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

BANQUE DU CANADA
BANK OF CANADA

Comité consultatif sur les paiements de détail
Attentes quant à la gestion du risque opérationnel

28 et 29 octobre 2020

La présente note vise à aider les participants à préparer la réunion d'octobre du Comité consultatif intérimaire sur les paiements de détail (le « Comité »), qui sera notamment consacrée aux attentes envisageables à l'égard des fournisseurs de services de paiement (FSP) de détail en ce qui concerne la gestion du risque opérationnel. Sur la base des renseignements obtenus en juillet et en août par la Banque du Canada (la « Banque ») auprès du Comité et des pratiques d'autres organismes de réglementation, les attentes suivantes pourraient s'avérer appropriées pour s'assurer que les FSP remplissent les objectifs réglementaires visant la gestion du risque opérationnel[1].

Les membres du Comité sont invités à formuler des commentaires sur tout aspect lié aux attentes envisageables décrites dans la présente note, en particulier sur :

1) **les obstacles d'ordre structurel ou pratique qui pourraient entraver la capacité du FSP à répondre à ces attentes;**
2) **la façon dont les attentes répertoriées pourraient ne pas être suffisantes pour remplir les objectifs réglementaires.**

Les commentaires concernant le point 1) pourraient notamment couvrir tout domaine dans lequel les attentes envisageables divergent sensiblement des normes internationales acceptées.

Dans la mesure du possible, les membres sont invités à donner leur avis sur l'application des attentes dans l'ensemble du secteur, ainsi que du point de vue de leur propre organisation.

Veuillez noter que ces attentes ont été rédigées par la Banque et sont toujours en cours d'élaboration. Des renseignements précis sont fournis uniquement pour clarifier les attentes et faciliter la discussion. **Ces attentes sont susceptibles d'être modifiées en fonction de consultations et de considérations réglementaires futures. En dernier ressort, c'est au gouvernement qu'incombe la responsabilité de proposer des lois et des règlements pour mettre en œuvre le nouveau cadre de surveillance.**

Contrairement aux réunions précédentes du Comité, aucune question de discussion particulière n'est énoncée dans la présente note, car l'objectif de cette séance sera de passer en revue les attentes envisageables et de recenser les préoccupations des participants.

---

[1] Les attentes envers les FSP quant à la gestion du risque opérationnel devraient se rattacher à trois objectifs : intégrité, confidentialité et disponibilité. Le cadre de surveillance applicable aux FSP est destiné à intégrer des mesures proportionnelles aux risques qu'ils représentent pour l'économie et, en conséquence, les attentes visent à mettre l'accent sur la protection des utilisateurs finaux, par rapport à la surveillance des institutions d'importance systémique et des institutions importantes.

ATTENTES ENVISAGEABLES

Cadre

Les FSP pourraient être appelés à se doter d'un cadre de gestion du risque opérationnel et d'intervention en cas d'incident (le « cadre[2] ») leur permettant de déterminer les risques opérationnels; de protéger leurs activités de paiement de détail contre ces risques; de détecter les incidents et de surveiller les pannes; d'intervenir en cas d'incident, puis de reprendre leurs activités. Il pourrait être requis que ce cadre soit :

- approuvé par un haut dirigeant de l'organisation[3], et par le conseil d'administration, si le FSP en est doté;
- documenté;
- communiqué au personnel et aux autres intervenants responsables de sa mise en œuvre.

On peut s'attendre à ce que le cadre du FSP soutienne la réalisation de certains objectifs de fiabilité opérationnelle, en particulier la préservation de la confidentialité et de l'intégrité et le maintien de niveaux adéquats de disponibilité des activités de paiement de détail du FSP et des systèmes, ainsi que des données ou des renseignements qui permettent la prestation ou la facilitation de ces activités.

- Pour déterminer ce qu'est un niveau « adéquat » de disponibilité, le FSP pourrait devoir prendre en compte les répercussions d'une indisponibilité sur ses utilisateurs finaux et les entités interconnectées (y compris les autres FSP).
- Le FSP pourrait être tenu d'adopter des cibles mesurables liées à ses objectifs de disponibilité, notamment un délai de reprise visé, une cible de disponibilité des systèmes et un point de reprise visé.

Le FSP pourrait être appelé à définir les rôles et les responsabilités pour tous les aspects de son cadre, que ce soit en temps normal, mais aussi lors de la détection et de la gestion des incidents. L'attribution des rôles et responsabilités devrait permettre de poser les bonnes questions et d'assurer une surveillance en ce qui concerne la gestion du risque opérationnel au sein du FSP, en fonction de sa taille, de ses activités et de sa complexité.

