures organisationnelles, des technologies et d'autres facteurs pertinents.

3.2.1 Les ressources humaines englobent le personnel employé directement par le FSP et celui fourni par un tiers, comme les mandataires, les tiers fournisseurs de services ou les entités affiliées.

3.2.2 Les ressources financières englobent le budget que le FSP alloue à l'établissement, à la mise en œuvre et au maintien de son cadre, y compris l'embauche, le recrutement et la formation des ressources humaines ainsi que les investissements dans des systèmes, des contrôles, des technologies, des biens et d'autres actifs.

3.2.3 Le FSP doit également prendre en compte les ressources humaines ou financières supplémentaires dont il pourrait avoir besoin pour mettre en œuvre son plan de réponse aux incidents et de rétablissement, ou pour couvrir des dépenses ponctuelles ou inattendues. Ces ressources pourraient comprendre celles d'un tiers (y compris une société mère ou autre entité affiliée), une assurance, du financement de la part d'une société mère ou d'investisseurs, ou le recours à des spécialistes externes.

3.3 Le FSP doit avoir un accès fiable et opportun à ses ressources humaines et financières en temps normal, tout comme en cas d'incident, afin d'assurer l'atteinte constante de ses objectifs et cibles de gestion des risques opérationnels.

3.4 Si le FSP se fie aux ressources d'un tiers pour l'établissement, la mise en œuvre ou le maintien de son cadre en temps normal, il doit prévoir le tout dans un contrat écrit.

3.4.1 Le FSP peut avoir besoin des ressources humaines ou financières d'un tiers (p. ex., spécialistes externes ou fonds de prévoyance) avant l'établissement d'un contrat. Dans cette situation, il doit

évaluer de manière réaliste comment il accéderait à ces ressources en temps opportun et, s'il y a lieu, comment il en assumerait le coût.

3.4.2 Dans tous les cas, le FSP doit prendre des mesures pour assurer son accès fiable et opportun à ces ressources.

3.5 Si le FSP prévoit de s'en remettre à une assurance pour accéder à des ressources financières (p. ex., afin de mettre en œuvre son plan de réponse aux incidents et de rétablissement), il doit pouvoir démontrer qu'il a réfléchi à sa capacité d'obtenir ces ressources à la hauteur du montant attendu et en temps requis.

3.6 Si le FSP utilise ses propres ressources financières ou le financement d'une société mère, il doit tenir compte de la manière dont ces ressources sont investies afin de s'assurer qu'elles seront disponibles à la hauteur du montant attendu et en temps requis.

3.7 La LAAPD n'impose aucune exigence de fonds propres au FSP et ne l'oblige pas à mettre en place des dispositions de résolution. Néanmoins, il est important que le FSP prenne en compte et planifie les coûts et les ressources nécessaires à l'établissement, à la mise en œuvre et au maintien de son cadre conformément à la LAAPD. Cette planification comprend une marge de manœuvre pour couvrir les coûts supplémentaires prévus et les besoins en ressources qui pourraient résulter d'un incident.

Compétences, formation et information

3.8 Conformément à l'alinéa 5(1)c) du *Règlement*, le cadre doit établir la compétence et la formation exigées des ressources humaines pour sa mise en œuvre et son maintien.

3.9 En vertu de l'article 7 du *Règlement*, le FSP doit veiller à ce que tous les employés et autres personnes ayant un rôle dans l'établissement, la mise en œuvre ou le maintien du cadre se voient fournir les renseignements et la formation nécessaires pour s'acquitter de ce rôle.

3.10 La formation doit viser les résultats suivants :

- la connaissance et la compréhension du cadre
- l'acquisition et le maintien des compétences nécessaires à l'établissement, à la mise en œuvre et au maintien du cadre, selon les besoins, lesquelles peuvent provenir d'une combinaison d'études, d'expérience et de formation

3.11 Le FSP doit veiller à ce que la formation adressée à ses employés et aux autres personnes :

- soit donnée régulièrement afin que les ressources humaines entretiennent les compétences et les connaissances nécessaires à l'exercice de leurs responsabilités
- soit mise à jour régulièrement, notamment pour tenir compte des changements apportés au cadre ou aux activités
- soit adaptée aux rôles et responsabilités de chaque personne, notamment aux compétences ou aux connaissances opérationnelles précises dont elle a besoin pour exercer ses rôles et responsabilités
- permette la formation mutuelle, au besoin, pour assurer la continuité des activités et éviter les lacunes potentielles résultant du roulement ou de l'absence de personnel, que ce soit en temps normal ou en cas de réponse et de rétablissement après un incident

3.12 C'est la structure du FSP et les particularités de son cadre qui détermineront quelles ressources humaines doivent recevoir de la formation et des renseignements au sujet du cadre. Parmi les ressources humaines pertinentes, il pourrait y avoir toute partie interne ou externe du FSP qui joue un rôle dans l'établissement, la mise en œuvre ou le maintien du cadre, notamment les mandataires et les tiers fournisseurs de services (y compris, le cas échéant, les entités affiliées).

3.13 Les communications concernant le cadre doivent faire en sorte que le personnel et les autres intéressés ont l'information dont ils ont besoin pour exercer leurs rôles et responsabilités relativement à l'établissement, à la mise en œuvre et au maintien du cadre (ou de certains de ses éléments). Le FSP doit également informer les ressources humaines de tout changement pertinent apporté au cadre, s'il y a lieu.

3.14 La Banque encourage le FSP à évaluer l'efficacité de ses formations pour s'assurer que les ressources humaines comprennent leurs rôles et responsabilités et savent comment les exercer.

Examen interne

3.15 Conformément au paragraphe 8(1) du *Règlement*, le FSP doit examiner son cadre au moins une fois par année et avant de faire une modification importante à ses activités ou à ses systèmes, politiques, procédures, processus, contrôles ou autres moyens de gestion des risques opérationnels.

3.16 Dans le cadre de cet examen, le FSP doit évaluer le caractère adéquat de ses ressources financières et humaines pour veiller à la mise en œuvre du cadre, aux termes de l'alinéa 8(2)c) du *Règlement* (voir également Examen interne). Le FSP doit être en mesure de démontrer :

- que les ressources humaines et financières nécessaires sont ou seront disponibles de manière fiable et opportune pour mettre en œuvre, établir et maintenir le cadre en temps normal tout comme en cas d'incident, afin qu'il puisse atteindre ses objectifs de gestion des risques opérationnels
- que ses ressources humaines sont suffisantes, ce qui comprend l'adéquation de leurs compétences et de leur formation

4. Objectifs

Cette section fournit des indications sur les alinéas 5(1)a), 5(1)b) et 8(2)b) du *Règlement*.

Résultats

- Le FSP fixe des objectifs pour assurer l'intégrité, la confidentialité et la disponibilité de ses activités associées aux paiements de détail et des systèmes, données et renseignements liés à l'exercice de ces activités.
- Le FSP définit des indicateurs et des cibles de fiabilité pour évaluer la réalisation de ses objectifs d'intégrité, de confidentialité et de disponibilité.
- Un cadre dirigeant surveille la réalisation des objectifs du FSP.

Indications

Objectifs

4.1 En vertu de l'alinéa 5(1)a) du *Règlement*, le cadre de gestion des risques et de réponse aux incidents doit énoncer ce qui suit parmi ses objectifs :

- « veiller à ce que le fournisseur de services de paiement puisse exécuter ses activités associées aux paiements de détail sans entrave, perturbation ou interruption, notamment en veillant à la disponibilité des systèmes, données et renseignements engagés dans l'exécution de ces activités
- préserver l'intégrité et la confidentialité de ces activités, systèmes, données et renseignements »

4.2 Pour la suite de la présente ligne directrice, ces objectifs seront appelés les « objectifs d'intégrité, de confidentialité et de disponibilité » du FSP.

4.3 Les objectifs d'intégrité, de confidentialité et de disponibilité doivent s'appliquer à l'ensemble des activités associées aux paiements de détail du FSP ainsi qu'aux systèmes, données et renseignements qui permettent ou facilitent ces activités. L'obligation de fixer des objectifs d'intégrité, de confidentialité et de disponibilité ainsi que des cibles et des indicateurs de fiabilité s'applique même dans les cas où les services du FSP sont fournis par un tiers fournisseur de services, ou en son nom par un mandataire.

4.3.1 Par exemple, le FSP a l'obligation d'établir un ou plusieurs objectifs liés à la disponibilité globale des activités associées aux paiements de détail qu'il fournit. Il doit également fixer, de façon plus détaillée, des objectifs concernant la disponibilité des systèmes, des données et des renseignements nécessaires à l'exercice de ces activités, d'une manière qui sert l'objectif global de disponibilité.

4.4 Les objectifs de disponibilité doivent être proportionnels, comme l'indique le paragraphe 5(2) du *Règlement*. Ainsi, les FSP ayant une ubiquité ou une interconnexion relativement grande établissent des objectifs de disponibilité plus rigoureux. Quoiqu'il en soit, sans égard à la proportionnalité, le FSP doit établir des objectifs pour préserver l'intégrité et la confidentialité.

4.5 Le FSP doit établir, mettre en œuvre et maintenir son cadre de manière à atteindre ses objectifs d'intégrité, de confidentialité et de disponibilité.

Cibles de fiabilité et indicateurs

4.6 En vertu de l'alinéa 5(1)b) du *Règlement*, le cadre doit fixer des cibles de fiabilité clairement définies et mesurables concernant les activités du FSP associées aux paiements de détail et la disponibilité de ses systèmes, données et renseignements.

4.7 Le FSP doit réfléchir à diverses cibles de fiabilité pour préciser les normes de rendement qu'il entend respecter dans le cadre de son objectif de disponibilité. La Banque recommande qu'un FSP ayant une ubiquité ou une interconnexion particulièrement grande établisse au minimum les types de cibles de fiabilité suivants :

- cible(s) de disponibilité du système
- objectif(s) quant au temps de rétablissement
- durée(s) maximale(s) d'interruption tolérable(s)
- objectif(s) de point de reprise.

4.8 Conformément à l'alinéa 5(1)b) du *Règlement*, le cadre doit aussi fixer des indicateurs servant à évaluer l'atteinte de chaque objectif d'intégrité, de confidentialité et de disponibilité.

4.9 Les cibles de fiabilité et les indicateurs doivent formuler clairement les normes de rendement et les mesures sous-jacentes dont le FSP compte faire le suivi pour s'assurer qu'il est capable d'atteindre ses objectifs d'intégrité, de confidentialité et de disponibilité.

4.10 Voir l'annexe C pour explorer d'autres facteurs à considérer concernant l'établissement, la mise en œuvre et le maintien des objectifs, des cibles de fiabilité et des indicateurs.

Évaluation du rendement par rapport aux objectifs

4.11 Conformément au paragraphe 8(1) et à l'alinéa 8(2)b) du *Règlement*, le FSP doit examiner son cadre au moins une fois par année et avant de faire des modifications importantes. L'examen doit notamment évaluer l'efficacité du FSP à atteindre ses objectifs d'intégrité, de confidentialité et de disponibilité compte tenu de ses cibles et indicateurs de fiabilité.

4.12 En évaluant son efficacité relativement à l'atteinte de ses objectifs, le FSP doit analyser des informations provenant de plusieurs sources, notamment :

- des données sur les incidents ayant entraîné des atteintes à l'intégrité ou à la confidentialité ou des pannes de systèmes, y compris le degré de réussite du FSP dans l'atteinte de ses cibles de fiabilité en réponse à ces incidents
- les mesures de rendement observées par rapport aux objectifs, aux cibles de fiabilité et aux indicateurs, telles que la disponibilité des systèmes au cours de la période concernée
- les résultats des essais et des examens indépendants, qui pourraient également indiquer dans quelle mesure le FSP est susceptible d'atteindre ses objectifs et ses cibles de fiabilité à l'avenir, par exemple une mise à l'essai du plan de réponse aux incidents du FSP pour vérifier dans quelle mesure il pourrait réussir à atteindre certains objectifs et certaines cibles

4.13 Si une évaluation indique que le FSP n'atteint pas ses objectifs, il doit examiner la nécessité d'améliorer son cadre pour que les objectifs, les cibles de fiabilité et les indicateurs soient atteints.

4.14 La Banque encourage le FSP à surveiller et à évaluer de façon continue son rendement par rapport à ses objectifs, à ses cibles de fiabilité et à ses indicateurs. Cette approche peut d'ailleurs être compatible avec

son obligation d'assurer un contrôle continu afin de déceler rapidement les incidents, les anomalies et les défaillances dans la mise en œuvre du cadre, comme le prévoit l'alinéa 5(1)h) du *Règlement*.

Approbations et rapports

4.15 Le cadre dirigeant responsable du risque opérationnel et de la réponse aux incidents ainsi que le conseil (s'il y en a un) doivent approuver les objectifs, les cibles de fiabilité et les indicateurs du FSP. Cette exigence s'inscrit dans leur obligation d'approuver le cadre, comme le prévoit le paragraphe 5(6) du *Règlement* (voir également Rôles et responsabilités).

4.16 Le cadre dirigeant doit être au courant du rendement du FSP par rapport à ses objectifs. Les résultats de l'évaluation du rendement du FSP, et toute considération d'amélioration du cadre, doivent être communiqués au cadre dirigeant pour approbation, conformément à l'article 8 du *Règlement*.

5. Recenser

Cette section fournit des indications sur les alinéas 5(1)e) et 5(1)f) du *Règlement*.

Résultats

- Le FSP recense et comprend ses risques opérationnels.
- Le FSP recense les actifs et les processus opérationnels entourant ses activités associées aux paiements de détail et les classe en fonction de leur importance et de leur sensibilité.

Indications

Recensement des risques opérationnels

5.1 La LAAPD définit le risque opérationnel comme l'un ou l'autre des risques ci-après qui entrave, perturbe ou interrompt une activité associée aux paiements de détail exécutée par un FSP :

- une défaillance des systèmes d'information ou du processus interne de ce FSP
- une erreur humaine
- une gestion défaillante ou inadéquate
- une perturbation causée par un événement externe

5.2 L'alinéa 5(1)f) du *Règlement* exige que le cadre de gestion des risques et de réponse aux incidents recense les risques opérationnels auxquels le FSP est sujet et décrive leurs causes éventuelles.

5.3 La Banque attend du FSP qu'il établisse, mette en œuvre et maintienne des procédures pour recenser ses risques opérationnels et les causes éventuelles. Le FSP doit aussi déterminer les risques inhérents, définis comme des risques présents avant la mise en œuvre de contrôles ou de mesures d'atténuation.

5.4 Les risques auxquels chaque FSP est exposé dépendent de la nature et de la complexité de ses activités, de sa propriété, de ses structures organisationnelles, de ses technologies et d'autres facteurs pertinents. Au minimum, le FSP doit recenser les risques opérationnels liés à chacun des aspects ci-dessous (alinéa 5(1)f) du *Règlement*).

- Continuité des activités et résilience : risque pour la capacité du FSP à exercer des activités associées aux paiements de détail en raison de l'indisponibilité de personnes, de processus, de systèmes, de locaux ou de tiers.
- Cybersécurité : risque d'accès non autorisé, d'utilisation malveillante et non malveillante, de défaillance, de fuite, d'interruption, de modification ou de destruction du système d'information ou des données du FSP en raison d'une cyberattaque ou d'une atteinte à la protection des données.
- Fraude : risque d'activités intentionnelles provenant de menaces internes (d'une entité ayant un accès autorisé aux systèmes, aux données ou aux renseignements) ou externes (d'une entité n'ayant pas d'accès autorisé aux systèmes, aux données ou aux renseignements) visant à provoquer une perte des actifs, des produits ou des données du FSP ou à en tirer profit.
- Gestion des données et des renseignements : risques liés à une défaillance dans la gestion des renseignements ou des données sur l'ensemble de leur cycle de vie.
- Technologies de l'information : risque lié à l'inadéquation, à l'interruption, à la défaillance, à la perte ou à l'utilisation malveillante des systèmes de technologies de l'information, des infrastructures, du

personnel ou des processus qui permettent de répondre aux besoins opérationnels du FSP et de les soutenir.

- Ressources humaines : risque lié à l'inadéquation ou à l'insuffisance des ressources humaines ou des compétences requises.
- Conception et mise en œuvre de processus : risque lié à une défaillance dans la conception, la mise en œuvre, la documentation ou l'exécution efficaces d'un processus.
- Conception et mise en œuvre des produits : risque lié à une défaillance dans la conception, la mise en œuvre ou la gestion efficaces d'un produit ou d'un service.
- Gestion du changement : risque lié à l'incapacité de mettre en œuvre efficacement des changements, notamment en raison d'une conception ou d'une réalisation inefficace du projet (y compris, entre autres, des changements dans la structure de l'entreprise, la conception des produits, les services et la fourniture de technologies de l'information).
- Sécurité physique des personnes et des actifs : risque lié à l'incapacité de protéger les employés, les clients, les biens matériels ou les installations.
- Tiers : risque lié à une défaillance dans la gestion efficace des tiers, comme les tiers fournisseurs de services, les mandataires, les entités affiliées, les autres FSP et les infrastructures de marchés financiers. Le FSP doit prendre en compte le risque lié à tous les tiers, qu'il ait ou non un contrat avec eux (voir Tiers fournisseurs de services et Mandataires).

5.5 La liste ci-dessus n'est pas exhaustive. Le FSP doit prendre en compte tout autre risque opérationnel pertinent susceptible de provoquer une entrave, une perturbation ou une interruption de ses activités associées aux paiements de détail.

5.5.1 On inclut ici les risques opérationnels émanant d'activités du FSP non associées aux paiements de détail qui pourraient avoir une incidence sur ses activités associées aux paiements de détail.

5.5.2 En ce qui concerne le recensement des risques, la Banque encourage également le FSP à considérer sa dépendance à un tiers, à un actif, à un système, à une ressource humaine, à un rôle ou à un autre facteur (risque de concentration) pour déterminer si cette situation peut entraver sa capacité à atteindre ses objectifs.

5.6 L'alinéa 5(1)f) du *Règlement* précise que le cadre doit décrire les causes éventuelles des risques opérationnels du FSP. Il s'agit notamment des causes d'incidents susceptibles de provoquer une entrave, une perturbation ou une interruption de ses activités associées aux paiements de détail. Les causes éventuelles que le FSP devrait envisager sont les suivantes :

- une défaillance des systèmes d'information ou du processus interne de ce FSP
- une erreur humaine
- une gestion défaillante ou inadéquate
- une perturbation causée par un événement externe (aux termes de l'article 2 de la LAAPD)

5.7 En recensant les risques opérationnels et leurs causes éventuelles, le PSP doit être en mesure de dégager les deux résultats suivants :

- classer en ordre d'importance les risques opérationnels recensés
- tenir compte de ce classement des risques opérationnels pour orienter les systèmes, politiques, procédures, processus et contrôles nécessaires à l'atténuation de ces risques (voir Protéger)

5.8 Le FSP doit examiner et mettre à jour ses risques opérationnels et leurs causes éventuelles au moins une fois par année ou à mesure qu'il recense de nouveaux risques (et après qu'un incident se soit produit, s'il y a lieu). Il doit notamment évaluer les risques émergents ou changeants résultant de modifications dans les environnements externes et internes.

