BANQUE DU CANADA
BANK OF CANADA

En bref : Le risque opérationnel et la réponse aux incidents

Le présent document complémentaire fait un survol de la ligne directrice *Le risque opérationnel et la réponse aux incidents* (la ligne directrice) et résume les exigences de gestion des risques opérationnels et de réponse aux incidents applicables aux fournisseurs de services de paiement (FSP). Il comprend également des considérations sur la portée de ces exigences et une liste de questions pour aider les FSP à évaluer et respecter ces exigences.

Le présent document ne remplace ni ne modifie la ligne directrice. Il doit être lu conjointement avec :

- la ligne directrice *Le risque opérationnel et la réponse aux incidents*
- la *Loi concernant les activités associées aux paiements de détail* (LAAPD)
- le *Règlement sur les activités associées aux paiements de détail* (le *Règlement*)

Il vise à aider les FSP à se conformer aux exigences de gestion des risques opérationnels et de réponse aux incidents de la LAAPD et du *Règlement*. Bien qu'il s'adresse principalement aux FSP qui en sont aux premières étapes de l'établissement et de la mise en œuvre de leur cadre de gestion des risques opérationnels et de réponse aux incidents (le cadre), d'autres FSP pourraient aussi le trouver utile.

Les considérations décrites dans le présent document ne sont pas exhaustives et ne couvrent pas toutes les exigences de la LAAPD et du *Règlement*. Tous les FSP doivent lire et respecter la LAAPD, le *Règlement* et la ligne directrice.

Comprendre les attentes en matière de gestion des risques opérationnels et de réponse aux incidents

Cette section explique ce qu'est un risque opérationnel, et décrit les exigences de gestion des risques opérationnels et de réponse aux incidents qui s'appliquent à vous, en tant que FSP, dans le contexte de la LAAPD.

Risque opérationnel

La LAAPD définit le risque opérationnel ainsi : « 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 : une défaillance des systèmes d'information ou du processus interne de ce fournisseur; une erreur humaine; une gestion défaillante ou inadéquate; une perturbation causée par un événement externe. »

Incident

La LAAPD définit un incident ainsi : « 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. »

Portée

Tous les FSP assujettis à la LAAPD doivent satisfaire aux exigences de gestion des risques opérationnels et de réponse aux incidents. Ces exigences s'appliquent à toutes leurs activités associées aux paiements de détail, y compris les services connexes fournis par un tiers.

Proportionnalité et approche fondée sur les risques

La Banque est consciente que les FSP représentent un groupe très diversifié d'entités. Vous devez adapter votre cadre de gestion des risques et de réponse aux incidents en fonction de ce qui suit :

- le type de risques opérationnels auxquels vous vous exposez
- la nature et la complexité de vos activités
- la taille et la structure de votre organisation
- les technologies que vous utilisez
- tout autre facteur pertinent

Exigences de gestion des risques opérationnels et de réponse aux incidents

Vous devez établir, mettre en œuvre et maintenir un cadre de gestion des risques opérationnels et de réponse aux incidents. Le cadre doit être conçu pour préserver l'intégrité, la confidentialité et la disponibilité de vos activités associées aux paiements de détail.

Pour ce faire, vous devez :

- recenser les risques opérationnels auxquels vous pourriez vous exposer en exerçant des activités associées aux paiements de détail
- protéger vos activités associées aux paiements de détail contre ces risques opérationnels
- déceler les incidents, les anomalies et les défaillances dans la mise en œuvre du cadre
- répondre aux incidents et vous en rétablir
- examiner et mettre à l'essai votre cadre
- gérer les risques liés au recours à des tiers

En cas de réponse à un incident ou de rétablissement après un incident, vous devez respecter les obligations de déclaration prévues par la LAAPD et le *Règlement*. Si un incident a des répercussions importantes sur certaines parties, vous devez en aviser toutes les parties concernées et la Banque dans un délai de 48 heures. Pour des précisions sur ces obligations, reportez-vous à la ligne directrice *La déclaration des incidents*.

Établir un cadre

Cette section énonce les exigences de gestion des risques opérationnels et de réponse aux incidents qui s'appliquent à vous, et répertorie des questions et des facteurs à prendre en considération pour vous aider à respecter ces exigences.

Pour en savoir plus sur chaque sujet, reportez-vous à la ligne directrice *Le risque opérationnel et la réponse aux incidents*.

Cadre

Votre cadre doit être documenté et disponible. Il doit également être adapté à votre propre situation et aux risques auxquels vous vous exposez. Pour plus d'informations, reportez-vous à l'**Introduction** et à la **section 1**, **Documentation et disponibilité du cadre**, de la ligne directrice.