Le FSP pourrait devoir démontrer qu'il aurait accès à des ressources financières et humaines suffisantes pour mettre en œuvre son cadre, ce qui comprend ses dispositifs et son plan d'intervention en cas d'incident. Les ressources humaines devraient être suffisamment qualifiées et formées.

Le FSP pourrait être tenu de revoir son cadre au moins une fois par an, à la suite de tout changement important touchant les activités ou les mécanismes de contrôle du risque opérationnel, et à la suite d'incidents opérationnels notables.

---

[2] Le terme « cadre » pourrait couvrir les objectifs, les rôles et les responsabilités, les systèmes, les politiques, les procédures et les contrôles qui font partie des activités menées par le FSP dans le domaine de la gestion du risque opérationnel.

[3] C'est-à-dire une personne qui est responsable des activités du FSP et de la prise de décision au sein de celui-ci.

Déterminer les risques opérationnels

Le FSP pourrait devoir déterminer et documenter tous les risques opérationnels plausibles et toutes les sources plausibles de ces risques. Les processus adoptés pour répondre à cette attente devraient être adaptés à la taille, aux activités et à la complexité du FSP.

Parmi les sources plausibles de risque opérationnel que le FSP pourrait être amené à prendre en compte, citons notamment les menaces internes; les menaces externes; les pratiques en matière d'emploi; les clients, les produits et les pratiques commerciales; les dommages aux biens matériels; les interruptions d'activités et les pannes de systèmes; l'exécution, la livraison et la gestion des processus; les tiers, dont les utilisateurs finaux, les infrastructures de marché financier, les autres FSP, les mandataires, et les fournisseurs de services externes; les autres activités du FSP; le changement et la gestion du changement; l'erreur humaine; les catastrophes naturelles et autres situations d'urgence.

Le FSP pourrait également être tenu de dresser l'inventaire des biens qui devraient être protégés afin d'atteindre ses objectifs de disponibilité opérationnelle (à savoir la préservation de la confidentialité et de l'intégrité et le maintien de niveaux adéquats de disponibilité). Pour dresser cet inventaire, il peut être opportun pour le FSP de prendre en compte la mesure dans laquelle le bien est essentiel à la réalisation des activités de paiement de détail.

Protéger

Le FSP pourrait devoir établir des mesures de protection pour atténuer tous les risques opérationnels plausibles de manière à atteindre les objectifs quant à la préservation de la confidentialité et de l'intégrité et au maintien de niveaux adéquats de disponibilité.

Ces mesures de protection seraient censées :

- protéger les biens que le FSP a définis comme étant essentiels à la réalisation des activités de paiement de détail;
- atténuer la probabilité de destruction, de modification ou de perturbation accidentelle ou délibérée des données et renseignements et des systèmes;
- protéger les données et l'information pendant qu'elles sont stockées, utilisées ou transmises.

Le FSP pourrait être appelé à évaluer jusqu'à quel point ses mesures de protection sont adaptées au vu des répercussions qu'une atteinte à la confidentialité, à l'intégrité ou à la disponibilité pourrait avoir sur ses utilisateurs finaux et les entités interconnectées (par exemple, d'autres FSP) auxquelles il fournit des services. Il pourrait être exigé que cette évaluation prenne en compte le nombre d'utilisateurs finaux et d'entités interconnectées susceptibles d'être touchés.

Contrôler l'accès

Dans le cadre de ses mesures de protection, le FSP pourrait devoir établir des contrôles qui réduisent au minimum le risque d'accès par des parties internes et externes non autorisées. L'ampleur des contrôles d'accès mis en œuvre par le FSP (c'est-à-dire l'adoption de contrôles multiniveaux[4]) devrait être adaptée aux répercussions sur les activités de paiement de détail que pourrait avoir un accès non autorisé aux

[4] Le concept de contrôles d'accès « multiniveaux » vise à saisir comment un seul niveau de contrôle pourrait ne pas suffire selon le caractère essentiel du bien (c'est-à-dire les données, les technologies de l'information et de la communication).

données ou renseignements et aux systèmes qui permettent la prestation ou la facilitation de ces activités.

Le contrôle de l'accès devrait permettre au FSP :

- d'atténuer les risques de menaces internes liés aux changements de statut d'emploi;
- de limiter aux seules personnes autorisées l'accès aux données et renseignements et aux systèmes;
- de suivre, de consigner et d'examiner l'historique des accès et des activités;
- de consigner et d'examiner les activités de maintenance et de réparation.

Détecter

Le FSP pourrait être tenu d'établir des mécanismes de contrôle permettant la détection des incidents opérationnels et des défaillances des mesures de contrôle du risque opérationnel. Pour ce faire, il conviendrait de mettre préalablement en place des processus de transmission des incidents aux échelons supérieurs et de prise de décision concernant ce type d'incidents et de défaillances.