5.9 Le FSP doit recenser les risques opérationnels liés aux modifications importantes qui seraient apportées à ses activités ou systèmes, politiques, procédures, processus, contrôles ou autres moyens de gestion des risques opérationnels. Ces modifications importantes pourraient amener de nouveaux risques ou changer les risques préalablement recensés. Le FSP doit établir et mettre en œuvre toute modification nécessaire à son cadre pour gérer ces risques avant que soient apportées les modifications (voir, par exemple, Protéger et Détecter).

Recensement des actifs et des processus opérationnels

5.10 L'alinéa 5(1)e) du *Règlement* précise que le cadre du FSP doit « recense[r] les actifs – notamment les systèmes, les données et les renseignements – et processus opérationnels engagés dans l'exécution des activités associées aux paiements de détail du fournisseur de services de paiement ».

5.11 Les actifs et les processus opérationnels que doit recenser le FSP dépendent de la nature et de la complexité de ses activités, de sa propriété, de ses structures organisationnelles, de ses technologies et d'autres facteurs pertinents.

5.12 Le recensement des actifs et des processus opérationnels doit inclure, entre autres, tous les actifs et processus opérationnels pour lesquels une entrave, une perturbation ou une interruption nuirait à l'exercice d'activités associées aux paiements de détail par le FSP. Voici une liste non exhaustive des types d'actifs entourant les activités associées aux paiements de détail du FSP :

- les données ou les renseignements qui permettent au FSP d'exercer des activités associées aux paiements de détail (voir la politique *La protection des fonds des utilisateurs finaux*), à la fois lorsque ces données et renseignements sont en transit et lorsqu'ils sont utilisés et stockés au repos
- les systèmes physiques ou virtuels, le matériel ou d'autres biens matériels que le FSP utilise pour faciliter des activités associées aux paiements de détail
- les logiciels ou les applications que le FSP utilise pour faciliter des activités associées aux paiements de détail
- les personnes et les lieux qui servent au FSP à exercer ses activités associées aux paiements de détail

5.13 Le FSP doit recenser tout actif ou processus opérationnel entourant ses activités associées aux paiements de détail, quel que soit son emplacement géographique ou le lieu d'exécution opérationnelle du processus. Il doit aussi tenir compte des actifs et des processus opérationnels qui sont détenus ou exécutés en dehors de l'organisation, notamment par des tiers (y compris les entités affiliées), des mandataires et des utilisateurs finaux.

5.14 Les actifs ou processus opérationnels qui ne sont pas engagés dans l'exercice des activités associées aux paiements de détail pourraient être considérés comme exclus du champ de supervision direct de la Banque (p. ex., les systèmes servant uniquement à des activités de marketing ou de publicité).

5.15 L'alinéa 5(1)e) du *Règlement* exige également que le cadre classe ces actifs et processus opérationnels en fonction de leur sensibilité et de leur importance pour l'exécution des activités associées aux paiements de détail du FSP. La classification des actifs et des processus opérationnels sert à l'élaboration des systèmes, politiques, procédures, processus, contrôles et autres moyens nécessaires à l'atteinte des objectifs d'intégrité, de confidentialité et de disponibilité du FSP.

5.15.1 En évaluant le degré de sensibilité des données, des renseignements ou des processus opérationnels, le FSP doit considérer à quel point il est important, pour ses activités associées aux paiements de détail et pour l'atteinte de ses objectifs d'intégrité, de confidentialité et de disponibilité, que :

- les données, les renseignements ou les processus soient disponibles
- l'intégrité des données, des renseignements ou des processus soit maintenue
- les données, les renseignements ou les processus restent confidentiels

5.15.2 De même, en évaluant l'importance des actifs autres que les données, les renseignements ou les processus opérationnels, le FSP doit considérer à quel point il est important, pour ses activités associées aux paiements de détail et pour l'atteinte de ses objectifs d'intégrité, de confidentialité et de disponibilité, que :

- l'actif ou le processus soit disponible (pleinement opérationnel)
- l'intégrité de l'actif ou du processus soit maintenue

6. Protéger

Cette section fournit des indications sur l'alinéa 5(1)g) du *Règlement*.

Résultat

- Le FSP préserve l'intégrité, la confidentialité et la disponibilité de ses activités associées aux paiements de détail en atténuant les risques opérationnels ainsi qu'en protégeant les actifs et les processus opérationnels qui servent à ces activités.

Indications

Protection des actifs et des processus opérationnels

6.1 L'alinéa 5(1)(g) du *Règlement* exige que le cadre de gestion des risques et de réponse aux incidents du FSP « décri[ve] les systèmes, politiques, procédures, processus, contrôles et tout autre moyen que le fournisseur de services de paiement doit avoir en place pour atténuer ses risques opérationnels et protéger les actifs et processus opérationnels » qui sont liés à l'exécution de ses activités associées aux paiements de détail. Ainsi, le FSP doit établir, mettre en œuvre et maintenir des éléments de protection pour atténuer ses risques opérationnels et protéger les actifs (y compris les données) et les processus opérationnels entourant ses activités associées aux paiements de détail. Il doit également décrire ces éléments de protection dans le cadre, y compris la protection des données et des renseignements en transit, en attente et en cours d'utilisation.

6.2 Le FSP doit établir, mettre en œuvre et maintenir ses éléments de protection d'une manière adaptée à sa situation particulière. Ce faisant, il doit prendre en considération :

- le niveau inhérent des risques auxquels il est exposé et les répercussions potentielles de ces risques sur ses activités associées aux paiements de détail, ses actifs et ses processus opérationnels
- sa capacité à atteindre ses objectifs d'intégrité, de confidentialité et de disponibilité
- son ubiquité et son interconnexion, aux termes du paragraphe 5(2) du *Règlement* (plus l'ubiquité et l'interconnexion d'un FSP sont grandes, plus ses éléments de protection doivent être rigoureux)

6.3 Le FSP doit adopter une approche fondée sur les risques en ce qui concerne les éléments de protection de son cadre. Ainsi, en atténuant ses risques opérationnels, le FSP doit veiller à ce que le degré de protection soit approprié à l'importance des risques auxquels il est exposé.

6.4 Le FSP doit aussi concevoir ses éléments de protection sur plusieurs niveaux, en guise de redondance s'il y a défaillance ou contournement d'un élément donné (p. ex., un contrôle en particulier).

6.5 Une fois que le FSP a établi les éléments de protection de son cadre, il doit examiner l'adéquation et l'efficacité de ces éléments pour ce qui est d'atténuer les risques opérationnels et de protéger ses actifs et ses processus opérationnels. Ainsi, le FSP doit déterminer si ses risques résiduels sont conformes aux objectifs et, en cas de divergence, prendre des mesures pour améliorer le niveau de protection.

Éléments de protection concernant les technologies de l'information et la cybersécurité

6.6 La Banque s'attend à ce que tous les FSP soient exposés à des risques entourant la cybersécurité et les technologies de l'information. Le FSP est tenu de recenser ses risques opérationnels relevant de ce domaine, entre autres risques. Il doit aussi établir, mettre en œuvre et maintenir des éléments de

protection pour atténuer ces risques et protéger ses actifs et ses processus opérationnels, conformément aux alinéas 5(1)f) et 5(1)g) du *Règlement*.

6.7 En ce qui concerne l'atténuation des risques entourant les technologies de l'information et la cybersécurité, la Banque recommande que le FSP établisse, mette en œuvre et maintienne des éléments de protection portant sur les résultats et concepts suivants :

- la gestion des accès, y compris l'accès physique
- la gestion des vulnérabilités, les mesures correctives et l'application de correctifs
- les logiciels de sécurité
- la configuration sécurisée des appareils
- la sécurité des réseaux
- les services de technologies de l'information sécurisés en nuage et externalisés
- les supports sécurisés liés à des systèmes d'information
- le cycle de développement des systèmes sécurisés
- les autres contrôles pertinents à la nature des activités du FSP

6.8 Il est attendu que ces résultats et concepts soient pertinents pour tous les FSP. La manière dont le FSP concrétise chaque résultat ou concept, y compris la nature des éléments de protection qu'il adopte, dépend de sa situation.

6.9 Voir l'annexe D pour en savoir plus sur les éléments de protection recommandés à l'égard des risques entourant les technologies de l'information et la cybersécurité.

7. Déceler

Cette section fournit des indications sur les alinéas 5(1)h) et 5(1)j) du *Règlement*.

Résultats

- Le FSP établit, maintient et met en œuvre des capacités de contrôle et de détection en continu.
- Le FSP décèle rapidement les incidents et les anomalies dans ses activités associées aux paiements de détail et les défaillances dans la mise en œuvre de son cadre de gestion des risques et de réponse aux incidents.
- Le FSP soumet les anomalies et les défaillances dans la mise en œuvre de son cadre à l'attention des intéressés pertinents (décideurs compris) en temps opportun afin de permettre des interventions rapides.

Indications

Détection et surveillance continue

7.1 Conformément à l'alinéa 5(1)h) du *Règlement*, le cadre doit décrire les systèmes, politiques, procédures, processus, contrôles et tout autre moyen que le FSP doit avoir en place pour assurer un contrôle continu afin de déceler rapidement les incidents, les anomalies pouvant signaler un risque opérationnel émergent et les défaillances dans la mise en œuvre du cadre :

7.1.1 Le terme « rapidement » signifie qu'il doit vite déceler ces éléments, tout en tenant compte des circonstances particulières. Autrement dit, à moins que le FSP n'ait une justification raisonnable pour tarder à les déceler, il doit prioriser leur détection.

7.1.2 Dans ce contexte, le terme « continu » signifie que les systèmes, politiques, procédures, contrôles et autres moyens du FSP permettent d'être constamment tenu au courant et sont analysés à une fréquence favorisant la prise de décisions fondées sur les risques.

7.2 Comme l'indique les sous-alinéas 5(1)h)(i), (ii) et (iii) du *Règlement*, le contrôle continu doit englober les éléments ci-après :

- les activités associées aux paiements de détail des fournisseurs de services de paiement
- les systèmes, les données et les renseignements qui sont engagés dans l'exécution de ces activités
- les éléments de protection qui ont été mis en place pour atténuer les risques opérationnels et protéger les actifs et les processus opérationnels

7.3 La détection d'anomalies et de défaillances dans la mise en œuvre du cadre devrait favoriser :

- la compréhension par le FSP de son environnement à risque, notamment des domaines où les risques dépassent l'appétit
- le recensement de risques nouveaux ou émergents qui pourraient nuire à l'intégrité, à la confidentialité ou à la disponibilité des activités associées aux paiements de détail du FSP ou des systèmes, données ou renseignements qui permettent ou facilitent ces activités
- la détection de problèmes dans le fonctionnement du cadre, en particulier les éléments de protection du cadre
- la détection des incidents par le FSP

7.4 Voici une liste non exhaustive de possibles anomalies et défaillances dans la mise en œuvre du cadre :

- les changements apportés sans autorisation à des systèmes ou à des actifs
- l'usage abusif d'un accès par des employés, des tiers fournisseurs de services ou des mandataires
- les infractions aux politiques internes (p. ex., formation obligatoire, exigences d'approbation ou de conservation des documents)
- l'entrave ou la perturbation des systèmes ou des contrôles
- les tentatives commises par des entités externes pour entraver, perturber ou interrompre des activités associées aux paiements de détail

Capacités de contrôle continu

7.5 Le FSP doit établir, mettre en œuvre et maintenir des systèmes, des politiques, des procédures, des processus, des contrôles et d'autres moyens de contrôle continu et de détection pour qu'il soit plus facile de déceler rapidement les incidents, les anomalies et les défaillances dans la mise en œuvre du cadre.

7.6 Les capacités de contrôle continu et de détection du FSP doivent :

- être conçues pour faciliter le processus de réponse aux incidents du FSP et soutenir la collecte d'informations en vue d'enquêter sur les incidents, les anomalies et les défaillances dans la mise en œuvre du cadre (p. ex., pour déterminer la cause première d'un incident)
- couvrir tous les types d'incidents et d'anomalies, ainsi que tous les éléments pertinents du cadre (surtout les éléments de protection, comme ceux liés à la cybersécurité, à la sécurité de l'information et à la sécurité physique)
- permettre la détection d'incidents ou d'anomalies entourant les services fournis par des tiers fournisseurs de services et, s'il y a lieu, de toute défaillance dans la mise en œuvre du cadre par ces tiers
- permettre la détection d'incidents, d'anomalies et de défaillances dans la mise en œuvre du cadre par des mandataires, s'il y a lieu

7.7 Pour en savoir plus sur la relation entre le contrôle continu, la détection des incidents, la réponse aux incidents et le rétablissement après un incident, voir l'annexe E.

7.8 Le FSP doit adopter une approche fondée sur les risques en ce qui concerne ses capacités de contrôle continu et de détection. Autrement dit, si un incident, une anomalie ou une défaillance dans la mise en œuvre peut avoir des répercussions importantes ou est susceptible de se produire, le FSP doit renforcer la rigueur de ses capacités de contrôle continu et de détection.

Contrôles concernant les technologies de l'information et la cybersécurité

7.9 En ce qui concerne les risques entourant les technologies de l'information et la cybersécurité, la Banque recommande que le FSP établisse, mette en œuvre et maintienne des capacités de contrôle continu et de détection relatives aux résultats et aux concepts suivants :

- les indicateurs clés et les seuils internes (qui, si dépassés, déclenchent une action ou une décision)
- l'enregistrement et la surveillance (p. ex., par des journaux d'accès et de trafic)
- les défenses du réseau
- la détection des programmes malveillants
- la détection et la prévention des intrusions

- la détection des vulnérabilités
- la surveillance de sécurité
- la sécurité physique (p. ex., par des journaux d'accès)
- les renseignements sur les menaces
- d'autres contrôles pertinents

7.10 Ces résultats et concepts devraient être pertinents pour tous les FSP. La manière dont le FSP réalise chacun d'entre eux dépend de sa situation.

7.11 Voir l'annexe F pour en savoir plus sur les contrôles recommandés dans le domaine des technologies de l'information et de la cybersécurité en ce qui concerne les capacités de contrôle continu et de détection.

Recours hiérarchique en cas d'incidents, d'anomalies et de défaillances dans la mise en œuvre

7.12 En vertu de l'alinéa 5(1)j) du *Règlement*, le cadre doit prévoir un plan pour répondre aux anomalies et aux défaillances dans sa mise en œuvre.

7.13 Ce plan doit établir des politiques et des procédures clairement définies pour les recours hiérarchiques et la prise de décisions en cas d'anomalies ou de défaillances dans la mise en œuvre. Il doit :

- établir des seuils et des délais internes pour que le FSP puisse faire progresser de façon méthodique et en temps opportun le traitement des anomalies et des défaillances dans la mise en œuvre du cadre, ce qui pourrait comprendre l'établissement de seuils d'alerte à partir desquels ses systèmes de détection déclencheraient un recours hiérarchique
- définir des rôles et des responsabilités, notamment les personnes responsables de la prise de décision
- mettre en place des processus pour que les décideurs reçoivent en temps opportun des renseignements exacts sur l'anomalie ou la défaillance entourant la mise en œuvre du cadre
- s'il y a lieu, établir des seuils internes et déterminer les personnes responsables des décisions à prendre lorsqu'une anomalie se produit ou est décelée par des mandataires
- s'il y a lieu, établir les mesures à prendre lorsqu'un tiers fournisseur de services informe le FSP d'une anomalie qui se produit chez ce tiers ou qui est détectée par lui

7.14 Le FSP doit également établir, mettre en œuvre et maintenir des politiques et des procédures clairement définies pour le signalement des incidents et la coordination des réponses aux incidents. Pour en savoir plus, voir Réponse et rétablissement.

8. Réponse et rétablissement

Cette section fournit des indications sur l'alinéa 5(1)i) du *Règlement*.

Résultats

- Le PSP a un plan pour répondre aux incidents et s'en rétablir. Ce plan est conçu pour que le FSP puisse continuer à exercer des activités associées aux paiements de détail sans interruption, endiguer les répercussions de tout incident et continuer à préserver l'intégrité, la confidentialité et la disponibilité continues des données, renseignements ou systèmes liés aux paiements de détail.
- Le FSP répartit des rôles et des responsabilités et élabore des politiques, des processus et des procédures de mise en œuvre du plan qui permettent d'agir en temps opportun en réponse à un incident.
- Le FSP enquête sur la cause première de tous les incidents et prend des mesures pour remédier à toute lacune ou vulnérabilité décelée dans son cadre de gestion des risques et de réponse aux incidents.
- Le FSP remplit son obligation de déclarer sans délai les incidents qui ont des répercussions importantes sur un utilisateur final, un FSP ou une chambre de compensation (voir l'article 18 de la LAAPD).

Indications

Plan de réponse aux incidents

8.1 En vertu de l'alinéa 5(1)i) du *Règlement*, le cadre du FSP doit « établi[r] un plan de réponse aux incidents – concernant notamment le rétablissement après les incidents –, relatif notamment aux incidents qui mettent en cause un mandataire ou un tiers fournisseur de services ou qui sont décelés par un de ceux-ci ».

8.2 Le plan de réponse aux incidents du FSP doit couvrir tous les incidents plausibles qui pourraient être causés par les risques opérationnels du FSP, à la fois les incidents possibles en temps normal et les événements majeurs ou de crise.

8.3 Durant la conception et l'établissement de son plan de réponse aux incidents, le FSP doit définir et catégoriser les événements plausibles qui pourraient nuire à ses activités et à l'atteinte de ses objectifs. Par exemple, le FSP doit y traiter des incidents qui seraient susceptibles :

- soit de présenter un risque pour la préservation de l'intégrité et de la confidentialité des données, renseignements ou systèmes qui soutiennent l'exercice d'activités associées aux paiements de détail
- soit de limiter la disponibilité des activités associées aux paiements de détail du FSP ou les données, renseignements ou systèmes qui soutiennent l'exercice d'activités associées aux paiements de détail, y compris les incidents qui rendraient indisponibles ou défaillants des processus ou des actifs critiques ou sensibles pendant un laps de temps important, notamment en entraînant la perte de technologies, de données, de personnes, d'installations ou d'un tiers

8.4 Bien que le plan doive couvrir tous les incidents plausibles, si un incident – ou une catégorie d'incidents – peut avoir des répercussions importantes ou est susceptible de se produire, le FSP doit renforcer la rigueur des plans de réponse à ces incidents.