Questions et facteurs à prendre en considération

- Votre cadre est-il consigné par écrit?
- Conservez-vous tous les documents relatifs à votre conformité aux exigences réglementaires?
- Comment veillez-vous à ce que votre cadre soit disponible pour les personnes qui jouent un rôle dans sa mise en œuvre et son maintien?
- Votre cadre est-il adapté à votre situation, y compris au type et à l'importance des risques auxquels vous vous exposez?
- Lors de l'établissement de votre cadre, avez-vous tenu compte des répercussions possibles d'une entrave, d'une perturbation ou d'une interruption de vos activités associées aux paiements de détail?

Objectifs

Vous devez vous fixer des objectifs pour préserver l'intégrité, la confidentialité et la disponibilité de vos activités associées aux paiements de détail, et suivre l'atteinte de ces objectifs à l'aide de cibles de fiabilité et d'indicateurs. Pour plus d'informations, reportez-vous à la **section 2**, **Objectifs**, de la ligne directrice.

Questions et facteurs à prendre en considération

- Quels sont vos objectifs en matière d'intégrité, de confidentialité et de disponibilité?
- Comment ces objectifs assurent-ils l'intégrité, la confidentialité et la disponibilité de vos activités associées aux paiements de détail?
- Comment surveillez-vous et évaluez-vous l'atteinte de vos objectifs?
- Avez-vous fixé des cibles de fiabilité et des indicateurs pour évaluer si vos objectifs sont atteints?

Rôles et responsabilités

Vous devez assurer la répartition et le maintien des rôles et responsabilités pour tous les aspects de votre cadre, y compris les rôles et responsabilités confiés à des tiers. Pour plus d'informations, reportez-vous à la **section 3**, **Rôles et responsabilités**, de la ligne directrice.

Questions et facteurs à prendre en considération

- Quels sont les rôles et les responsabilités nécessaires pour vous assurer de pouvoir efficacement atténuer les risques opérationnels et répondre aux incidents?
- Avez-vous défini les rôles et les responsabilités dans le cours normal des activités et lors de la réponse aux incidents?
- Comment veillez-vous à ce qu'il y ait une surveillance et un examen critique suffisants pour que ces rôles et responsabilités soient assumés efficacement?
- Avez-vous nommé un cadre dirigeant? Cette personne devrait :
    - surveiller votre conformité aux exigences réglementaires en matière de risques opérationnels, de réponse aux incidents et de déclaration des incidents
    - prendre les décisions importantes relativement à votre gestion des risques opérationnels et des incidents, et aux mesures que vous prenez en réponse à ces risques et incidents
    - approuver le cadre, au moins une fois par année et après toute modification importante qui y est apportée
- Si vous avez un conseil d'administration, celui-ci est-il également responsable d'approuver le cadre au moins une fois par année?

Ressources humaines et financières

Vous devriez disposer d'un accès rapide et fiable aux ressources humaines et financières pour établir, mettre en œuvre et maintenir votre cadre. Pour plus d'informations, reportez-vous à la **section 4**, **Ressources humaines et financières**, de la ligne directrice.

Questions et facteurs à prendre en considération

- Quelles sont les ressources humaines nécessaires pour assumer les rôles et responsabilités établis?
- Comment faites-vous en sorte d'avoir un accès rapide et fiable à ces ressources, tant dans le cours normal des activités que lors de la réponse aux incidents?
- Quelles sont les compétences, la formation et l'information dont les ressources humaines (internes ou externes) ont besoin pour s'acquitter des responsabilités qui leur sont confiées?
    - Comment veillez-vous à ce que vos ressources humaines reçoivent l'information et la formation nécessaires?
- Quelles ressources financières sont requises pour établir, mettre en œuvre et maintenir le cadre, tant dans le cours normal des activités que lors de la réponse aux incidents?

Recenser

Vous devez recenser et comprendre vos risques opérationnels, vos actifs et vos processus opérationnels. Pour plus d'informations, reportez-vous à la **section 5**, **Recenser**, de la ligne directrice.

Questions et facteurs à prendre en considération

- Quels sont les risques opérationnels qui pourraient entraîner une entrave, une perturbation ou une interruption de vos activités associées aux paiements de détail?
- Quelles sont les causes potentielles de ces risques opérationnels?
- Quels sont les actifs (systèmes, données et renseignements) et les processus opérationnels qui sont liés à vos activités associées aux paiements de détail?
    - Quels actifs et processus opérationnels doivent être disponibles et fonctionner comme prévu pour que vous puissiez effectuer efficacement vos activités associées aux paiements de détail?
- Quelles sont la sensibilité et l'importance de chaque actif et processus opérationnel recensé?
    - Quelle est leur importance pour l'exécution des activités associées aux paiements de détail et l'atteinte de vos objectifs en matière de confidentialité, d'intégrité et d'imputabilité?