Intervention et reprise

Intervenir en cas d'incident

Le FSP pourrait être tenu de mener rapidement une enquête lors de la détection d'un incident. Il pourrait être requis que cette enquête porte sur la nature et la ou les causes premières de l'incident, ainsi que sur ses répercussions sur les activités de paiement de détail du FSP, les utilisateurs finaux et les autres FSP ou parties concernées.

En cas d'incident, le FSP pourrait être tenu de prendre des mesures pour :

- prévenir ou atténuer d'autres atteintes à la confidentialité, à l'intégrité ou à la disponibilité, pendant que l'incident fait l'objet d'une enquête;
- remédier aux vulnérabilités ou lacunes repérées lors de sa réponse à l'incident et de son enquête.

Ces mesures pourraient être classées par ordre de priorité au moyen d'une approche fondée sur les risques.

Il pourrait être exigé que le FSP ne reprenne ses activités normales qu'après avoir vérifié que l'intégrité et la confidentialité des données et renseignements et des systèmes ont été rétablies de manière suffisante pour une reprise en toute sécurité.

Rôles et responsabilités pour intervenir en cas d'incident

Le FSP pourrait être censé établir des rôles et des responsabilités précis pour les interventions en cas d'incident. Il pourrait s'agir de préciser qui, au sein de l'organisation, serait responsable de l'exécution des tâches de notification, de coordination et de traitement liées à un incident, ainsi que de définir les processus de transmission aux échelons supérieurs et de prise de décision. Des formations et des mises à l'essai seraient requises pour vérifier que ces rôles et responsabilités pourraient être exercés comme prévu en cas d'incident.

Cadre d'intervention en cas d'incident et plans de continuité des opérations

Dans son cadre de gestion du risque opérationnel et d'intervention en cas d'incident, le FSP pourrait être tenu d'établir un plan décrivant la manière dont il réagirait à un incident et assurerait la reprise des activités. Ce plan devrait tenir compte de tous les événements susceptibles de présenter un risque pour la

préservation de la confidentialité et de l'intégrité et le maintien de niveaux adéquats de disponibilité, ou un risque pour la prestation ou la facilitation des activités de paiement de détail. Il pourrait s'agir d'événements susceptibles de provoquer l'indisponibilité de personnes, de processus ou de systèmes essentiels ou de leur porter atteinte pendant des périodes prolongées.

Les objectifs du plan pourraient être les suivants : déterminer comment le FSP renouerait avec ses objectifs de fiabilité opérationnelle et faciliter le retour aux activités normales. Dans cette optique, le plan devrait permettre de déterminer, rapidement et avec certitude, l'état de toutes les transactions au moment de la perturbation.

Pour atteindre ces objectifs, le plan serait censé aborder une série de questions, notamment :

- comment le FSP s'attend à récupérer les données perdues ou corrompues, à corriger les problèmes d'intégrité des données et à poursuivre ou reprendre ses activités de paiement de détail, à la suite d'un incident – et la rapidité avec laquelle il compte y parvenir;
- les ressources humaines et financières dont le FSP devrait disposer (ou auxquelles il devrait avoir accès) pour mettre en œuvre le plan;
- les processus manuels ou les autres solutions de rechange que le FSP pourrait envisager d'adopter en cas d'indisponibilité des systèmes principaux;
- la prise en compte des cadres d'intervention en cas d'incident ou des plans de continuité des opérations de ses fournisseurs de services externes.

On pourrait également s'attendre à ce que le FSP précise les modalités de mise en œuvre du plan, telles que : le ou les déclencheurs de la mise en œuvre du plan et de la transmission de l'incident aux échelons supérieurs; les modalités de notification et de traitement de l'incident jusqu'à sa conclusion; et les modalités de coordination avec les parties prenantes internes et externes.

Mises à l'essai et audit

Le FSP pourrait être appelé à établir un programme de mise à l'essai pour valider la pertinence et l'efficacité du cadre, et en repérer les lacunes ou les vulnérabilités. Ce programme pourrait être censé :

- recourir à diverses méthodologies et pratiques de façon à ce que chaque mise à l'essai soit adéquate pour valider la pertinence et l'efficacité de la composante particulière du cadre visée;
- couvrir tous les éléments du cadre du FSP de manière exhaustive, au moins tous les trois ans.

Les mises à l'essai devraient être fondées sur des scénarios de menaces pertinentes et connues, ainsi que sur un ensemble adéquat de scénarios graves, mais plausibles. Il pourrait être exigé que chaque mise à l'essai soit conçue de façon à évaluer si le FSP serait en mesure de remplir ses objectifs de fiabilité opérationnelle en réponse à ces scénarios. Les mises à l'essai pourraient devoir porter sur des solutions temporaires manuelles si le FSP en est doté.