8.5 Les sous-alinéas 5(1)i)(i) à (viii) du *Règlement* précisent que le plan de réponse aux incidents doit établir :

- des politiques, des processus et des procédures pour sa mise en œuvre et pour l'augmentation de l'intensité de la réponse à l'incident, où le FSP doit aussi tenir compte, s'il y a lieu, des procédures

de réponse aux incidents de ses tiers fournisseurs de services et de la nécessité de coordonner sa réponse à l'incident avec celle du tiers fournisseur de services

- les mesures à prendre pour atténuer les répercussions d'un incident, et des indications quant au délai minimum requis pour la mise en œuvre de ces mesures par le FSP
- l'obligation, pour le FSP, d'amorcer une enquête dès qu'il prend connaissance d'un incident (et les éléments précisément visés par l'enquête)
- l'obligation pour le FSP de prendre des mesures immédiates, alors même que l'enquête se poursuit, afin de prévenir ou d'atténuer toute autre atteinte, notamment à l'intégrité, à la confidentialité ou à la disponibilité des systèmes, données et renseignements
- l'obligation pour le FSP de prendre, aussitôt que possible, des mesures permettant de traiter la ou les causes premières établies de l'incident
- des politiques et des procédures pour le signalement des incidents aux intéressés internes pertinents et la coordination de la réponse aux incidents avec ceux-ci
- des mesures pour déterminer promptement l'état des opérations au moment de l'incident, tandis que le FSP doit également récupérer ou réparer les données perdues ou autrement touchées par l'incident
- des politiques et des procédures concernant la tenue de documents pour chaque incident

Rôles et responsabilités, signalement et recours hiérarchique

8.6 Conformément à l'alinéa 5(1)d) du *Règlement*, le FSP doit répartir les rôles et les responsabilités entourant la mise en œuvre du cadre, que ce soit en temps normal ou en cas de réponse aux incidents et de rétablissement.

8.7 Le FSP doit prédéterminer, définir clairement et consigner d'avance les rôles, les responsabilités, les politiques et les procédures entourant le signalement et la coordination. Il doit appliquer ces politiques et procédures après la détection d'un incident, ce qui lui permettra d'y répondre en temps opportun.

8.8 En ce qui concerne la réponse aux incidents, les rôles et responsabilités du FSP doivent préciser qui est responsable :

- de signaler les incidents aux intéressés concernés, soit à la fois aux échelons internes supérieurs et à la Banque, s'il y a lieu
- de coordonner la réponse du FSP à un incident (p. ex., le propriétaire du système, le responsable de la réponse à l'incident, l'équipe de réponse aux incidents, les tiers, les mandataires et le personnel de soutien nécessaire à l'exercice de certains rôles et responsabilités)
- de résoudre les incidents
- de suivre la mise en œuvre de tout plan de mesures correctives jusqu'à son terme
- de planifier, d'examiner et de mettre à jour le plan de réponse aux incidents afin d'en assurer l'efficacité continue

8.9 Dans le cadre de son plan de réponse aux incidents, le FSP doit déterminer lorsqu'il serait nécessaire de collaborer avec ses mandataires pour soutenir les mesures de réponse. Par exemple, cette collaboration pourrait être requise lorsque l'incident concerne des activités associées aux paiements de détail exercées ou soutenues par des mandataires.

8.10 Conformément au sous-alinéa 5(1)i)(vi), les politiques et procédures du FSP pour le signalement des incidents aux intéressés internes et externes pertinents, et la coordination de la réponse aux incidents avec

ceux-ci, doivent traiter, entre autres, du délai et des renseignements communiqués pour le signalement et la coordination. Le cadre dirigeant est un intéressé interne, de même que les mandataires au besoin.

8.11 Les politiques et procédures de signalement et de coordination des réponses aux incidents doivent :

- exiger que le FSP informe en temps opportun les intéressés internes et externes pertinents (y compris les tiers et les mandataires), notamment en donnant des précisions sur l'incident, les communications et les plans d'action
- fournir des indications et des critères clairs pour les recours hiérarchiques internes en cas d'incident afin d'informer et de faire intervenir les décideurs concernés
- faciliter l'obligation réglementaire du FSP de signaler certains incidents à la Banque ainsi qu'aux utilisateurs finaux, aux FSP et aux chambres de compensation des systèmes de compensation et de règlement ayant subi des répercussions importantes, conformément à l'article 18 de la LAAPD

8.12 Le FSP doit communiquer les rôles, les responsabilités, les politiques et les procédures de signalement et de coordination aux employés et aux intéressés (internes ou externes) qui jouent un rôle dans la réponse aux incidents. Les ressources humaines responsables de la réponse aux incidents doivent avoir les compétences nécessaires pour assumer leurs responsabilités, et le FSP doit les former. Ces exigences sont précisées aux sections Rôles et responsabilités et Ressources humaines et financières.

8.13 Le FSP doit mettre à l'essai son plan de réponse aux incidents pour vérifier qu'il peut être mis en œuvre comme prévu, conformément à la section Mises à l'essai.

Réponse à un incident

8.14 Dès qu'un incident est décelé, le FSP doit mettre en œuvre son plan de réponse aux incidents, qui nécessite des mesures immédiates d'enquête et d'endiguement concernant l'incident, quelle que soit son importance. En vertu du sous-alinéa 5(1)i)(i) du *Règlement*, le plan de réponse aux incidents doit contenir des politiques, des processus et des procédures clairement définis pour sa mise en œuvre.

8.15 Conformément au sous-alinéa 5(1)i)(iii) du *Règlement*, dans le cadre de son enquête, le FSP doit établir ce qui suit à l'égard de l'incident :

- sa cause première
- ses répercussions possibles ou avérées sur les activités associées aux paiements de détail (p. ex., interruptions et nombre d'opérations touchées)
- ses répercussions possibles ou avérées sur les utilisateurs finaux
- ses répercussions possibles ou avérées sur les autres FSP et sur les chambres de compensation des systèmes de compensation et de règlement qui ont été désignés en vertu du paragraphe 4(1) de la *Loi sur la compensation et le règlement des paiements*
- ses répercussions possibles ou avérées sur les systèmes, données et renseignements engagés dans l'exécution des activités associées aux paiements de détail

8.16 Lorsqu'un incident a des répercussions importantes sur un utilisateur final, un FSP ou une chambre de compensation, le FSP doit le signaler sans délai aux personnes physiques ou entités ayant subi des répercussions importantes ainsi qu'à la Banque du Canada, conformément à l'article 18 de la LAAPD. Voir la ligne directrice *La déclaration des incidents*.

8.17 Lorsqu'un tiers fournisseur de services ou un mandataire décèle un incident, une anomalie ou une défaillance dans la mise en œuvre du cadre, il incombe au FSP de déterminer s'il s'agit d'un incident qui le concerne. Si c'est le cas, il est tenu d'enquêter sur cet incident.

8.18 Conformément à son plan de réponse aux incidents, lorsqu'il répond à un incident, le FSP doit :

- appliquer les mesures d'atténuation prédéterminées, comme les processus manuels ou les solutions de rechange, selon les besoins, pour réduire les répercussions de l'incident (sous-alinéa 5(1)i)(ii) du *Règlement*)
- prendre des mesures immédiates visant à prévenir ou réduire toute autre atteinte pendant qu'une enquête est en cours, notamment à l'intégrité, à la confidentialité ou à la disponibilité des systèmes, données et renseignements (sous-alinéa 5(1)i)(iv) du *Règlement*)
  - Par exemple, selon la nature de l'incident, le FSP peut être amené à interrompre ses activités associées aux paiements de détail ou à révoquer certains privilèges ou accès d'utilisateurs à certains systèmes ou données.
  - Si le FSP voit la disponibilité, l'intégrité ou la confidentialité de ses données compromise et qu'il continue d'exercer ses activités associées aux paiements de détail tout en enquêtant sur l'incident et en le réglant, il doit confirmer qu'il est capable d'endiguer le problème (p. ex., mettre les données compromises en quarantaine) pour prévenir toute autre atteinte.
- déterminer l'état des opérations au moment de toute interruption du service, récupérer les données perdues ou corrompues et régler les problèmes d'intégrité (sous-alinéa 5(1)i)(vii) du *Règlement*)
- considérer la nécessité de coordonner sa réponse avec celle d'un tiers fournisseur de services, s'il y a lieu (sous-alinéa 5(1)i)(i) du *Règlement*)
- mettre en œuvre aussitôt que possible des mesures permettant de traiter la cause première établie par l'enquête (sous-alinéa 5(1)i)(v) du *Règlement*)
  - Cette exigence inclut la mise en œuvre, en temps opportun, de toute mesure nécessaire à la préservation de l'intégrité, de la confidentialité et de la disponibilité de ses activités associées aux paiements de détail ainsi qu'aux systèmes, données ou renseignements qui permettent ou facilitent ces activités.

8.19 En plus de s'attaquer à la cause première de l'incident, le FSP devrait tenir compte des éventuelles leçons qu'il a tirées après avoir réglé un incident. Il doit notamment remédier aux vulnérabilités ou aux lacunes décelées lors de l'enquête, notamment dans le plan de réponse aux incidents ou sa mise en œuvre. Le FSP doit prioriser la correction des vulnérabilités ou des lacunes qui l'empêcheraient d'atteindre ses objectifs, ses cibles de fiabilité ou ses exigences réglementaires.

Documents

8.20 Conformément au sous-alinéa 5(1)i)(viii) du *Règlement*, le plan doit exiger que le FSP tienne, pour chaque incident, un document où sont consignés :

- les renseignements sur la cause première de l'incident et ses répercussions possibles ou avérées, telles que déterminées par l'enquête
- les mesures prises pour atténuer les répercussions de l'incident, pour prévenir ou atténuer toute autre atteinte pendant qu'une enquête est en cours et pour traiter la cause première établie par l'enquête
- la façon dont le FSP a signalé l'incident et coordonné la réponse à l'incident
- l'état des opérations relevées ainsi que les démarches qui ont permis de déterminer cet état, de récupérer toute donnée perdue ou corrompue et de régler tout problème d'intégrité de données

8.21 Le FSP doit consigner tous les aspects de l'enquête, des mesures, des mesures planifiées et des résultats relatifs à chaque incident.

9. Examen interne

Cette section fournit des indications sur l'article 8 du *Règlement*.

Résultats

- Le FSP examine son cadre de gestion des risques et de réponse aux incidents au moins une fois par année et avant de faire une modification importante à ses activités ou à sa gestion des risques opérationnels.
- Le FSP fait rapport des résultats de chaque examen au cadre dirigeant et prend des mesures pour corriger les lacunes ou les vulnérabilités décelées par l'examen.

Indications

9.1 Conformément au paragraphe 8(1) du *Règlement*, le FSP doit mener un examen de son cadre dans chacun des cas suivants :

- au moins une fois par année
- avant d'apporter une modification importante à ses activités ou à ses systèmes, politiques, procédures, processus, contrôles ou autres moyens de gestion des risques opérationnels

9.2 Le paragraphe 8(2) du *Règlement* précise que l'examen doit évaluer :

- la conformité du cadre avec les exigences de l'article 5 du *Règlement*
- l'efficacité du FSP à atteindre ses objectifs d'intégrité, de confidentialité et de disponibilité, compte tenu de ses cibles et indicateurs
- le caractère adéquat des ressources financières et humaines du FSP pour la mise en œuvre du cadre

9.3 Les examens annuels doivent avoir une grande portée afin d'englober la conformité générale du cadre avec les normes exigées par la LAAPD et le *Règlement*. Ils doivent notamment évaluer l'exhaustivité, l'adéquation et l'efficacité du cadre en ce qui concerne l'identification et l'atténuation des risques opérationnels et la réponse aux incidents, compte tenu de la situation du FSP. Dans ce contexte, la portée de l'examen doit inclure, au minimum, tous les éléments suivants :

- la capacité du FSP à atteindre ses objectifs d'intégrité, de confidentialité et de disponibilité
- l'adéquation et l'efficacité générales du cadre pour ce qui est de recenser, protéger et déceler les risques opérationnels et les incidents, de même que pour répondre aux incidents et s'en rétablir
- la suffisance des rôles et responsabilités répartis ainsi que l'adéquation des ressources humaines et financières
- les arrangements pris par le FSP pour évaluer et atténuer les risques provenant de tiers fournisseurs de services et de mandataires

9.4 Les examens internes effectués avant une modification importante (aux activités du FSP ou à son environnement opérationnel) doivent servir à ce que les modifications n'entravent pas la capacité du FSP à atténuer les risques ou à répondre aux incidents. Les examens du cadre qui précèdent une modification importante peuvent être plus ciblés, se concentrant sur les éléments pertinents ou touchés par la modification.

9.5 Conformément au paragraphe 8(3) du *Règlement*, pour chaque examen, le FSP doit tenir un document où sont consignés :

- la date de l'examen
- sa portée
- sa méthodologie
- ses résultats

9.5.1 En ce qui concerne la méthodologie de l'examen interne, le document doit inclure les facteurs et les sources d'information pris en compte. Voir l'annexe G pour en savoir plus sur les sources d'information et les facteurs qu'un FSP pourrait considérer dans le cadre de son examen.

9.5.2 En ce qui concerne les résultats de l'examen, le document doit inclure tous les résultats, comme les lacunes ou les vulnérabilités, issus de l'examen.

9.6 Si l'examen permet de déceler des lacunes, des vulnérabilités ou des points à améliorer, le FSP doit mettre à jour son cadre en temps opportun afin de pouvoir continuer à satisfaire aux exigences en matière de risque opérationnel et de réponse aux incidents établies dans la LAAPD et le *Règlement*.

9.6.1 Conformément au paragraphe 8(4) du *Règlement*, le FSP doit faire rapport des résultats de chaque examen au cadre dirigeant, s'il y en a un, pour approbation par ce dernier.

9.6.2 La Banque encourage le FSP à adopter une approche fondée sur les risques pour hiérarchiser les mesures correctives à prendre en réponse aux vulnérabilités, aux lacunes ou aux points à améliorer, en tenant compte de l'importance des risques qui en découlent.

10. Mises à l'essai

Cette section fournit des indications sur l'article 9 du *Règlement*.

Résultats

- Le FSP met en œuvre un programme de mise à l'essai afin de déceler les lacunes dans son cadre de gestion des risques et de réponse aux incidents.
- Les intéressés pertinents participent activement aux essais.
- Le FSP prend des mesures pour combler les lacunes et les vulnérabilités décelées pendant les essais.

Indications

Objectifs

10.1 Conformément au paragraphe 9(1) du *Règlement*, le FSP doit établir et mettre en œuvre une méthode de mise à l'essai afin de déceler toute lacune dans l'efficacité des systèmes, politiques, procédures, processus, contrôles et autres moyens prévus par le cadre de gestion des risques et de réponse aux incidents et aussi afin d'en déceler les vulnérabilités. Le FSP doit s'assurer que sa méthode de mise à l'essai :

- est en proportion aux répercussions que pourraient avoir une entrave ou une perturbation à ses activités associées aux paiements de détail – ou une interruption de ces activités – sur les utilisateurs finaux et les autres FSP, compte tenu notamment de son ubiquité et interconnexion
- est conçue compte tenu à la fois des risques opérationnels ayant une forte probabilité de survenir et de ceux ayant des répercussions graves
- prévoit l'utilisation d'essais qui engagent les intéressés internes pertinents, notamment les mandataires, les décideurs et les personnes physiques responsables de la gestion des risques opérationnels du FSP
- tient compte de la dépendance du FSP aux intéressés externes, notamment les tiers fournisseurs de services
- prévoit la fréquence et la portée des mises à l'essai
- prévoit la mise à l'essai avant que ne soit apportée toute modification importante à ces systèmes, politiques, procédures, processus, contrôles ou autres moyens – ou à une opération du FSP qui y toucherait – afin d'en évaluer les effets

Méthode, portée, fréquence et proportionnalité des mises à l'essai

10.2 Le FSP doit consigner par écrit sa méthode de mise à l'essai et s'assurer qu'elle fournit une approche structurée concernant chacun des éléments suivants :

- la portée des mises à l'essai
- la méthode de mise à l'essai, y compris la justification de la méthode choisie pour chaque essai
- la fréquence des mises à l'essai
- les principes qui demanderaient la participation de certains intéressés à un ou plusieurs essais
- les processus de communication interne des résultats de chaque essai

- les principes guidant toute réaction aux résultats des essais, notamment pour déterminer si, comment et quand le FSP doit remédier aux lacunes ou aux vulnérabilités décelées

10.3 La portée des mises à l'essai (p. ex., les systèmes, politiques, procédures, processus, contrôles et autres moyens soumis aux essais) doit être suffisamment large pour déceler les défaillances dans le cadre de gestion des risques et de réponses aux incidents du FSP.

10.4 Le FSP doit adopter une approche fondée sur les risques en ce qui concerne la portée et la fréquence des mises à l'essai. Plus un système, une politique, une procédure, un processus, un contrôle ou un autre moyen est important, plus sa mise à l'essai doit être fréquente et approfondie. Le FSP doit aussi prioriser la mise à l'essai des éléments de son cadre dont le risque inhérent est élevé. Cela comprend les situations particulières où une défaillance des systèmes, politiques, procédures, processus, contrôles ou autres moyens aurait pour répercussions potentielles l'entrave, la perturbation ou l'interruption des activités associées aux paiements de détail du FSP.

10.5 Quant au principe de proportionnalité, l'approche générale appliquée à la méthode de mise à l'essai doit être appropriée au niveau d'ubiquité et d'interconnexion du FSP. Autrement dit, le FSP ayant une ubiquité ou une interconnexion relativement grande doit réaliser des essais plus nombreux et approfondis.

Types d'essais

10.6 La Banque s'attend à ce que la méthode de mise à l'essai couvre trois grandes catégories d'essais afin de satisfaire aux exigences réglementaires :

10.6.1 Vérification et validation des contrôles : ces essais sont spécialement axés sur l'évaluation de l'efficacité et la détection des lacunes dans les différents éléments qui constituent le cadre (comme les systèmes, les politiques, les procédures, les processus et les contrôles), y compris les lacunes dans la manière dont ces éléments ont été établis, mis en œuvre ou maintenus.