Protéger

Vous êtes responsable de préserver l'intégrité, la confidentialité et la disponibilité de vos activités associées aux paiements de détail en atténuant les risques opérationnels ainsi qu'en protégeant les actifs et les processus opérationnels. Pour plus d'informations, reportez-vous à la **section 6**, **Protéger**, de la ligne directrice.

Questions et facteurs à prendre en considération

- Quels éléments de protection (systèmes, politiques, procédures, processus, contrôles ou autres moyens) sont nécessaires pour atténuer les risques opérationnels auxquels vous vous exposez et protéger vos actifs et vos processus opérationnels?
- Comment vous assurez-vous que les éléments de protection sont efficaces pour atténuer les risques opérationnels, protéger les actifs et les processus opérationnels, et soutenir l'atteinte de vos objectifs?

Déceler

Vous devez déceler et faire remonter rapidement les incidents, les anomalies et les défaillances dans la mise en œuvre du cadre. Pour plus d'informations, reportez-vous à la **section 7**, **Déceler**, de la ligne directrice.

Questions et facteurs à prendre en considération

- Quels types d'incidents et d'anomalies pourraient survenir dans vos activités associées aux paiements de détail?
- Quels types de défaillances pourraient survenir dans la mise en œuvre de votre cadre?
- Comment assurez-vous une surveillance en continu pour déceler rapidement ces incidents, anomalies et défaillances?

- Comment réagissez-vous lorsqu'une anomalie ou une défaillance dans la mise en œuvre du cadre est décelée?
    - Quels sont vos processus de recours hiérarchique et de prise de décision?

Réponse et rétablissement

Vous devez utiliser le plan que vous avez établi pour répondre aux incidents et vous en rétablir. Pour plus d'informations, reportez-vous à la **section 8**, **Réponse et rétablissement**, de la ligne directrice.

Questions et facteurs à prendre en considération

- Quel est votre plan pour répondre aux incidents et vous en rétablir?
- Le plan de réponse et de rétablissement couvre-t-il tous les incidents plausibles, y compris ceux qui mettent en cause un tiers ou qui sont décelés par celui-ci?
- Le plan de réponse et de rétablissement indique-t-il comment vous allez :
    - faire enquête sur les répercussions d'un incident et prendre des mesures pour les atténuer immédiatement
    - répondre à un incident et rétablir les activités associées aux paiements de détail, tout en préservant leur confidentialité et leur intégrité
    - faire remonter, signaler et coordonner la réponse aux incidents avec les parties prenantes internes et externes
    - faire enquête sur la cause première de chaque incident et la traiter
    - garder une trace de chaque incident et des plans d'action associés
- Comment vous assurez-vous que la Banque, ainsi que les utilisateurs finaux, les autres FSP et les chambres de compensation ayant subi des répercussions importantes, sont avisés dans les 48 heures suivant un incident ayant de telles répercussions?

Tiers fournisseurs de services et mandataires

Dans le cadre de la gestion des risques associés aux tiers que vous effectuez, vous devez gérer les risques provenant du recours à des tiers fournisseurs de services ou des mandataires. Pour plus d'informations, reportez-vous à la **section 12**, **Tiers fournisseurs de services**, et à la **section 13**, **Mandataires**, de la ligne directrice.

Questions et facteurs à prendre en considération

Si vous recevez des services liés à une fonction de paiement de la part de **tiers fournisseurs de services** :

- Quels sont les risques auxquels vous vous exposez en ayant recours à des tiers fournisseurs de services? Comment gérez-vous ces risques?
- Quelles seraient les répercussions sur vos activités associées aux paiements de détail en cas d'altération des services fournis par un tel tiers?
- Quelles mesures de diligence raisonnable prenez-vous pour atténuer adéquatement les risques qui découlent du fait que vous confiez la prestation de certains services à des tiers?
    - À tout le moins, une évaluation est-elle exercée chaque année et avant la conclusion, le renouvellement, la prolongation ou la modification substantielle d'un contrat?
    - Qu'est-ce qui est vérifié lors de l'évaluation d'un tiers fournisseur de services?
    - Quels contrôles compensatoires sont nécessaires pour atténuer les risques associés aux tiers fournisseurs de services?
- Quels rôles et responsabilités doivent être établis pour superviser et surveiller le rendement des tiers fournisseurs de services?