Chaque mise à l'essai pourrait être censée :

- faire intervenir les parties prenantes et les décideurs internes concernés;
- tenir compte des dépendances du FSP vis-à-vis des parties prenantes externes telles que les fournisseurs de services externes et les mandataires, et faire participer celles qui sont concernées, le cas échéant.

On pourrait s'attendre à ce que des mises à l'essai individuelles soient effectuées régulièrement, au moins une fois par an, ainsi qu'avant tout changement important dans les activités du FSP.

Après une mise à l'essai, le FSP devrait tirer des leçons et déterminer si son cadre devrait être bonifié ou modifié.

Audits

Le FSP pourrait être tenu de procéder à un audit interne, un audit externe ou un examen indépendant de certaines composantes de son cadre (soit les politiques, les systèmes, les contrôles, les procédures et les processus), de façon régulière, au moins une fois tous les deux ans. Par ailleurs, tous les éléments de son cadre devraient être audités ou soumis à un examen indépendant sur une période de trois ans.

L'objectif d'un audit, ou d'un examen indépendant, serait d'évaluer :

- la mesure dans laquelle les politiques, les systèmes, les procédures et les processus du FSP respectent les exigences en matière de gestion du risque opérationnel énoncées dans le cadre de surveillance des paiements de détail;
- si les politiques et procédures de prise de décision, ainsi que les rôles et responsabilités du FSP lui permettent de remplir les objectifs de préservation de la confidentialité et de l'intégrité et de maintien de niveaux adéquats de disponibilité.

Si le FSP a à sa disposition un auditeur interne, un service d'audit interne ou un auditeur externe, on pourrait s'attendre à ce que l'audit interne ou externe soit effectué par le service ou l'auditeur en question. À défaut de telles ressources, il pourrait être requis qu'un examen indépendant soit mené par une ou plusieurs personnes au sein du FSP qui n'interviennent pas dans les fonctions de gestion du risque opérationnel.

Fournisseurs de services externes

Si le FSP fait appel à des fournisseurs de services externes, il pourrait être tenu de faire preuve de diligence raisonnable à l'égard de ces prestataires, en couvrant leurs pratiques dans le domaine de la gestion du risque opérationnel et les risques opérationnels auxquels il pourrait être confronté en faisant appel à leurs services.

Le FSP pourrait être appelé à établir des critères de gestion des risques opérationnels à prendre en compte lors de la sélection et de la gestion des fournisseurs de services externes. Ces critères pourraient inclure les volets suivants :

- la manière dont le fournisseur de services externes informe et consulte le FSP avant d'apporter des modifications aux dispositions prises avec celui-ci (p. ex., modifications des connexions avec le FSP, des produits fournis au FSP, du stockage ou de l'utilisation des données);
- les modalités permettant au fournisseur de services externes d'informer le FSP en cas de violation des données ou d'autres incidents opérationnels;
- les dispositions liées à la gestion de la sécurité des connexions externes.

Les accords conclus par le FSP avec ses fournisseurs de services externes pourraient notamment être censés :

- décrire précisément la répartition des responsabilités entre le prestataire de services externes et le FSP;
- énoncer des modalités précises concernant la propriété et la confidentialité des données.

Mandataires

Si le FSP fait appel à des mandataires, il pourrait être tenu d'évaluer si les activités de paiement de détail fournies en son nom par ceux-ci respectent les exigences quant à la gestion du risque opérationnel énoncées dans le cadre de surveillance des paiements de détail proposé.

Les accords conclus par le FSP avec ses mandataires pourraient notamment être censés :

- décrire précisément la répartition des responsabilités entre le mandataire et le FSP;
- énoncer des modalités précises concernant la propriété et la confidentialité des données.

Transmission de rapports à la Banque

Pour vérifier que le FSP respecte les attentes, la Banque pourrait demander à recevoir des documents ou d'autres rapports régulièrement (p. ex., chaque année) ou à la suite d'un changement important, entre autres :

- le cadre, les politiques, les procédures, les contrôles, et les rôles et responsabilités documentés (p. ex., comme mentionné tout au long de la présente note);
- les documents relatifs aux objectifs de fiabilité du FSP, et les rapports sur les résultats obtenus au regard de ces objectifs;
- les documents ou rapports du FSP concernant la détermination des risques et des biens essentiels;
- les rapports sur l'exécution et les résultats des examens et des évaluations;
- les rapports sur le recours à des fournisseurs de services externes et à des mandataires, ainsi que des éléments attestant les accords conclus avec ces parties et de la diligence raisonnable exercée à leur égard;
- les rapports sur l'exécution et les résultats des mises à l'essai et des audits.