10.6.2 Essais basés sur des scénarios : ces essais doivent être conçus pour évaluer si le cadre du FSP (y compris la planification de la gestion des incidents) préservera l'intégrité, la confidentialité et la disponibilité des deux éléments suivants :

- les activités associées aux paiements de détail du FSP
- les systèmes, données ou renseignements qui permettent ou facilitent ces activités
  - Le FSP doit concevoir son programme de mise à l'essai pour couvrir divers scénarios au fil du temps, afin d'évaluer le fonctionnement des éléments clés du cadre.
  - Pour cette catégorie d'essais, il est particulièrement important de tenir compte des risques opérationnels ayant une forte probabilité de survenir et de ceux ayant des répercussions graves.

10.6.3 Essais relatifs aux modifications : la mise à l'essai est un élément fondamental de la gestion du changement. Elle fait en sorte que le cadre restera adéquat et efficace après qu'une modification importante est apportée aux activités ou aux systèmes, politiques, procédures, processus, contrôles ou autres moyens du FSP. La portée de ces essais doit couvrir les éléments du cadre et des activités qui seront touchés par la modification.

10.7 Dans chaque catégorie d'essai, le FSP doit utiliser diverses pratiques afin que chaque essai puisse déceler les lacunes d'efficacité ou les vulnérabilités du système, de la politique, de la procédure, du processus ou du contrôle pertinent. Le FSP doit choisir ses pratiques de mise à l'essai en fonction de ses activités opérationnelles et de ses activités associées aux paiements de détail.

10.8 Voir l'annexe H pour en savoir plus sur les types d'essais.

Intéressés

10.9 En vertu des sous-alinéas 9(1)c)(i) et (ii) du *Règlement*, le FSP doit effectuer des essais qui :

- « engagent les intéressés internes pertinents, notamment les mandataires, les décideurs et les personnes physiques responsables de la gestion des risques opérationnels du fournisseur de services de paiement;
- « tiennent compte de la dépendance du fournisseur de services de paiement aux intéressés externes, notamment les tiers fournisseurs de services. »

10.10 Pour déterminer les intéressés internes, les décideurs et les personnes physiques responsables de la gestion des risques opérationnels à engager dans un essai et pour établir le degré d'engagement de chacun d'entre eux, le FSP doit prendre en compte les éléments suivants :

- la nature et l'objectif de l'essai effectué
- la répartition des rôles et responsabilités pour l'établissement, la mise en œuvre et le maintien de son cadre, ou pour le système, la politique, la procédure, le processus ou le contrôle précis mis à l'essai

10.11 Les FSP qui ont recours à des mandataires devraient les inclure dans la portée de leurs essais, notamment lorsque ces mandataires établissent, mettent en œuvre ou maintiennent les éléments du cadre qui sont mis à l'essai (tels que les systèmes, les politiques, les procédures, les processus ou les contrôles).

10.12 Lors des essais, le FSP doit également tenir compte de sa dépendance à l'égard des intéressés externes, y compris les tiers fournisseurs de services ou d'autres tiers.

10.13 Par exemple, la mise à l'essai du plan de réponse aux incidents du FSP pourrait avoir pour objectif de vérifier le degré de préparation organisationnelle, notamment dans quelle mesure les intéressés comprennent le plan et seront capables de le mettre en œuvre s'il le faut. Dans cet exemple, pour être le plus efficace possible, l'essai devrait engager tous les intéressés qui jouent un rôle dans la mise en œuvre du plan de réponse aux incidents. Voici des éléments pouvant être pris en considération :

- les mandataires qui exercent un rôle ou une responsabilité concernant le plan de réponse aux incidents
- les hypothèses émises sur la disponibilité des services ou des ressources qui dépendent de tiers fournisseurs de services ou d'autres parties externes

Résultats des essais

10.14 Après un essai, le FSP doit tirer des leçons et déterminer s'il lui faut bonifier ou modifier son cadre, ses systèmes, ses politiques, ses procédures, ses processus et ses contrôles.

10.15 Le FSP doit prendre des mesures en temps opportun pour corriger les lacunes et vulnérabilités afin de pouvoir continuer à satisfaire aux exigences en matière de risque opérationnel définies à l'article 17 de la LAAPD et à l'article 9 du *Règlement*. La Banque s'attend à ce qu'il adopte une approche fondée sur les risques pour hiérarchiser et mettre en œuvre les mesures à prendre dans ce contexte.

10.16 Le FSP doit également se demander s'il y a lieu d'évaluer la possibilité que la lacune ou la vulnérabilité ait été exploitée avant d'être détectée et corrigée.

10.17 Lorsque les essais effectués avant une modification importante indiquent des lacunes ou des vulnérabilités, la Banque attend du FSP qu'il évalue la nécessité de les corriger avant la mise en œuvre de cette modification importante et qu'il en consigne les résultats, s'il y a lieu.

Documents

10.18 En vertu du paragraphe 9(2) du *Règlement*, le FSP doit tenir un document où sont consignés les renseignements suivants :

- la date de chaque essai
- la méthode utilisée pour chaque essai, notamment une explication indiquant en quoi l'essai est conforme aux exigences consistant à engager les intéressés internes pertinents et à tenir compte de la dépendance du FSP aux intéressés externes
- le résultat de l'essai
- toute mesure corrective prise ou à prendre

10.19 En ce qui concerne la méthode utilisée, le document doit indiquer la portée de l'essai, comme les systèmes informatiques et les activités associées aux paiements de détail sur lesquels l'essai a été effectué, ainsi que les facteurs et les sources d'information pris en compte. En ce qui concerne le résultat, le document doit inclure l'analyse par le FSP des lacunes et des vulnérabilités décelées et les raisons pour lesquelles il n'a pas corrigé certaines lacunes ou vulnérabilités, le cas échéant.

10.20 Le paragraphe 9(3) du *Règlement* indique que le FSP doit veiller à ce que le document mentionné ci-dessus soit fourni au cadre dirigeant, s'il y en a un.

11. Examen indépendant

Cette section fournit des indications sur l'article 10 du *Règlement*.

Résultats

- Si le FSP dispose d'un auditeur interne ou externe, une ressource indépendante et compétente doit procéder à l'examen indépendant.
- Le FSP prend des mesures pour corriger les lacunes et les vulnérabilités du cadre de gestion des risques et de réponse aux incidents qui sont décelées pendant les examens indépendants.

Indications

Objectifs, méthodologie et portée

11.1 Conformément au paragraphe 10(1) du *Règlement*, le FSP qui dispose d'un auditeur interne ou externe doit veiller à ce que, au moins une fois tous les trois ans, une personne physique compétente qui n'a pas participé à l'établissement, à la mise en œuvre ou au maintien du cadre de gestion des risques et de réponse aux incidents effectue un examen indépendant des éléments suivants :

- la conformité de chaque élément du cadre de gestion des risques et de réponse aux incidents aux exigences applicables de l'article 5 du *Règlement*;
- la conformité du FSP à chaque exigence prévue aux articles 6 à 9 du *Règlement*.

11.2 L'examen indépendant doit évaluer dans quelle mesure le cadre, y compris sa mise en œuvre et son maintien, est conforme à tous les aspects des exigences en matière de risque opérationnel et de réponse aux incidents définies dans la LAAPD et son règlement d'application.

11.2.1 En particulier, l'examen indépendant doit fournir l'assurance que le FSP est capable de recenser et d'atténuer les risques opérationnels et de répondre aux incidents d'une manière efficace qui lui permet d'atteindre ses objectifs d'intégrité, de confidentialité et de disponibilité. L'examen indépendant doit porter sur l'exhaustivité et l'efficacité du cadre, notamment en vérifiant si le cadre (et les systèmes, politiques, procédures, processus, contrôles et autres éléments qui le composent) a été établi, mis en œuvre et maintenu comme prévu.

11.2.2 Si le FSP fait appel à des tiers fournisseurs de services ou à des mandataires, l'examen indépendant doit aussi porter sur les services fournis par ces parties ainsi que les précautions prises par le FSP pour sélectionner et évaluer ces parties.

11.3 Le FSP « dispose d'un auditeur externe » s'il fait régulièrement appel aux services d'un auditeur externe pour fournir une assurance indépendante, y compris pour la communication de l'information financière. Le recours ponctuel à un auditeur externe à des fins spécialisées, comme la réalisation d'essais précis, ne signifie pas que le FSP « dispose d'un auditeur externe ».

11.4 En vertu du paragraphe 10(1) du *Règlement,* l'examen indépendant doit être effectué par une personne physique compétente qui n'a pas participé à l'établissement, à la mise en œuvre ou au maintien du cadre du FSP.

11.5 L'obligation de procéder à un examen indépendant vient compléter, sans remplacer, l'obligation du FSP d'examiner son cadre au moins une fois par année (prévue au paragraphe 8(1) du *Règlement*).

11.5.1 Néanmoins, les résultats de l'examen indépendant peuvent être utilisés dans le cadre de l'examen interne du FSP. Voir la section Examen interne.

11.6 Selon le cas, le FSP peut utiliser les résultats d'un audit ou d'un examen indépendant effectué à d'autres fins (p. ex., certification indépendante, rapport sur des systèmes ou contrôles organisationnels) pour satisfaire à l'obligation d'examen indépendant. Il doit alors démontrer par écrit que la portée de cet audit ou examen indépendant correspond aux exigences du *Règlement* et englobe les activités associées aux paiements de détail du FSP ainsi que les actifs, processus opérationnels, données, systèmes d'information ou cadres connexes. Si sa portée ne correspond pas aux exigences ou est incomplète, le FSP doit procéder à un autre examen indépendant pour traiter les éléments omis des vérifications existantes.

Résultats de l'examen indépendant

11.7 L'examen indépendant doit déceler toute lacune ou vulnérabilité dans le cadre du FSP, notamment l'absence de systèmes, politiques, procédures, contrôles ou autres éléments du cadre ainsi que les faiblesses relatives à tous ces éléments, à leur établissement, à leur mise en œuvre ou à leur maintien.

11.8 À la suite de l'examen indépendant, le FSP doit relever les leçons tirées et déterminer les lacunes ou les vulnérabilités nécessitant des ajouts ou des modifications à son cadre. Le FSP doit mettre en œuvre toutes les modifications nécessaires à son cadre pour pouvoir continuer de satisfaire aux exigences en matière de risque opérationnel et de réponse aux incidents établies dans la LAAPD et le *Règlement*. Cela comprend sa capacité à atteindre ses objectifs en matière d'intégrité, de confidentialité et de disponibilité. La Banque attend du FSP qu'il adopte une approche fondée sur les risques pour hiérarchiser et mettre en œuvre les mesures découlant d'un examen indépendant.

11.9 Conformément au paragraphe 10(3) du *Règlement*, le FSP doit faire rapport au cadre dirigeant de toute lacune ou vulnérabilité décelée par l'examen indépendant ainsi que de toutes mesures correctives.

11.10 Le FSP doit vérifier que les mesures correctives ont été mises en œuvre comme prévu (p. ex., dans le cadre du prochain examen interne ou indépendant).

Documents

11.11 Conformément au paragraphe 10(2) du *Règlement*, « le fournisseur de services de paiement obtient un document où sont consignés le nom de l'examinateur – ou, si l'examinateur a effectué l'examen pour le compte d'une entité autre que le fournisseur de services de paiement, le nom de cette entité –, la date de l'examen et une description de la portée, de la méthodologie et des résultats de l'examen ».

12. Tiers fournisseurs de services

Cette section fournit des indications sur le paragraphe 5(3) du *Règlement*.

Résultats

- Le cadre de gestion des risques et de réponse aux incidents du FSP permet de gérer les risques découlant du recours à un tiers fournisseur de services.
- Le FSP détermine l'importance de faire appel à un tiers fournisseur de services pour obtenir les services requis et ajuste en conséquence ses processus d'évaluation et de surveillance du fournisseur de services.
- Le FSP évalue les risques entourant le recours à un tiers fournisseur de services tous les ans ainsi qu'avant de conclure, renouveler, proroger ou modifier substantiellement un contrat avec ce tiers.
- Les responsabilités sont clairement réparties entre le FSP et le tiers fournisseur de services.
- Le FSP met en place des contrôles compensatoires, selon le cas, pour s'assurer qu'il reste conforme aux exigences réglementaires lorsqu'il fait appel à des tiers fournisseurs de services.
- Le FSP surveille le rendement du tiers fournisseur de services pour s'assurer de sa capacité à fournir des services comme prévu et en conformité avec les objectifs du FSP et les exigences réglementaires.

Indications

Champ d'application à l'égard des tiers fournisseurs de services

12.1 Aux termes de l'article 2 de la LAAPD, un tiers fournisseur de services est une personne physique ou une entité qui fournit à un FSP un service lié à une fonction de paiement au titre d'un contrat et qui n'est pas l'un de ses employés ni l'un de ses mandataires.

12.1.1 La présente ligne directrice se concentre sur les tiers fournisseurs de services qui offrent des services pertinents à la situation de conformité du FSP relativement à la LAAPD et au *Règlement*. La Banque estime qu'il s'agit généralement de services qui, s'ils étaient altérés ou défaillants, entraîneraient ou pourraient raisonnablement entraîner une entrave, une perturbation ou une interruption de la capacité du FSP à exercer ses activités associées aux paiements de détail ou à recenser et atténuer ses risques opérationnels et à répondre aux incidents. Voir l'annexe I pour obtenir des exemples de services qui peuvent être liés à une fonction de paiement.

12.1.2 Les services exacts liés aux fonctions de paiement d'un FSP dépendent du FSP et de ses ententes. Dans tous les cas, chaque FSP doit évaluer lesquels de ses tiers fournisseurs de services répondent aux critères d'application.

12.1.3 Les services qui ne sont que secondaires à l'exercice des activités associées aux paiements de détail du FSP, ou secondaires à sa gestion du risque opérationnel, peuvent être considérés comme exclus de ces exigences (p. ex., elles peuvent exclure les tiers fournisseurs de services qui soutiennent seulement les ventes, la publicité ou la paie ou qui fournissent seulement des services juridiques).

12.2 La définition d'un tiers fournisseur de services englobe :

- les entités affiliées au FSP qui, en vertu d'un contrat, lui fournissent un service lié à une fonction de paiement qu'il exécute

- les autres FSP (visés ou non par la LAAPD) qui, en vertu d'un contrat, lui fournissent un service lié à une fonction de paiement qu'il exécute, y compris les FSP qui fournissent un accès à des services bancaires liés à la détention de fonds
- les personnes physiques (c.-à-d. tout individu) et les entités qui fournissent des services dans le cadre d'un contrat
- n'importe quel lieu géographique où seraient situés le tiers fournisseur de services ou les technologies qu'il utilise pour fournir des services au FSP

12.3 Lorsque le FSP s'appuie sur une entité affiliée pour exercer des activités associées aux paiements de détail ou gérer le risque opérationnel, la Banque recommande que leur relation soit régie par une entente contractuelle. Le FSP doit donc traiter l'entité affiliée comme un tiers fournisseur de services. Toutefois, qu'il y ait entente contractuelle ou non, le FSP doit utiliser son cadre pour gérer les risques associés à une entité affiliée ou à tout autre tiers, conformément à la LAAPD.

Gestion des risques associés aux tiers

12.4 Conformément à son obligation de recenser les risques opérationnels, le FSP doit recenser et atténuer les risques liés au recours à des tiers fournisseurs de services. Ainsi, il doit traiter du recours à des tiers fournisseurs de service dans son cadre (en vertu des alinéas 5(1)f) et g) du *Règlement*).

12.5 Cela dit, la présente section de la ligne directrice concerne précisément les ententes que le FSP doit établir, mettre en œuvre et maintenir pour comprendre, évaluer et surveiller ses relations avec des tiers et les risques opérationnels connexes. Le FSP doit établir, mettre en œuvre et maintenir des mécanismes pour :

- comprendre l'importance du recours à un tiers fournisseur de services et la façon dont cela modifie son profil de risque
- évaluer les tiers fournisseurs de services avant de faire appel à leurs services, notamment en ce qui concerne leurs pratiques de gestion des risques et leur rendement opérationnel
- établir des contrats avec les tiers fournisseurs de services et répartir clairement les rôles et les responsabilités, y compris en ce qui concerne la propriété, l'intégrité, la confidentialité et la disponibilité des données et renseignements
- évaluer et surveiller les tiers fournisseurs de services engagés
- créer des contrôles compensatoires, s'il y a lieu, y compris des plans de résiliation

12.6 Nous explorons chacun de ces mécanismes plus en détail dans les sections suivantes.

12.7 Le FSP doit respecter les exigences réglementaires, y compris lorsqu'il fait appel à des tiers fournissant des services liés à ses activités associées aux paiements de détail. En vertu de l'article 87 de la LAAPD, le FSP est responsable de la violation commise par un tiers fournisseur de services dans le cadre de son contrat.

12.8 Le FSP ne doit pas recourir à des tiers fournisseurs de services d'une manière qui entraverait la capacité de la Banque à surveiller sa conformité avec la LAAPD. De plus, il doit être en mesure de satisfaire à toutes les exigences de déclaration, y compris en ce qui concerne les documents et les demandes de renseignements.

12.9 Le recours à un tiers fournisseur de services ou les changements entourant le recours à un tiers fournisseur de services peuvent être considérés comme un changement important et doivent, entre autres, être déclarés à la Banque du Canada (voir le paragraphe 22(2) de la LAAPD). Pour en savoir plus, voir la ligne directrice *Les avis de changement important ou d'activité nouvelle*.

Importance du service confié à un tiers

12.10 Avant d'engager un tiers fournisseur de services pour un service lié à une fonction de paiement, le FSP doit comprendre l'importance que revêt ce service dans le cadre de ses activités associées aux paiements de détail. Pour ce faire, il doit évaluer les répercussions que subiraient ces activités en cas d'altération du service en question. Le FSP doit élaborer une approche officialisée et documentée pour évaluer l'importance des services qu'il compte confier à des tiers.

12.11 Cette détermination de l'importance d'un service doit contribuer à l'approche fondée sur les risques qu'emploie le FSP pour gérer les risques associés aux tiers; elle doit influencer la rigueur des évaluations visant les tiers fournisseurs de services, des activités de passation de contrats, de surveillance et de résiliation ainsi que de tout contrôle compensatoire appliqué par le FSP.

12.12 Le FSP doit réviser périodiquement l'importance des services qu'il reçoit de tiers fournisseurs de services pour déterminer si la nature de ces services demeure ou devient importante dans le cadre de ses activités associées aux paiements de détail.