Si un **mandataire** effectue des activités associées aux paiements de détail en votre nom :

- Quels sont les risques auxquels vous vous exposez en ayant recours à des mandataires? Comment gérez-vous ces risques?
- Quelles mesures de diligence raisonnable prenez-vous pour atténuer adéquatement les risques qui découlent du recours à un mandataire?
    - Quels sont les critères minimaux que vous exigez qu'un mandataire potentiel remplisse avant de conclure une entente avec lui?
    - Procédez-vous à une évaluation des mandataires au moins une fois par année?
    - Quels contrôles compensatoires sont nécessaires pour atténuer les risques associés aux mandataires?
- Quels rôles et responsabilités doivent être établis pour superviser et surveiller le rendement des mandataires?

Examiner et mettre à l'essai le cadre

Examen interne

Vous devez examiner votre cadre au moins une fois par an et avant d'y apporter des modifications importantes, et vous devez corriger toutes les lacunes ou vulnérabilités cernées lors de l'examen. Pour plus d'informations, reportez-vous à la **section 9**, **Examen interne**, de la ligne directrice.

Questions et facteurs à prendre en considération

- Effectuez-vous un examen interne de votre cadre au moins une fois par an et avant d'y apporter des modifications importantes?
- L'examen interne évalue-t-il :
    - la conformité du cadre aux exigences réglementaires
    - l'efficacité du cadre à favoriser l'atteinte des objectifs de confidentialité, d'intégrité et de disponibilité
    - l'adéquation des ressources humaines et financières
- Comment donnez-vous suite aux résultats des examens internes?

Mises à l'essai

Vous devez mettre à l'essai tous les éléments de votre cadre pour recenser et corriger les lacunes. Pour plus d'informations, reportez-vous à la **section 10**, **Mises à l'essai**, de la ligne directrice.

Questions et facteurs à prendre en considération

- Effectuez-vous des mises à l'essai de votre cadre?
    - Quel type de mises à l'essai effectuez-vous pour recenser efficacement les lacunes dans l'efficacité et les vulnérabilités du cadre?
    - Quelle est la portée des mises à l'essai?
    - À quelle fréquence effectuez-vous ces mises à l'essai?
- Comment donnez-vous suite aux résultats des mises à l'essai?

Examen indépendant

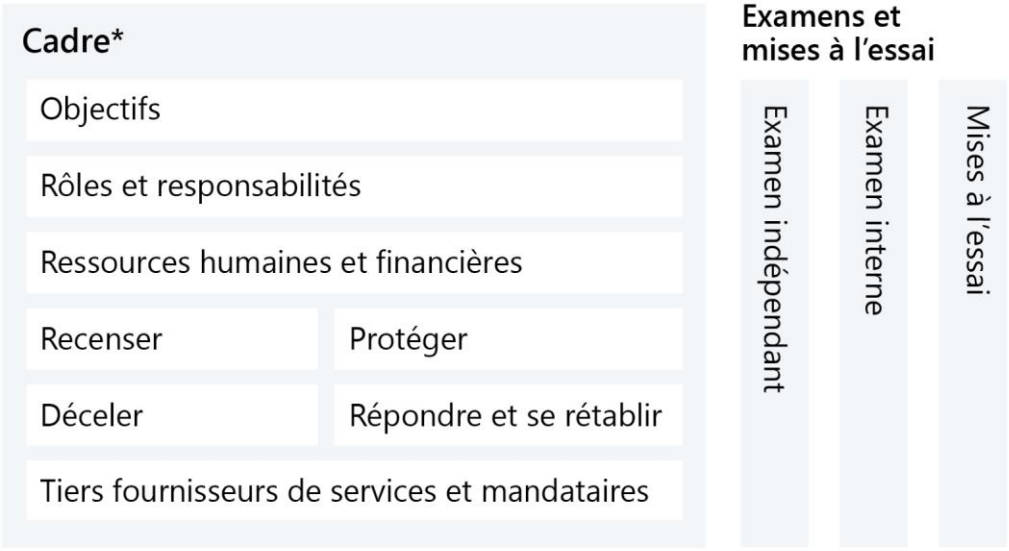
Si vous avez un auditeur interne ou externe, un examen indépendant du cadre doit être effectué au moins une fois tous les trois ans, et vous devez corriger les lacunes et les vulnérabilités décelées. Pour plus d'informations, reportez-vous à la **section 11**, **Examen indépendant**, de la ligne directrice.

Questions et facteurs à prendre en considération

- Si vous avez un auditeur interne ou externe, veillez-vous à ce qu'un examen indépendant soit effectué au moins une fois tous les trois ans?

    - L'examen est-il effectué par une personne indépendante et compétente?
- L'examen indépendant évalue-t-il la conformité à l'article 5 et aux articles 6 à 9 du *Règlement*?
- Comment donnez-vous suite aux résultats des examens indépendants?

Figure 1 : **Exigences de gestion des risques et de réponse aux incidents**



* Le cadre de tout FSP doit être approuvé et disponible.