Évaluation des tiers fournisseurs de services

Objectifs, méthodologie et portée

12.13 Les sous-alinéas 5(3)a)(i) à (v) du *Règlement* précisent que si un FSP obtient d'un tiers fournisseur de services des services liés à une fonction de paiement, le cadre du FSP doit établir comment le FSP évaluera :

- « la capacité du tiers fournisseur de services à protéger les données et les renseignements obtenus du fournisseur de services de paiement ou en exécutant des services pour lui,
- « la sécurité des connexions du tiers fournisseur de services à destination et en provenance des systèmes du fournisseur de services de paiement,
- « la manière dont le tiers fournisseur de services informe ou consulte le fournisseur de services de paiement avant de modifier ses services, le mode de prestation de ses services ou ses pratiques de gestion des risques opérationnels,
- « la manière dont le rendement du tiers fournisseur de services peut être surveillé, notamment les modalités selon lesquelles ce dernier préviendrait le fournisseur de services de paiement lorsqu'il détecte une atteinte à ses données, renseignements ou systèmes ou à ceux du fournisseur de services de paiement, ou toute autre réduction, détérioration ou défaillance des services fournis au fournisseur de services de paiement,
- « les pratiques de gestion des risques du tiers fournisseur de services relatives aux services que celui-ci fournit au fournisseur de services de paiement ».

12.14 Le FSP doit établir, mettre en œuvre et maintenir une approche officialisée et documentée pour évaluer les tiers fournisseurs de services.

12.15 En menant par précaution des évaluations détaillées (diligence raisonnable), le FSP améliore sa compréhension de ce qui suit :

- les arrangements pris par le tiers fournisseur de services en matière de gestion des risques
- le rendement réel du tiers fournisseur de services ainsi que sa capacité à fournir les services demandés, y compris son expérience, ses capacités techniques, sa solidité financière et son efficacité opérationnelle
- les risques auxquels le FSP s'expose en recourant à un tiers fournisseur de services et les conséquences sur sa conformité à la LAAPD

12.16 Par exemple, en ce qui a trait aux arrangements pris par le tiers fournisseur de services en matière de gestion des risques, il est particulièrement important que le FSP comprenne :

- les cibles de fiabilité et les indicateurs opérationnels du tiers fournisseur de services, son rendement par rapport à ces cibles et indicateurs, et les moyens de surveillance entourant les services à fournir au FSP
- l'environnement de contrôle interne lié aux services que le tiers fournisseur de services fournit au FSP
- les arrangements pris par le tiers fournisseur de services en matière de gestion des risques liés à la sécurité de l'information et à la cybersécurité et la manière dont il contrôle et met à l'essai sa propre application de son cadre de sécurité de l'information et de cybersécurité
- les arrangements pris par le tiers fournisseur de services pour réagir en cas d'atteinte à ses données, renseignements et systèmes ou à ceux du FSP, ou en cas de toute autre réduction, détérioration ou défaillance des services fournis au FSP ou en son nom, et pour s'en rétablir
    - Le FSP doit examiner l'aide que pourrait lui apporter le tiers fournisseur de services advenant une telle atteinte.
- les mesures de gestion de la continuité des activités et de reprise après sinistre, ainsi que leur mise à l'essai par le tiers fournisseur de services
- les accords de sous-traitance, c'est-à-dire la dépendance du tiers fournisseur de services envers des sous-traitants et la manière dont il gère le risque découlant de son propre recours à des tiers (risque lié aux sous-traitants), ce qui peut influencer la capacité du FSP à contrôler le rendement du tiers fournisseur de services
- les processus mis en place par le tiers fournisseur de services pour vérifier son respect des normes du secteur, ainsi que des normes industrielles auxquelles il adhère

12.17 L'annexe I présente des exemples d'outils et de ressources pouvant être utilisés par le FSP pour recueillir des renseignements à l'appui de son évaluation d'un tiers fournisseur de services, et des exemples de facteurs à prendre en considération lors de cette évaluation.

12.18 Le FSP doit également évaluer la manière dont il sera informé des changements apportés chez le tiers fournisseur de services qui sont applicables aux services qu'il reçoit, et la manière dont il surveillera le rendement du tiers fournisseur de services.

Approche fondée sur les risques

12.19 Dans le contexte d'une approche fondée sur les risques, le FSP peut adapter sa méthode d'évaluation s'il continue à satisfaire à toutes les exigences réglementaires visées au paragraphe 5(3) du *Règlement*. Autrement dit, il peut adapter la profondeur des évaluations à l'importance du tiers fournisseur de services.

12.19.1 Dans ce contexte, l'approche fondée sur les risques doit permettre au FSP de se concentrer sur les tiers fournisseurs de services qui présentent le plus grand risque tout en assurant une surveillance suffisante des autres tiers fournisseurs de services. Par exemple, dans le cas d'une entente qui est jugée non importante, il peut être approprié que le FSP suive un processus d'évaluation simplifié pour ne traiter que les exigences principales.

12.19.2 Certains tiers fournisseurs de services sont des entités réglementées. Si la réglementation du tiers fournisseur de services s'applique au service que cette entité fournit au FSP (surtout si elle est réglementée pour des risques semblables à ceux visés à l'article 17 de la LAAPD), le FSP peut en tenir compte pour déterminer le degré d'évaluation à réaliser auprès de ces entités.

12.19.3 Le FSP peut également adopter une approche sur mesure pour évaluer les tiers fournisseurs de services qui sont des entités affiliées.

Fréquence

12.20 Conformément à l'alinéa 5(3)a) du *Règlement*, le cadre du FSP doit indiquer comment le FSP compte effectuer ces évaluations au moins une fois par année à l'égard de chacun de ses tiers fournisseurs de services, et avant de conclure, renouveler, proroger ou modifier substantiellement un contrat avec le tiers fournisseur de services dans le cadre d'un service lié à une fonction de paiement.

12.20.1 Ainsi, en plus de l'évaluation qu'il effectue à l'égard du tiers fournisseur de services avant de conclure, renouveler, proroger ou modifier substantiellement un contrat avec lui, le FSP doit également évaluer chaque tiers fournisseur de services au moins une fois par année.

Documents

12.21 Conformément à l'alinéa 5(3)b) du *Règlement*, le cadre doit exiger que le FSP tienne un document où sont consignés les dates, la portée et le résultat des évaluations mentionnées ci-dessus.

12.22 Ce document doit également faire état des risques que le FSP recense dans le cadre de son recours à un tiers fournisseur de services, ainsi que de tout contrôle compensatoire que le FSP établit dans son propre cadre pour atténuer ces risques (voir également l'article 12.27 sous « Contrôles compensatoires » plus loin).

Passation de contrats et répartition des responsabilités

12.23 Lorsqu'il conclut, renouvelle, proroge ou modifie substantiellement un contrat avec un tiers fournisseur de services, le FSP doit se demander si l'entente contractuelle lui permettrait de rester assidu dans l'atteinte de ses objectifs d'intégrité, de confidentialité et de disponibilité et sa conformité aux exigences réglementaires.

12.24 En vertu de l'alinéa 5(3)c) du *Règlement*, le cadre du FSP doit « répartir clairement les responsabilités entre le fournisseur de services de paiement et le tiers fournisseur de services, notamment à l'égard de la propriété, de l'intégrité, de la confidentialité et de la disponibilité des données et renseignements ».

12.24.1 Le FSP doit s'assurer que la répartition des responsabilités entre le tiers fournisseur de services et lui-même est claire et documentée. La Banque s'attend à ce que cette répartition soit expliquée dans le contrat qui lie le FSP au tiers fournisseur de services.

12.25 L'annexe I présente des exemples de modalités que le FSP est encouragé à envisager dans le cadre d'une entente contractuelle avec un tiers fournisseur de services.

12.26 Le FSP doit également veiller à réaliser périodiquement un examen formel des ententes (p. ex., révision de contrat) afin de s'assurer qu'elles restent adéquates.

Contrôles compensatoires

12.27 Toutefois, les contrats ne constituent pas à eux seuls des contrôles suffisants. La capacité à établir sur mesure des modalités contractuelles spécifiques peut varier d'un FSP ou d'un tiers fournisseur de services à l'autre. Dans certains cas, le FSP peut être dans l'impossibilité de négocier toutes les modalités d'un contrat. Même lorsqu'elles sont négociées, ces modalités peuvent s'avérer insuffisantes pour atténuer les risques opérationnels découlant de la dépendance à un tiers fournisseur de services. Dans les deux cas, le FSP peut également devoir mettre en place des systèmes, politiques, procédures, processus ou contrôles supplémentaires (c.-à-d. des contrôles compensatoires) pour gérer ces risques.

12.28 Voici des exemples de contrôles compensatoires :

- un suivi élargi de la capacité du tiers fournisseur de services à continuer de fournir le service, notamment de sa situation financière et, s'il y a lieu, de sa situation réglementaire
- les contrôles et essais de sécurité continus réalisés par le FSP, comme la surveillance des données ou le contrôle et la mise à l'essai des interconnexions techniques avec les tiers fournisseurs de services
- l'intégration des tiers fournisseurs de services, ou des services qu'ils fournissent, au cadre de gestion des risques opérationnels du FSP (p. ex., inclure les services fournis dans la méthode de mise à l'essai du FSP, et inclure les entraves, perturbations ou interruptions de service dans le plan de réponse aux incidents)

12.29 L'élaboration de plans de résiliation constitue également un contrôle compensatoire essentiel pour gérer le risque d'une relation avec un tiers. Le FSP peut devoir mettre fin à sa relation avec un tiers fournisseur de services pour diverses raisons. Quelle que soit la raison, la Banque encourage le FSP à élaborer un plan de résiliation pour s'assurer qu'il sera toujours en mesure d'atteindre ses objectifs d'intégrité, de confidentialité et de disponibilité.

12.30 Le plan de résiliation pourrait prévoir ce qui suit :

- la capacité d'une nouvelle partie (un fournisseur de services particulier ou des ressources internes) à respecter les exigences de capacités, de ressources et de délais pour ces services ou ces activités
- les risques liés à sa mise en œuvre
- la capacité du FSP à atteindre ses objectifs de confidentialité, de disponibilité et d'intégrité
- la capacité du FSP à rester conforme aux exigences réglementaires

12.31 Le FSP doit consigner les contrôles compensatoires supplémentaires qu'il a mis en place pour atténuer les risques découlant des négociations contractuelles, notamment lorsqu'il n'a pas pu négocier des modalités spécifiques.

Surveillance

12.32 Il est attendu que le FSP évalue comment il surveillera le rendement de ses tiers fournisseurs de services et qu'il mène à bien cette surveillance (sous-alinéa 5(3)a)(iv) du *Règlement*).

12.33 La Banque s'attend à ce que le FSP surveille tous les tiers fournisseurs de services, y compris ceux qui sont des entités affiliées.

12.34 Les activités de surveillance doivent être conçues pour que :

- le tiers fournisseur de services continue à respecter les normes de service convenues de la manière attendue
- les objectifs du FSP soient atteints
- le FSP reste conforme aux exigences réglementaires

12.35 La surveillance doit aussi viser les atteintes aux données, renseignements ou systèmes du FSP ou du tiers fournisseur de services ainsi que toute autre réduction, détérioration ou défaillance des services fournis au FSP. La Banque encourage le FSP à surveiller le respect des modalités contractuelles par le tiers fournisseur de services, ainsi que son rendement par rapport aux cibles et aux ententes de prestation de services. La surveillance peut également aider le FSP à déceler des changements dans le niveau et le type de risques associés à sa relation avec le tiers fournisseur de services.

12.36 Dans le contexte d'une approche fondée sur les risques, le FSP doit adapter la rigueur de sa surveillance à l'importance du tiers fournisseur de services.

12.36.1 Le FSP doit surveiller étroitement les tiers fournisseurs de services importants, par exemple en augmentant la fréquence et la complexité de la surveillance ainsi que le nombre de ressources qui y sont consacrées.

12.36.2 Dans le cas d'un tiers fournisseur de services présentant un profil de risque moindre, une surveillance adéquate pourrait consister à contrôler son rendement opérationnel par rapport aux normes convenues et aux modalités contractuelles. Ce contrôle devrait être effectué au moins une fois par année.

12.36.3 Même si le tiers fournisseur de services est une entité réglementée, la Banque encourage le FSP à vérifier régulièrement que ce tiers demeure soumis au régime de réglementation applicable.

12.37 Parmi les mesures de surveillance, le tiers fournisseur de services doit aviser le FSP des problèmes et des incidents porteurs de risque, notamment s'il détecte des atteintes aux données, renseignements ou systèmes et toute autre réduction, détérioration ou défaillance des services. Le FSP doit s'assurer qu'il reçoit ces avis en temps opportun.

12.38 La surveillance peut également conduire à la détection d'incidents, d'anomalies ou de défaillances dans la mise en œuvre du cadre. Voir les sections Déceler et Réponse et rétablissement. Lorsqu'un tiers fournisseur de services informe le FSP d'une atteinte, d'une réduction, d'une détérioration ou d'une défaillance des services qu'il fournit, il incombe au FSP de déterminer si cet événement répond aux exigences de déclaration des incidents prévues à l'article 18 de la LAAPD. Voir la ligne directrice *La déclaration des incidents*.

12.39 Le FSP doit consigner les résultats des activités de surveillance. Il doit également en faire rapport au décideur concerné (y compris, le cas échéant, au cadre dirigeant) afin de faciliter la prise de décision concernant les pratiques de gestion des risques associés aux tiers.

13. Mandataires

Cette section fournit des indications sur le paragraphe 5(4) du *Règlement*.

Résultats

- Le cadre de gestion des risques et de réponse aux incidents du FSP permet de gérer les risques découlant du recours à un mandataire.
- Avant de conclure un accord, le FSP s'assure que ses mandataires répondent à un ensemble de critères de base en matière de gestion des risques opérationnels.
- Les responsabilités sont clairement réparties entre le FSP et son mandataire.
- Le FSP effectue des évaluations au moins une fois par année pour vérifier la capacité du mandataire à fournir ses services comme prévu et en conformité avec les objectifs du FSP et les exigences réglementaires.
- Le FSP met en place des contrôles compensatoires, s'il y a lieu, pour s'assurer qu'il reste conforme aux exigences réglementaires lorsqu'il fait appel à des mandataires.

Indications

Champ d'application à l'égard des mandataires

13.1 Dans le contexte de la LAAPD, un mandataire est une personne physique ou une entité qui a l'autorité d'exercer des activités associées aux paiements de détail en tant que mandataire d'un FSP enregistré. Dans ce type de relation, le FSP fait appel à une personne physique ou à une entité (le mandataire) pour qu'elle exécute des activités associées aux paiements de détail en son nom.

13.2 Conformément à ses obligations d'identification et d'atténuation des risques opérationnels, le FSP est tenu de recenser et d'atténuer les risques associés aux relations avec des mandataires. Le recours à des mandataires doit donc être traité dans son cadre.

13.3 Néanmoins, cette section concerne précisément les ententes que le FSP doit établir, mettre en œuvre et maintenir pour comprendre, contrôler et vérifier les pratiques de gestion des risques de ses mandataires. Le FSP doit établir, mettre en œuvre et maintenir des mécanismes pour :

- effectuer des évaluations détaillées des mandataires avant de faire appel à leurs services, afin de s'assurer qu'ils répondent à certains critères de base
- établir des ententes contractuelles appropriées avec les mandataires et répartir clairement les rôles et les responsabilités, y compris en ce qui concerne la propriété, l'intégrité, la confidentialité et la disponibilité des données et renseignements
- évaluer et surveiller les mandataires engagés
- créer des contrôles compensatoires, y compris des plans de résiliation

13.4 Nous examinons plus en détail chacun de ces mécanismes dans les sections qui suivent.

13.5 Le FSP doit satisfaire aux exigences réglementaires, y compris lorsque des services sont fournis en son nom par un mandataire. En vertu de l'article 87 de la LAAPD, le FSP est responsable des violations commises par ses mandataires dans le cadre de leur mandat.

13.6 Le recours à des mandataires ne doit pas se faire d'une manière qui altérerait la capacité de la Banque à surveiller la conformité du FSP à la LAAPD. De plus, le FSP doit être en mesure de satisfaire à toutes les

exigences de déclaration, y compris en ce qui concerne les documents et les demandes de renseignements.

Critères et évaluation des mandataires

Objectifs, méthodologie et portée

13.7 Selon l'alinéa 5(4)a) du *Règlement*, si le FSP prévoit faire appel à des mandataires pour l'exécution d'activités associées aux paiements de détail, son cadre doit « prévoir des critères de gestion des risques opérationnels que les mandataires doivent satisfaire ».

13.8 En définitive, l'objectif de ces critères doit être de garantir que le mandataire sera capable d'exercer des activités associées aux paiements de détail au nom du FSP d'une manière conforme aux exigences de gestion des risques opérationnels et de réponse aux incidents établies en vertu de l'article 17 de la LAAPD.

13.9 Les critères établis par le FSP dépendent de sa relation avec le mandataire. L'approche adoptée par le FSP pour élaborer ses critères peut varier en fonction de la nature de la relation.

13.10 Les critères du FSP doivent au moins porter sur les éléments suivants relativement au mandataire :

- ses dispositifs de gestion des risques liés aux technologies de l'information et à la cybersécurité, y compris la manière dont il contrôle et met à l'essai le respect de son propre cadre de gestion des risques liés aux technologies de l'information et à la cybersécurité
- ses dispositifs de gestion des incidents, y compris la manière dont il signalera les incidents au FSP
- ses cibles de fiabilité et indicateurs opérationnels, et son rendement en la matière
- ses plans de gestion de la continuité des activités et de reprise après sinistre, et la mise à l'essai de ces plans
- les arrangements pris en matière de gestion des risques associés aux tiers, pour que le FSP comprenne la manière dont le mandataire gère les risques liés à ses propres sous-traitants
- les arrangements pris en matière de planification des capacités et de gestion du changement, pour que le FSP comprenne comment il sera informé des changements que le mandataire prévoit apporter à ses services
- les normes du secteur auxquelles il adhère et les processus qu'il applique pour en vérifier le respect
- les arrangements pris pour aviser le FSP des modifications apportées à ses systèmes, politiques, procédures, processus ou contrôles
- la facilité à surveiller son rendement
- sa capacité à se conformer à ses propres systèmes, politiques, procédures, processus ou contrôles
- sa capacité à se conformer aux ententes contractuelles négociées avec le FSP

13.11 Les critères à établir dépendent de la relation entre le FSP et le mandataire. Le FSP peut varier son approche pour élaborer ces critères selon la nature de la relation.

13.12 Conformément à l'alinéa 5(4)b) du *Règlement*, le cadre du FSP doit « interdire au fournisseur de services de paiement de faire appel à un mandataire pour l'exécution d'activités associées aux paiements de détail si le mandataire ne satisfait pas les critères ».

13.12.1 Par conséquent, le FSP doit évaluer le mandataire avant de conclure une entente avec lui. Si les résultats de l'évaluation indiquent que le mandataire ne répond pas ou ne sera pas en mesure de répondre aux critères, le FSP s'abstenir ou se retirer de toute entente avec lui.

13.13 Étant donné que le FSP est responsable des actions de ses mandataires, il doit être en mesure de comprendre et de vérifier leurs pratiques de gestion des risques. En menant par précaution une évaluation détaillée (diligence raisonnable) donne au FSP une meilleure idée :

- du respect continu de ses critères par le mandataire
- des arrangements pris par le mandataire en matière de gestion des risques
- du rendement du mandataire
- des risques auxquels il s'expose en recourant au mandataire, et des conséquences sur sa situation de conformité avec la LAAPD

13.14 L'annexe J présente des exemples d'outils et de ressources que le FSP pourrait utiliser pour recueillir de l'information dans le cadre de son évaluation des mandataires par rapport aux critères établis.

Fréquence et documents

13.15 Selon l'alinéa 5(4)c) du *Règlement*, le cadre du FSP doit également « traiter de la manière dont le fournisseur de services de paiement effectue, au moins une fois par année, une évaluation de la conformité aux critères et des pratiques des mandataires en matière de gestion du risque opérationnel ».

13.15.1 Ainsi, en plus d'évaluer un mandataire avant de conclure une entente avec lui, le FSP doit aussi évaluer ses mandataires au moins une fois par année.

13.16 Le cadre du FSP doit exiger que le FSP tienne un document où sont consignés la date et le résultat de chaque évaluation mentionnée ci-dessus (alinéa 5(4)d) du *Règlement*).

Passation de contrats et répartition des responsabilités

13.17 Lorsqu'un FSP conclut une entente avec un mandataire, la Banque s'attend à ce qu'il encadre cette entente par des modalités contractuelles adaptées à la nature de l'entente. En effet, le FSP doit établir des ententes contractuelles avec ses mandataires pour s'assurer de pouvoir atteindre assidûment ses objectifs d'intégrité, de confidentialité et de disponibilité et rester conforme aux exigences réglementaires.

13.18 Selon l'alinéa 5(4)e) du *Règlement*, le cadre du FSP doit « répartir clairement les responsabilités entre le fournisseur de services de paiement et le mandataire, notamment à l'égard de la propriété, de l'intégrité, de la confidentialité et de la disponibilité des données et renseignements ».

13.18.1 Le FSP doit s'assurer que la répartition des responsabilités entre le mandataire et lui est clairement documentée. La Banque s'attend à ce que cette répartition soit expliquée dans le contrat qui lie le FSP au mandataire.

13.19 Le FSP doit également réaliser périodiquement un examen formel des ententes (p. ex., révision de contrat) afin de s'assurer que les contrats restent adéquats.

Contrôles compensatoires

13.20 Le FSP doit mettre en place des contrôles compensatoires pour gérer les risques de faire appel à des mandataires. Il doit déterminer ces contrôles en fonction du niveau de risque associé à un mandataire.

13.21 L'élaboration de plans de résiliation constitue un contrôle compensatoire essentiel pour gérer le risque d'une relation avec un mandataire. Le FSP peut devoir mettre fin à sa relation avec un mandataire pour diverses raisons. Quelle que soit la raison, la Banque encourage le FSP à élaborer un plan de résiliation pour s'assurer qu'il sera toujours en mesure d'atteindre ses objectifs d'intégrité, de confidentialité et de disponibilité.

13.22 Le plan de résiliation pourrait prévoir ce qui suit :

- les capacités, les ressources et les délais nécessaires à l'exécution de ces services ou activités, ou au transfert de ces services ou activités à un autre mandataire
- les risques liés à sa mise en œuvre
- la capacité du FSP à atteindre ses objectifs de confidentialité, de disponibilité et d'intégrité
- la capacité du FSP à rester conforme aux exigences réglementaires

Surveillance

13.23 La Banque encourage le FSP à surveiller les mandataires pour pouvoir prendre connaissance et tenir compte des changements concernant le niveau et le type de risques associés à la relation. Le FSP doit surveiller leur rendement général ainsi que leur respect des modalités contractuelles, des cibles de rendement et des ententes de prestation de services.

13.24 Le FSP doit effectuer sa surveillance selon une approche fondée sur les risques et documenter cette approche pour justifier la rigueur des activités de surveillance entourant certains mandataires.

Annexe A : Glossaire

anomalie

Événement ou activité qui s'écarte des opérations standard ou normales.

approche fondée sur les risques

Adéquation entre la rigueur de la supervision et la nature et l'ampleur des risques que présentent le fournisseur de services de paiement et sa situation particulière.

cadre dirigeant

Aux termes de l'article 1 du *Règlement sur les activités associées aux paiements de détail*, « s'agissant d'une entité, l'une ou l'autre des personnes suivantes :

« a) un membre de son conseil d'administration qui est aussi son employé à temps plein;

« b) le premier dirigeant, directeur de l'exploitation, président, directeur de la gestion du risque, secrétaire, trésorier, contrôleur de gestion, directeur financier, comptable en chef, auditeur en chef ou actuaire en chef, ou la personne qui exerce des fonctions semblables à celles qu'exerce normalement le titulaire de l'un de ces postes;

« c) tout autre dirigeant relevant directement du conseil d'administration, du premier dirigeant ou du directeur de l'exploitation ».

cause première

Facteur(s) sous-jacent(s) d'un incident porteur de risque opérationnel.

cible de fiabilité

Mesures quantifiables du niveau de rendement servant à évaluer la conformité avec les objectifs de disponibilité d'un fournisseur de services de paiement.

confidentialité

Propriété selon laquelle une donnée ou une information n'est pas diffusée ni divulguée à des personnes physiques, entités, processus ou systèmes non autorisés; préservation des restrictions autorisées entourant l'accessibilité et la divulgation des données et des renseignements.

disponibilité[2]

Propriété d'un service accessible et utilisable à la demande par une entité autorisée; possibilité d'accès et de recours fiable et opportun à un service de paiement, à un système, à des données ou à des renseignements.

éléments de protection

Éléments du cadre, y compris les systèmes, politiques, procédures, processus, contrôles et autres moyens, qui sont mis en œuvre pour atténuer les risques opérationnels et protéger les actifs et les processus opérationnels.

fournisseur de services de paiement

Aux termes de l'article 2 de la *Loi sur les activités associées aux paiements de détail*, « personne physique ou entité qui exécute une fonction de paiement dans le cadre d'un service ou d'une activité commerciale qui n'est pas accessoire à un autre service ou à une autre activité commerciale ».

incident

Aux termes de l'article 2 de la *Loi sur les activités associées aux paiements de détail*, « événement ou série d'événements liés qui sont non planifiés par le fournisseur de services de paiement et qui entravent, perturbent ou interrompent – ou qui pourraient vraisemblablement entraver, perturber ou interrompre – une activité associée aux paiements de détail exécutée par le fournisseur de services de paiement ».

Pour en savoir plus, voir la ligne directrice *La déclaration des incidents*.

indicateurs

Mesures (quantitatives ou qualitatives) permettant de contrôler l'exposition au risque et d'évaluer la conformité avec les objectifs d'intégrité, de confidentialité et de disponibilité du fournisseur de services de paiement.

intégrité

Exactitude et complétude; absence de modification ou de destruction indue d'un système, de données ou de renseignements.

LAAPD

Loi sur les activités associées aux paiements de détail

mandataire

Personne physique ou entité qui a l'autorité d'exercer des activités associées aux paiements de détail en représentant un fournisseur de services de paiement. Cette relation est mise en place par le mandant du

---

2 Les définitions des termes « disponibilité », « intégrité » et « confidentialité » s'alignent sur les sources de référence suivantes :

- ISO 27000:2018, *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire*.
- National Institute of Standards and Technology (2020). *Security and Privacy Controls for Information Systems and Organizations*, publication spéciale 800-53, révision 5, septembre.

fournisseur de services de paiement. Dans la *Loi sur les activités associées aux paiements de détail*, les termes anglais « agent » et « mandatary » sont traduits indifféremment par « mandataire » en français.

proportionnalité

Adéquation entre la rigueur de la gestion des risques et les répercussions que pourraient avoir une entrave, une perturbation ou une interruption des activités associées aux paiements de détail du fournisseur de services de paiement sur les utilisateurs finaux et les autres fournisseurs de services de paiement, compte tenu notamment de son ubiquité et interconnexion.

réponse

Mesures prises pour limiter les répercussions d'un incident; comprend le rétablissement, c'est-à-dire les mesures prises pour reprendre les activités.

résultats

Principales attentes à l'égard d'un fournisseur de services de paiement en ce qui a trait aux exigences énoncées dans la *Loi sur les activités associées aux paiements de détail* et son règlement d'application.

risque opérationnel

Aux termes de l'article 2 de la *Loi sur les activités associées aux paiements de détail*, « l'un ou l'autre des risques ci-après qui entrave, perturbe ou interrompt une activité associée aux paiements de détail exécutée par un fournisseur de services de paiement :

« a) une défaillance des systèmes d'information ou du processus interne de ce fournisseur;

« b) une erreur humaine;

« c) une gestion défaillante ou inadéquate;

« d) une perturbation causée par un événement externe ».

tiers

Parties avec lesquelles le fournisseur de services de paiement a conclu un contrat, ou celles avec lesquelles il n'en a pas conclu, selon ses arrangements et sa structure organisationnelle. Exemples :

- tiers fournisseurs de services
- mandataires
- entités affiliées
- autres fournisseurs de services de paiement
- infrastructures de marchés financiers (aussi appelées *systèmes de compensation et de règlement*)

tiers fournisseur de services

Aux termes de l'article 2 de la *Loi sur les activités associées aux paiements de détail*, « personne physique ou entité qui fournit à un fournisseur de services de paiement un service lié à une fonction de paiement au titre d'un contrat et qui n'est pas l'un de ses employés ni l'un de ses mandataires ».

ubiquité et interconnexion

Indicateurs des répercussions qu'une entrave, une perturbation ou une interruption des activités associées aux paiements de détail du fournisseur de services de paiement pourrait avoir sur les utilisateurs finaux et sur les autres fournisseurs de services de paiement. Les informations utilisées par la Banque pour établir l'ubiquité et l'interconnexion sont les suivantes :

- nombre d'utilisateurs finaux auxquels le fournisseur de services de paiement fournit des services correspondant à des activités associées aux paiements de détail
- valeur des fonds détenus pour des utilisateurs finaux par le fournisseur de services de paiement
- valeur des transferts électroniques de fonds effectués par le fournisseur de services de paiement dans le cadre d'une activité associée aux paiements de détail
- nombre de transferts électroniques de fonds effectués par le fournisseur de services de paiement dans le cadre d'une activité associée aux paiements de détail
- nombre de fournisseurs de services de paiement auxquels le fournisseur de services de paiement fournit des services correspondant à des activités associées aux paiements de détail

Annexe B : Documentation du cadre

1. La liste ci-dessous présente les types de documents que le FSP doit envisager de créer et de tenir avec son cadre. Elle n'est pas exhaustive.
    - Une description de l'approche de gestion des risques opérationnels et de réponse aux incidents, y compris des références aux politiques et procédures pertinentes.
    - Les objectifs, cibles de fiabilité et indicateurs, ainsi qu'une explication de la façon dont ils ont été établis, ce qui comprend :
        - une définition claire de la relation entre les objectifs, les cibles de fiabilité et les indicateurs du FSP
        - une description de la manière dont le FSP a pris en compte le principe de proportionnalité
        - les sources de données, la fréquence du suivi et l'analyse effectuée
    - Les rôles et responsabilités en matière de gestion des risques opérationnels et de réponse aux incidents, avec les descriptions de poste, les liens hiérarchiques et les accords d'approbation, les structures organisationnelles et toute autre documentation précisant comment les rôles et responsabilités du FSP assurent une fonction de surveillance et d'examen critique.
    - Les procédures d'évaluation de l'adéquation des ressources humaines et financières (compétences et formation des ressources humaines comprises), une description indiquant si le FSP a un accès fiable et opportun à ces ressources, et les résultats de ces évaluations; les pièces justificatives comprennent les documents relatifs aux compétences du personnel et à la formation donnée (contenu, exécution, présence, etc.).
    - Les politiques et procédures de recensement des risques opérationnels ainsi que la description des risques recensés et de leurs causes.
    - Les politiques et procédures de recensement et de catégorisation des actifs et des processus opérationnels, ainsi que la description des actifs et des processus opérationnels du FSP, de leur importance et de leur sensibilité.
    - La documentation des systèmes, politiques, procédures, processus, contrôles et autres moyens utilisés pour atténuer les risques opérationnels et protéger les actifs et les processus opérationnels, détecter les incidents, les anomalies et les défaillances dans la mise en œuvre du cadre, et réagir aux incidents.
    - La documentation, y compris les guides de préparation, de mise en œuvre, d'exploitation, de configuration et d'utilisation, relative aux systèmes entourant l'exécution des activités associées aux paiements de détail ou la gestion des risques opérationnels.
    - Les plans de réponse aux incidents, de rétablissement et d'enquête en cas d'incident.
    - Les politiques et procédures pour l'établissement de rapports, l'examen, l'approbation, la réalisation d'essais et d'examens indépendants et le maintien du cadre.
    - Les descriptions et autres documents justificatifs des examens, des essais et des examens indépendants, dont les plans de mise à l'essai et d'examen, les dates de réalisation, les membres du personnel et autres parties concernés, la portée, les résultats, les mesures de suivi et les plans de mise en œuvre de ces mesures, et les raisons pour lesquelles certaines mesures sont recommandées ou non.
    - La justification des approches adoptées.

Annexe C : Objectifs, cibles de fiabilité et indicateurs

Objectifs, cibles et indicateurs

1. Le FSP fixe des objectifs pour officialiser les limites d'intégrité, de confidentialité et de disponibilité dans lesquelles ses activités associées aux paiements de détail doivent se dérouler.
2. Les cibles de fiabilité et les indicateurs représentent des mesures clés de rendement, de risque ou de contrôle qui décrivent comment sont mesurés les objectifs du FSP. Les FSP utilisent ces cibles et indicateurs pour détailler la manière dont ils mesurent un objectif en particulier.
    - Par exemple, le FSP pourrait mesurer l'atteinte d'un objectif de disponibilité en surveillant l'efficacité de plusieurs systèmes et processus opérationnels qui soutiennent des activités associées aux paiements de détail, chacun ayant ses propres cibles de disponibilité et ses propres indicateurs de risque et de contrôle. Il pourrait ensuite agréger les données des cibles et des indicateurs pour déterminer s'il atteint son objectif de disponibilité.
    - Dans cet exemple, les cibles de fiabilité pourraient être le nombre d'heures d'interruption d'une fonction de paiement, ou encore le nombre ou pourcentage de clients touchés. Les indicateurs pourraient être les incidents ayant des répercussions sur le processus ou système opérationnel concerné, ou encore le nombre ou le pourcentage d'actifs en fin de vie utilisés (voir d'autres exemples ci-dessous).
3. Le FSP doit veiller à ce que ses objectifs, cibles de fiabilité et indicateurs soient fixés de manière cohérente. Il est tenu de fixer des objectifs pour préserver l'intégrité, la confidentialité et la disponibilité de ses activités associées aux paiements de détail ainsi que des systèmes, données et renseignements liés à l'exercice de ces activités. Selon les activités du FSP, l'atteinte de ces objectifs peut dépendre de plusieurs actifs et processus opérationnels. Le FSP pourrait aussi devoir fixer des objectifs d'intégrité, de confidentialité ou de disponibilité pour ces actifs et processus. Il doit veiller à ce que les cibles de fiabilité et les indicateurs fixés pour chaque actif et processus opérationnel favorisent l'atteinte de ses objectifs globaux.

Cibles de fiabilité et indicateurs

4. Le FSP doit tenir compte de plusieurs facteurs lorsqu'il fixe des cibles de fiabilité et des indicateurs. Ces cibles ou indicateurs doivent :
    - avoir un lien étroit avec le risque (y compris avec son facteur déterminant ou sa cause) ou l'objectif, ou tout autre lien pertinent
    - permettre de détecter rapidement les objectifs menacés (le FSP doit envisager de définir des indicateurs avancés et des indicateurs tardifs
    - reposer sur des données qui sont disponibles ou accessibles de manière cohérente et fréquente, et dont la fiabilité ne fait pas de doute pour le FSP
    - avoir une précision adaptée au niveau de détail nécessaire pour faire le suivi de l'objectif visé, c'est-à-dire qu'ils peuvent être fixés au niveau d'un système ou d'un actif, d'un produit ou d'un service et d'une unité ou d'un secteur organisationnel, ou à tout autre niveau pertinent
    - tenir compte des interdépendances entre les systèmes ou les actifs, les produits ou les services et les unités ou les secteurs organisationnels, ou de toute autre interdépendance pertinente
    - être alignés sur d'autres éléments du cadre du FSP (p. ex., les cibles de fiabilité doivent être cohérentes avec ses plans de réponse aux incidents)

5. Comme l'indique l'article 4.7 sous « Objectifs », la Banque recommande qu'un FSP ayant une ubiquité ou une interconnexion relativement grande établisse au minimum certaines cibles de fiabilité (liées à la disponibilité). Le FSP doit envisager ce qui suit lorsqu'il établit ses diverses cibles :
    - des cibles de disponibilité du système indiquant le pourcentage de temps pendant lequel un système, un processus, un service ou une fonction doit être pleinement fonctionnel et disponible
    - un objectif de rétablissement indiquant le délai maximal, défini par le FSP, au bout duquel une fonction, un système, un service ou un processus doit redevenir actif après sa perturbation
    - une durée maximale d'interruption tolérable indiquant l'intervalle maximal, défini par le FSP, pendant lequel une fonction, un système, un service ou un processus particulier peut être indisponible
        - Cette durée englobe l'objectif de rétablissement et le délai de reprise du système, du service, du processus ou de la fonction. Le « délai de reprise » est le temps dont le FSP aurait besoin pour vérifier l'intégrité du système et de toutes les données pertinentes et pour les mettre à jour (p. ex., en saisissant les données qui ont été recueillies manuellement pendant l'interruption).
        - Ainsi, la durée maximale d'interruption tolérable est la somme du temps de rétablissement visé et du délai de reprise.
    - des objectifs de point de reprise indiquant l'ampleur maximale d'une perte de données, mesurée en temps, que le FSP est prêt à accepter pour un système ou un ensemble de données particulier
6. Les indicateurs relatifs à la disponibilité pourraient également inclure des paramètres non temporels, comme le nombre de transactions ou de clients touchés.
7. Les indicateurs permettant d'évaluer si le FSP atteint ses objectifs d'intégrité et de confidentialité pourraient inclure les éléments suivants, entre autres :
    - le nombre d'atteintes à la protection des données signalées au cours d'une période donnée
    - les indicateurs liés au respect des politiques de protection des données du FSP (p. ex., le pourcentage de données critiques stockées protégées conformément à la norme du FSP, le pourcentage de serveurs critiques protégés par un logiciel de sécurité, le pourcentage de tiers visés par une évaluation complète des risques de fournisseur)
    - le suivi des mesures effectivement prises pour résoudre les problèmes (p. ex., le nombre de vulnérabilités en suspens pour les applications ou les postes de travail critiques et le nombre de mesures en suspens ou de vulnérabilités décelées dans le cadre d'une réponse à un incident, d'une mise à l'essai ou d'un examen indépendant)

Évaluation de l'atteinte des objectifs

8. Dans la plupart des cas, lorsque la surveillance indique que le FSP n'a pas atteint ses objectifs, ses cibles de fiabilité ou ses indicateurs, celui-ci est tenu d'améliorer son cadre afin de pouvoir atteindre ses objectifs à l'avenir. Toutefois, il peut y avoir des exceptions à cette règle, notamment lorsque le FSP n'a pas pu atteindre ses objectifs en raison de circonstances qui échappent à son pouvoir (p. ex., événements ponctuels et imprévisibles). Dans ce cas, la Banque s'attend à ce que le FSP évalue la probabilité que l'événement se reproduise et, selon cette évaluation, revoie son cadre afin de déterminer s'il faut y apporter des améliorations.
9. La Banque encourage le FSP à examiner régulièrement si ses objectifs, cibles et indicateurs demeurent appropriés. Il doit considérer toute évolution entourant ses activités, notamment en ce qui concerne son ubiquité et son interconnexion.

Annexe D : Éléments de protection concernant les technologies de l'information et la cybersécurité

La liste qui suit détaille les concepts et les résultats recommandés en matière de technologies de l'information et de cybersécurité que le FSP doit envisager d'adopter dans le cadre de ses éléments de protection généraux.

1. **Contrôle des accès :** le FSP doit établir, mettre en œuvre et maintenir des éléments de protection pour atténuer les risques concernant l'accès non autorisé aux actifs critiques ou sensibles. Le FSP doit suivre, enregistrer et examiner l'historique des activités d'accès aux actifs critiques et sensibles par les parties internes comme externes.
    - Les contrôles d'accès doivent comprendre à la fois des contrôles physiques et virtuels, en fonction de la source du risque que le FSP cherche à atténuer.
    - Pour que le FSP puisse gérer les identités et les comptes des utilisateurs internes et externes, il doit envisager de mettre en place une procédure pour accorder, retirer ou modifier les droits d'accès en temps opportun, suivant des processus d'autorisation prédéfinis. Ces processus d'autorisation doivent nécessiter l'intervention du responsable fonctionnel des renseignements auxquels on accède (le responsable de l'actif informationnel au sein du FSP), à même le processus de gestion des accès. La Banque encourage également le FSP à définir de façon individuelle l'accès à certains actifs, ce qui peut passer par des matrices d'accès qui définissent clairement les rôles entourant les activités associées aux paiements et le niveau (privilège) d'accès requis pour chaque rôle. En établissant des matrices d'accès, le FSP doit s'assurer que :
        - l'accès autorisé dépend de la personne ou du système devant accéder aux actifs, selon son rôle dans les activités associées aux paiements du FSP
        - les processus ou tâches de paiement sensibles ou critiques ne sont pas exécutés par une seule personne – ils sont validés par une autre personne (séparation des tâches) avant d'être exécutés, et la personne chargée de la validation connaît bien le processus ou la tâche et les risques qui y sont associés
        - seuls les droits d'accès minimaux (privilèges minimaux) requis pour accomplir et valider une tâche sont accordés aux personnes ou aux systèmes participant à des activités associées aux paiements – le FSP doit donc tenir compte du rôle de la personne ou du système et s'assurer que son accès et ses droits se limitent au minimum requis pour ce rôle (p. ex., les droits d'administrateur doivent être restreints, et l'accès aux systèmes doit être refusé s'il déborde du rôle en question)
    - La procédure d'octroi, de retrait ou de modification des droits d'accès doit tenir compte des fins d'emploi et des autres changements de ressources humaines ou de responsabilités. En cas de fin d'emploi, les droits d'accès doivent être rapidement retirés. Le FSP peut envisager d'établir, de mettre en œuvre et de maintenir un programme de gestion des comptes et des identifiants (création des authentifiants d'utilisateur) qui prévoit des étapes d'autorisation, d'attribution et de désactivation des identifiants. Ce processus doit respecter les critères ci-dessous :
        - Les droits d'accès et les privilèges système sont accordés en fonction des rôles et des responsabilités des ressources humaines, moyennant l'approbation des parties concernées au sein du FSP.

- Les utilisateurs privilégiés sont soumis à des contrôles d'accès supplémentaires (p. ex., ils doivent avoir des moyens d'authentification plus forts pour accéder aux actifs sensibles ou critiques). Il faut notamment renforcer la complexité des mots de passe et séparer les comptes d'utilisateurs privilégiés des comptes d'utilisateurs ordinaires. Lorsque c'est possible, la Banque encourage le FSP à utiliser des solutions automatisées qui contribuent à atténuer les risques associés aux privilèges d'accès. Il ne doit pas utiliser de comptes d'accès génériques ou partagés et doit s'assurer de pouvoir identifier les utilisateurs internes et externes.
- Les accès et autorisations attribués aux utilisateurs font régulièrement l'objet d'un examen confirmant qu'ils sont nécessaires et à jour (conformément aux indications du paragraphe plus haut concernant les droits d'accès minimaux).
- Les utilisateurs ayant accès aux actifs critiques utilisent l'authentification multifacteur, pour protéger les systèmes et les données contre tout accès non autorisé.
- Les utilisateurs ayant accès aux fonctions essentielles des systèmes utilisent l'authentification multifacteur, notamment les gestionnaires de comptes financiers, les administrateurs de systèmes ou du nuage, les utilisateurs privilégiés et la haute direction.
- Il y a une politique exigeant l'utilisation de mots de passe forts pour l'accès aux systèmes informatiques par des utilisateurs internes et externes.
- L'authentification multifacteur est une option proposée.
- La politique relative aux mots de passe comprend des indications sur la longueur des mots de passe et les façons sécuritaires de les stocker et de les transmettre.

- L'environnement de contrôle des accès doit permettre le suivi, l'enregistrement et l'examen des accès et des activités en ce qui concerne les actifs recensés, afin que le FSP puisse vérifier l'efficacité des contrôles d'accès qu'il a mis en œuvre. Cela doit viser les accès tant virtuels que physiques (p. ex., maintenance et réparations) aux actifs, y compris les données, les renseignements et les systèmes.

2. **Gestion des vulnérabilités, mesures correctives et application de correctifs :** les logiciels et les micrologiciels que le FSP utilise pour fournir ou faciliter les activités associées aux paiements de détail sont exposés à un risque de vulnérabilités en matière de sécurité. Pour se protéger contre ces menaces, le FSP doit envisager plusieurs processus et pratiques :
   - Établir, mettre en œuvre et maintenir des mesures correctives et l'application de correctifs pour tous les logiciels et micrologiciels. Le FSP devrait entre autres adopter une approche systémique pour découvrir et évaluer les vulnérabilités et les correctifs connus, afin de déterminer le risque auquel il est exposé et les priorités relatives à respecter pour le déploiement des correctifs. Il s'agit d'un processus continu qui nécessite de déceler et de corriger les vulnérabilités tout au long du cycle de vie du logiciel. Lorsque le logiciel vient d'un tiers, le FSP est encouragé à prendre ses précautions en vérifiant le cycle de développement logiciel du fournisseur, notamment en s'assurant qu'il dispose d'un solide programme de gestion des vulnérabilités.
   - Établir, mettre en œuvre et maintenir des calendriers de correction des vulnérabilités qui sont proportionnels à la sensibilité et à l'importance de l'actif et à la gravité de la vulnérabilité. En général, cela signifie que les actifs les plus sensibles ou importants pour les activités associées aux paiements doivent être corrigés en priorité. Le PSP doit aussi prioriser les vulnérabilités qui présentent les risques les plus élevés.

    - En outre, le FSP doit déterminer activement les logiciels et le matériel qui ne peuvent plus être mis à jour (en fin de vie utile) et les vulnérabilités connues de ces actifs qui ne sont peut-être pas corrigées. Le FSP doit envisager les prochaines étapes pour tout actif en fin de vie utile, comme son remplacement ou l'application de contrôles compensatoires pour atténuer les risques.
  - Établir, mettre en œuvre et maintenir des solutions de gestion des vulnérabilités et des correctifs. Ces solutions techniques facilitent l'analyse, la mise à l'essai et l'installation de correctifs pour protéger l'environnement opérationnel.
3. **Logiciels de sécurité :** le FSP est confronté à diverses menaces de programmes malveillants, notamment des virus, des vers, des chevaux de Troie, des rançongiciels et des logiciels espions. Pour s'en protéger, il doit faire ce qui suit :
   - Envisager d'établir, de mettre en œuvre et de maintenir des éléments pour protéger les actifs servant à ses activités associées aux paiements. Par exemple, il peut s'agir de systèmes de détection et de réponse aux points terminaux, d'antivirus, d'anti-programmes malveillants ou de pare-feux logiciels.
   - Veiller à ce que les antivirus, les anti-programmes malveillants, les systèmes de prévention ou de détection des intrusions, les pare-feux réseau, les systèmes de détection aux points terminaux ou tout autre logiciel de sécurité soient automatiquement mis à jour avec les signatures, les ensembles de règles, les renseignements et les bases de données sur les menaces (ou autres sources similaires) les plus récents, s'il y a lieu.
   - Configurer les logiciels de sécurité pour qu'ils effectuent régulièrement des analyses automatisées, s'il y a lieu.
4. **Configuration sécurisée des appareils :** les systèmes de technologie de l'information qui soutiennent les activités associées aux paiements du FSP pourraient être configurés d'une manière qui les rend vulnérables aux cyberattaques. Pour atténuer ce risque, le FSP doit envisager ce qui suit :
   - Suivre les directives de configuration de base du fabricant d'origine. En l'absence de ces directives, la Banque encourage le FSP à suivre les recommandations de base émises par des sources fiables et indépendantes.
   - Établir, mettre en œuvre et maintenir des configurations sécurisées pour tous ses appareils (p. ex., renforcer le système, notamment en modifiant tous les mots de passe par défaut, en évitant l'utilisation de comptes génériques, en limitant les fonctions inutiles et en autorisant toutes les fonctions de sécurité proportionnellement au niveau de risque que l'actif représente pour le FSP et ses activités associées aux paiements).
   - Revoir régulièrement ces configurations sécurisées pour s'assurer qu'elles sont constamment conformes.
5. **Sécurité du réseau :** le FSP doit protéger son réseau contre les menaces internes et externes. La Banque lui recommande d'envisager les stratégies suivantes, s'il y a lieu :
   - Établir, mettre en œuvre et maintenir des pare-feux protégeant spécifiquement les frontières entre son réseau d'entreprise et Internet.
   - Isoler les serveurs connectés à Internet du reste du réseau de l'entreprise.
   - Établir, mettre en œuvre et maintenir des solutions de sécurité réseau qui empêchent les utilisateurs et les systèmes du réseau de se connecter à des emplacements malveillants connus sur Internet (p. ex., pare-feu de contenu, pare-feu de système de noms de domaine ou autre technologie de filtrage des passerelles).

- Exiger une connectivité sécurisée (p. ex., authentification des ressources partagées et chiffrement en transit) pour toutes les ressources informatiques de l'entreprise, et exiger la connectivité à un réseau privé virtuel avec authentification multifacteur pour tous les accès à distance aux réseaux de l'entreprise. Le FSP ne devrait autoriser l'accès administratif aux actifs critiques et sensibles qu'à partir de ses adresses IP internes.
- Configurer la sécurité Wi-Fi de façon stricte (p. ex., les paramètres de chiffrement Wi-Fi, l'authentification, et la modification des paramètres par défaut et des mots de passe).
- Segmenter et séparer les réseaux (p. ex., séparation des réseaux Wi-Fi publics et des réseaux d'entreprise, et segmentation claire en fonction des différentes exigences de sécurité).
- Protéger les systèmes des points de vente et les autres systèmes critiques ou sensibles en les isolant d'Internet et des autres zones du réseau de l'entreprise. Le FSP doit envisager de suivre les normes pertinentes du secteur des paiements, notamment lorsqu'il stocke, traite ou transmet des cartes de paiement.
- Établir, mettre en œuvre et maintenir des protocoles de sécurité et d'authentification pour tous ses services de courriel.
- Établir, mettre en œuvre et maintenir un filtrage des courriels aux points d'entrée et de sortie.

6. **Services des technologies de l'information sécurisés en nuage et externalisés :** le FSP qui fait appel à des tiers fournisseurs de services est exposé à des risques opérationnels supplémentaires qui doivent être atténués. Pour protéger les données et les renseignements qu'il échange avec des tiers fournisseurs de services, ou qui sont utilisés ou stockés chez ces derniers, il doit envisager les stratégies suivantes :
   - Établir, mettre en œuvre et maintenir une approche pour :
     - évaluer son niveau d'acceptation quant à la manière dont ses tiers fournisseurs de services traitent les renseignements de nature délicate et y accèdent
     - évaluer son niveau d'acceptation quant aux territoires de compétence juridique dans lesquels ses tiers fournisseurs de services stockent ou utilisent les renseignements de nature délicate
   - Veiller à ce que son infrastructure informatique et ses utilisateurs communiquent en toute sécurité avec tous les services et applications infonuagiques.
   - Veiller à ce que les comptes administratifs des services infonuagiques utilisent une authentification multifacteur et diffèrent des comptes d'administrateur internes.
   - Protéger les données par chiffrement en transit et au repos.
7. **Supports sécurisés pour les systèmes d'information :** le FSP qui utilise des supports de systèmes d'information (que ce soit numériques, comme les clés USB, les disques compacts et les disques durs externes, ou non numériques, comme le papier et les microfilms) est confronté à de plus grandes menaces contre l'intégrité et la confidentialité des données, systèmes et renseignements servant à faciliter les activités associées aux paiements de détail. Pour contrer ces menaces, il doit envisager les stratégies suivantes :
   - Protéger et stocker en toute sécurité les supports numériques des systèmes d'information.
   - Maintenir la responsabilité des supports pendant leur utilisation ou leur transport en dehors des zones contrôlées.
   - Nettoyer les supports avant qu'ils soient éliminés, que le FSP s'en départisse ou qu'ils soient rendus disponibles pour une réutilisation.
   - S'assurer que les disques des supports amovibles ou portables sont entièrement chiffrés.
   - Utiliser des solutions de gestion des appareils mobiles, comme le chiffrement des disques et les fonctionnalités de suppression à distance.

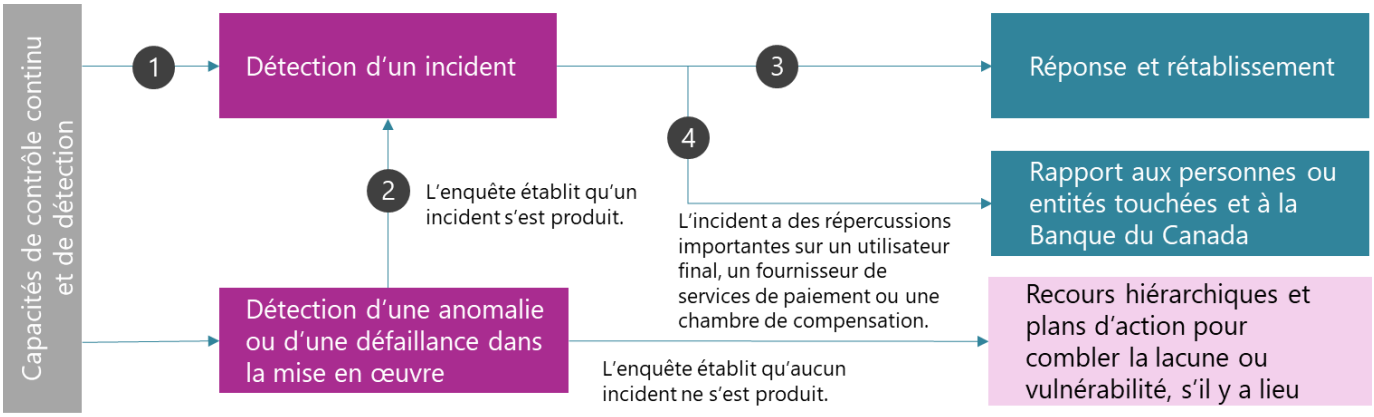
8. **Cycle de développement sécurisé des systèmes :** le FSP doit intégrer des considérations de sécurité à tous les stades du cycle de vie des systèmes et des logiciels, qu'ils soient personnalisés ou génériques. Pour être correctement établie, mise en œuvre et maintenue, l'approche du cycle de développement des systèmes doit comprendre au minimum ce qui suit :
    - Intégrer des considérations de sécurité dans l'acquisition, le développement et la gestion des systèmes du FSP.
    - Élaborer des architectures de sécurité pour les systèmes, y compris des exigences et des approches pour protéger leur intégrité, leur confidentialité et leur disponibilité.
    - Décrire toute dépendance à l'égard d'autres systèmes et services, tant internes qu'externes.
    - Décrire les rôles et les responsabilités en matière de sécurité.
    - Protéger les environnements de préproduction (développement et mise à l'essai), le cas échéant, en fonction des risques présentés par le système ou le composant du système.
    - Décrire les exigences de sécurité, les contrôles, la documentation et l'attribution des responsabilités pour l'acquisition de systèmes ou de services.
9. **Autres contrôles en fonction de la nature des activités du FSP :** Le FSP doit adopter tout autre système, politique, procédure, processus ou contrôle nécessaire pour atténuer les risques liés à la sécurité de l'information et à la cybersécurité ainsi qu'en protéger ses actifs et processus opérationnels.

Annexe E : Relation entre le contrôle continu, la détection des incidents et les plans de réponse et de rétablissement

Détection

1. La figure E-1 illustre la relation entre le contrôle continu, la détection des incidents et les mesures de réponse et de rétablissement.
   - En général, un incident peut être décelé à l'aide de capacités de contrôle continu ou de détection (figure E-1, numéro 1).
   - Les capacités de contrôle continu ou de détection peuvent permettre de déceler une anomalie ou une défaillance dans la mise en œuvre du cadre; il est ensuite possible qu'après enquête, on détermine qu'un incident s'est produit (figure E-1, numéro 2).
2. Lorsqu'il y a incident, le FSP doit mettre en œuvre des plans de réponse et de rétablissement, comme illustré au numéro 3 ci-dessous. Il doit déclarer sans délai les incidents qui ont des répercussions importantes sur un utilisateur final, un FSP ou une chambre de compensation. Cette déclaration doit avoir lieu auprès des personnes physiques ou entités ayant subi des répercussions importantes et auprès de la Banque du Canada, au plus tard 24 heures après la détection de l'incident (figure E-1, numéro 4).

Figure E-1 : Relation entre le contrôle continu, la détection des incidents et les plans de réponse et de rétablissement



Annexe F : Contrôles concernant les technologies de l'information et la cybersécurité

La liste qui suit précise les capacités de contrôle continu et de détection recommandées en matière de sécurité de l'information et de cybersécurité.

1. **Défenses du réseau :** Détectent les activités malveillantes (comme les cyberattaques) provenant de l'extérieur du réseau d'entreprise du FSP en analysant les données entrantes et sortantes. Il peut s'agir de pare-feux de périmètre, de passerelles sécurisées, de zones démilitarisées, etc.
2. **Détection des programmes malveillants :** Peut être assurée par un logiciel installé sur les points terminaux pour détecter les programmes malveillants, notamment les chevaux de Troie, les logiciels espions, les enregistreurs de frappe et les virus. Le terme « point terminal » désigne un appareil informatique qui communique avec un réseau auquel il est connecté. Cela comprend les serveurs, les téléphones intelligents, les ordinateurs portables, les tablettes et les terminaux points de vente.
3. **Détection et prévention des intrusions :** Capacité à détecter les événements au cours desquels une personne non autorisée obtient ou tente d'obtenir un accès non autorisé à un actif informatique. Il peut s'agir d'exploiter des outils comme la détection des intrusions, la surveillance de l'intégrité des fichiers et le déclenchement d'alertes en cas d'activités malveillantes.
4. **Détection des vulnérabilités :** Activités visant à détecter les faiblesses exploitables dans le code des logiciels, la configuration, les points terminaux actifs, etc. Pour détecter les vulnérabilités, on peut utiliser des outils d'analyse des vulnérabilités, des modèles de menaces, des renseignements sur les menaces, des vérifications de configuration de base, etc.
5. **Surveillance de la sécurité :** Mise en place de mesures pour surveiller de manière proactive les activités non autorisées ou malveillantes liées aux systèmes du FSP afin de détecter ces anomalies et d'y répondre. Il est possible d'utiliser des outils comme une solution de gestion des informations et des événements de sécurité afin d'examiner les journaux provenant de sources telles que la vidéosurveillance, les solutions de surveillance des performances des points terminaux et l'analyse du comportement des utilisateurs. Pour favoriser la rapidité de détection et de réponse, la Banque encourage le FSP à mettre en place des solutions permettant de recueillir et de mettre en corrélation des journaux provenant de diverses sources, dont celles décrites aux points 1 à 4 ci-dessus, en tirant parti des fonctionnalités d'une solution de gestion des informations et des événements de sécurité.
6. **Renseignements sur les menaces :** Obtention de renseignements sur les menaces de cybersécurité susceptibles de toucher les activités du FSP. Ce dernier peut alors exploiter ces renseignements pour mettre en place de manière proactive des contrôles visant à atténuer les risques auxquels il peut être exposé. Les sources de renseignements sur les menaces comprennent, entre autres, la collecte et l'analyse de journaux, les flux de menaces et les communautés et forums en ligne.
7. **Autres contrôles en fonction de la nature des activités du FSP :** Tout autre système, politique, procédure, processus ou contrôle nécessaire pour assurer le contrôle continu et la détection des risques liés à la sécurité de l'information et à la cybersécurité.

Annexe G : Examen interne

1. Les facteurs et les sources d'information dont le FSP doit tenir compte dans son examen peuvent dépendre du contexte de l'examen (examen annuel ou examen effectué à cause d'une modification importante), mais pourraient inclure ce qui suit :
    - tout changement dans les activités associées aux paiements de détail ou dans la manière dont le FSP exerce ses activités existantes associées aux paiements, y compris les changements technologiques ou opérationnels
    - les changements de plus grande envergure apportés aux activités, aux technologies ou aux opérations du FSP qui sont pertinents pour ses activités associées aux paiements de détail et l'atténuation du risque opérationnel lié à ces activités
    - les changements importants relatifs au volume et à la valeur des activités associées aux paiements de détail
    - l'évolution des facteurs de risque ou de l'environnement externe
    - les résultats observés en lien avec l'efficacité du cadre de gestion des risques et de réponse aux incidents, comme :
        - le rendement par rapport aux cibles, aux indicateurs, aux seuils de risque internes et à l'appétit pour le risque, le cas échéant
        - les leçons tirées des incidents (y compris les incidents qui n'atteignent pas les seuils de déclaration), ainsi que toute anomalie ou défaillance décelée dans la mise en œuvre du cadre
    - les leçons tirées des audits, des examens et des essais, ainsi que l'état d'avancement de la mise en œuvre des changements qui en découlent dans son cadre
    - le rendement des mandataires et des tiers fournisseurs de services, y compris les leçons tirées des évaluations de ces parties par le FSP

Annexe H : Mises à l'essai

Objectifs et portée

1. Afin de limiter l'effet des essais sur les données ou renseignements relatifs aux activités et à la production, s'il y a lieu, le FSP doit s'assurer que les environnements d'essai et de production sont distincts. Les environnements d'essai et les données ou renseignements servant aux essais doivent être visés par des contrôles d'accès et d'autres contrôles de sécurité. Voir Protéger.
2. Selon le cas, le FSP peut utiliser les résultats des essais effectués à d'autres fins pour démontrer sa conformité aux exigences de mise à l'essai du *Règlement*, pourvu qu'il atteigne les objectifs et les résultats exigés à l'article 9 du *Règlement*. Le FSP doit pouvoir démontrer à la Banque en quoi il satisfait à ces exigences. Si la portée des mises à l'essai ne remplit pas entièrement les exigences, il doit effectuer des essais supplémentaires.

Types d'essais

3. Les mises à l'essai peuvent passer par différentes approches, notamment :
    - des essais qui visent à évaluer le bon fonctionnement attendu d'un système, d'une politique, d'une procédure, d'un processus ou d'un contrôle, y compris dans des circonstances précises
    - des exercices visant à examiner et à vérifier comment les politiques, les procédures et les processus bien établis ont été respectés ou comment un contrôle a été exécuté récemment
    - une vérification de la sensibilisation ou de la compréhension des employés et des autres ressources humaines, comme des démonstrations du plan de réponse aux incidents (voir plus loin) et des exercices d'hameçonnage
4. Les mises à l'essai peuvent prendre différentes formes, notamment :
    - un examen de la documentation
    - des entrevues
    - des essais basés sur des échantillons
    - un examen des ordinateurs de bureau
    - des exercices de simulation
    - des démonstrations
    - des simulations
5. Dans le cadre d'une approche proportionnelle, les FSP ayant une grande ubiquité ou interconnexion pourraient effectuer des essais supplémentaires visant les risques liés aux technologies de l'information et à la cybersécurité, y compris des tests d'intrusion et des exercices de simulation d'attaques.
    - Test d'intrusion : l'objectif de ce test est d'évaluer la force globale de la défense d'une organisation (les technologies, les processus et le personnel) en simulant les objectifs et les actions d'un attaquant. Les tests d'intrusion doivent être effectués par des parties et des équipes possédant des compétences et une expérience démontrables, y compris une expertise technique en matière de sécurité des réseaux, des systèmes d'exploitation ou des applications.
    - Exercice de simulation d'attaques : leurs objectifs sont plus larges que ceux des tests d'intrusion, car il s'agit d'examiner le niveau de sécurité et de confidentialité des organisations ainsi que leur capacité à mettre en œuvre des cyberdéfenses efficaces. Les exercices consistent à évaluer ce niveau de sécurité

et de confidentialité en simulant les tentatives des adversaires de compromettre la mission et les fonctions commerciales d'une organisation.

6. Les mises à l'essai peuvent être effectuées à l'interne ou par un tiers. Bien que cela soit largement laissé à la discrétion du FSP, la Banque note que les mises à l'essai spécialisées, comme les tests d'intrusion, doivent être effectuées par des parties qualifiées.

Mises à l'essai basées sur des scénarios

7. Les essais ne sont pas tous basés sur des scénarios. Toutefois, ce type d'essais peut fournir des informations détaillées sur les résultats auxquels on peut s'attendre du cadre du FSP dans des circonstances particulières. Il devrait inclure :
   - la mise à l'essai des plans de réponse aux incidents, à partir de scénarios qui servent à vérifier les catégories d'incidents définies par le plan
   - la mise à l'essai des éléments de sécurité de l'information, à partir de scénarios qui servent à vérifier, par exemple, la capacité du FSP à résister à certains types de cyberattaques
8. Les scénarios doivent être basés sur des risques opérationnels pertinents et connus. Ils doivent être suffisamment rigoureux pour mettre à l'essai la totalité des éléments pertinents du cadre, dans la limite des situations auxquelles le FSP pourrait raisonnablement s'attendre (p. ex., selon les causes et les risques recensés).
9. Les scénarios doivent évoluer au fil du temps, à mesure que les activités du FSP changent ou que l'environnement des menaces se transforme (p. ex., pour tenir compte de menaces plus sophistiquées en matière de sécurité de l'information).
10. Le FSP doit documenter son raisonnement derrière le choix des scénarios.

Mise à l'essai du plan de réponse aux incidents

11. Dans le cadre de sa méthode de mise à l'essai, le FSP doit régulièrement mettre à l'essai son plan de réponse aux incidents. Cette mise à l'essai doit répondre à différents objectifs, notamment :
    - confirmer l'exhaustivité et l'efficacité du plan
    - s'assurer que les cibles de fiabilité du FSP peuvent être atteintes
    - vérifier et maintenir l'état de préparation organisationnelle pour mettre en œuvre le plan lorsqu'il le faut
12. Le FSP doit mettre à l'essai son plan de réponse aux incidents (possiblement dans le cadre de plusieurs exercices), notamment en ce qui concerne les voies de recours hiérarchique, les mécanismes de prise de décision ou de gouvernance et la capacité du personnel concerné et des autres intéressés à suivre et à mettre en œuvre le plan ainsi qu'à reprendre le cours normal des activités.
    - La mise à l'essai doit également permettre de vérifier que les processus de sauvegarde fonctionnent et que les données et renseignements sauvegardés peuvent être récupérés de manière fiable.
    - Si, dans le cadre de son plan de réponse aux incidents, le FSP a l'intention de recourir à d'autres modalités de traitement ou à des solutions de contournement manuelles, il doit également mettre à l'essai sa capacité à les utiliser.

Annexe I : Tiers fournisseurs de services

Exemples de services qui peuvent être liés à une fonction de paiement

1. Parmi les exemples de services qui peuvent être liés à une fonction de paiement, il y a les services où un tiers fournisseur de services :
    - stocke, traite, transmet ou consulte des données ou des renseignements touchés par l'exercice d'activités associées aux paiements de détail du FSP ou créés à même l'exercice de ces activités (y compris les services infonuagiques et les installations de stockage de sauvegarde)
    - gère ou maintient pour le FSP des systèmes d'information, des logiciels, du matériel, des technologies ou des actifs pertinents qui sont liés à l'exercice de ses activités associées aux paiements de détail
    - fournit des services liés au risque opérationnel pour le compte du FSP (p. ex., des services liés à l'établissement, à la mise en œuvre ou à la maintenance du cadre du FSP ou d'éléments de ce cadre, notamment des services visant à aider le FSP à atténuer les risques et les incidents liés à la cybersécurité, à la sécurité de l'information ou à la sécurité physique, ou visant à y répondre)
    - fournit, ou s'est engagé à fournir, des ressources financières ou humaines au FSP en rapport avec la prestation de ses services de paiement de détail ou avec l'établissement, la mise en œuvre ou la maintenance du cadre du FSP; cela peut inclure des ressources provenant d'un tiers fournisseur de services auxquelles le FSP a accès en permanence pour soutenir ses activités habituelles, ainsi que des ressources supplémentaires auxquelles le FSP a l'intention d'accéder en cas de réponse à un incident ou de rétablissement après un incident (p. ex., des ressources humaines comme des experts externes ou des ressources financières d'urgence fournies par une société mère ou par des investisseurs)
    - effectue des mises à l'essai ou des examens indépendants
    - fournit un compte, une assurance ou une garantie au FSP afin de protéger des fonds d'utilisateurs finaux

Importance

2. Voici des exemples de facteurs à considérer en évaluant l'importance d'une entente avec un tiers fournisseur de services :
    - l'influence de cette entente sur les activités associées aux paiements de détail du FSP, notamment si le tiers fournisseur de services manque à l'exercice de ses activités pendant une période donnée ou lui fait complètement défaut
    - la capacité du FSP à maintenir des contrôles internes suffisants et à satisfaire aux exigences réglementaires, notamment si un tiers fournisseur de services manque à l'exercice de ses activités pendant une période donnée ou lui fait complètement défaut
    - la possibilité de remplacer le service fourni en temps opportun, notamment de le confier efficacement à un autre fournisseur ou de le rapatrier au sein du FSP
    - le degré de risque de concentration, c'est-à-dire le risque accru pouvant découler du fait que plusieurs services sont confiés au même tiers fournisseur de services

Évaluation des tiers fournisseurs de services

3. Les évaluations exigent qu'un FSP accède à différents types d'informations sur le tiers fournisseur de services afin de comprendre s'il peut fournir les services requis, s'aligner sur les objectifs du FSP et se conformer assidûment aux exigences réglementaires, et si des contrôles compensatoires supplémentaires sont nécessaires. Le FSP peut utiliser divers outils et ressources pour recueillir des informations complémentaires, y compris :
    - une analyse des états financiers
    - des certifications de parties indépendantes, des résultats d'audits, des résultats d'essais ou d'autres rapports indépendants sur l'environnement de contrôle et le rendement du fournisseur de services
    - des questionnaires ou des sondages
    - des documents préparés par le tiers fournisseur de services (p. ex., description des pratiques de gestion des risques)
    - des statistiques convenues d'avance (des mesures comme les ententes de prestation de services) et d'autres éléments (tels que les changements apportés au service ou à la manière dont il est fourni) déclarées par le fournisseur de services
    - des droits d'audit, des visites sur place et des réunions avec le fournisseur de services
    - des déclarations concernant la nature et l'étendue des relations de sous-traitance qui revêtent une importance pour les fonctions de paiement du FSP, ce qui peut aussi éclairer le FSP sur les risques de concentration
4. Les arrangements et les outils exacts utilisés varient d'un FSP à l'autre et peuvent dépendre de sa relation avec le tiers fournisseur de services.

Passation de contrats et répartition des responsabilités

5. La Banque reconnaît que les FSP n'ont pas nécessairement tous la même capacité d'établir des modalités contractuelles spécifiques sur mesure. Néanmoins, elle encourage le FSP à examiner si certaines modalités peuvent être établies dans leurs ententes contractuelles, notamment :
    - la nature et l'étendue des services à fournir
    - les ententes de prestation de services et les objectifs de rendement concernant la fiabilité opérationnelle, l'intégrité, la confidentialité, la disponibilité et d'autres mesures nécessaires
    - les obligations de déclaration (y compris le type et la fréquence des rapports) et les autres mécanismes de surveillance (tels que le droit pour le FSP d'évaluer, ou de faire évaluer par un auditeur indépendant, le service fourni par le tiers fournisseur de services) permettant au FSP de surveiller le rendement du tiers fournisseur de services
    - le signalement des violations ou des autres entraves, perturbations ou interruptions touchant les services fournis au FSP
    - les obligations prévoyant que le tiers fournisseur de services déclare qu'il a recours à d'autres fournisseurs de services importants, que ce soit par un contrat de sous-traitance ou d'autres ententes
    - les obligations prévoyant que le tiers fournisseur de services déclare les changements qu'il apporte à ses technologies, à ses services, à ses processus de gestion des risques ou aux autres fournisseurs de services importants auxquels il a recours, y compris les sous-traitants
    - l'accès et les obligations en matière d'audit ou de mise à l'essai

- les modalités de communication entre le FSP et le tiers fournisseur de services, y compris dans le cadre des activités normales et en cas d'incidents ou d'autres anomalies
- les exigences et les renseignements en matière de cybersécurité et de sécurité physique, y compris les arrangements entourant la protection des données
- la propriété des actifs
- la planification en cas d'urgence, comme les plans de continuité des activités, de réponse aux incidents et de reprise après sinistre, y compris les arrangements pris par le tiers fournisseur de services pour répondre à une atteinte aux données, renseignements et systèmes du FSP, ou aux siens, ainsi qu'à toute autre entrave, perturbation ou interruption touchant les services fournis au FSP ou en son nom
- les arrangements pris pour toute assistance que le tiers fournisseur de services fournirait au FSP
- la responsabilité et l'indemnisation
- les modalités de résolution des différends
- les modalités de résiliation, tant pour le FSP que pour le tiers fournisseur de services, couvrant le délai de résiliation et la manière dont les données seront traitées

Annexe J : Mandataires

Critères et évaluation des mandataires

1. Les évaluations exigent qu'un FSP accède à différents types de renseignements sur le mandataire afin de comprendre s'il peut fournir les services requis, s'aligner sur les objectifs du FSP et se conformer assidûment aux exigences réglementaires, et si des contrôles compensatoires supplémentaires sont nécessaires. Le FSP peut utiliser divers outils et ressources pour recueillir des renseignements complémentaires, y compris :
    - des audits, des visites sur place et des réunions avec le mandataire
    - une analyse des états financiers du mandataire
    - des déclarations du mandataire au FSP, par exemple concernant des statistiques (des mesures comme les ententes de prestation de services) et d'autres éléments (tels que les changements apportés au service ou à la manière dont il est fourni)
    - des résultats d'audits, des certifications de parties indépendantes, des résultats d'essais ou d'autres rapports indépendants sur l'environnement de contrôle et le rendement du mandataire
    - des questionnaires ou des sondages envoyés au mandataire par le FSP
    - des documents préparés par le mandataire (p. ex., description des pratiques de gestion des risques)
2. Les arrangements et les outils utilisés varient d'un FSP à l'autre et peuvent dépendre de sa relation avec le mandataire.