BANQUE DU CANADA
BANK OF CANADA

Comité consultatif sur les paiements de détail

Risque opérationnel

26 et 27 août 2020

La présente note a pour but d'aider les participants à se préparer à la réunion d'août 2020 du Comité consultatif sur les paiements de détail (le « Comité »). En juillet, le Comité s'est penché sur les objectifs et la portée d'éventuelles attentes envers les fournisseurs de services de paiement (FSP) quant à la gestion du risque opérationnel et, de façon générale, sur les concepts potentiellement associés à ces attentes. Comme mentionné aux séances de juillet, les séances d'août seront basées sur la « pièce jointe nº 1 » des documents de travail de juillet, jointe plus loin à titre de référence.

Cette réunion a pour but d'aider la Banque à :

- mieux connaître les pratiques de gestion du risque opérationnel des membres du Comité;
- voir si des points nécessitent une interprétation ou des éclaircissements.

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

Comme mentionné en juillet, les normes de gestion des risques peuvent être envisagées d'un point de vue fonctionnel. De façon générale, il est prévu que les FSP devront se doter d'un **cadre de gestion du risque opérationnel** qui leur permettra : de **déterminer** les risques opérationnels; de **protéger** leurs activités de paiement contre ces risques; de **détecter** les incidents opérationnels; d'**intervenir** en cas d'incident, puis de **reprendre** leurs activités. Les FSP pourront aussi être appelés à **évaluer** et à **tester** leur cadre, ainsi que les politiques, procédures et contrôles connexes, et à tirer des leçons de ces tests pour renforcer leurs capacités de gestion du risque opérationnel. C'est sur cette approche fonctionnelle que se fonde la structure de la présente note.

Questions à débattre

Cadre

1) Dans le document de juillet, on pouvait lire que les exigences en matière de risque opérationnel envers les FSP se rattacheraient à trois objectifs :

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

   a) D'après l'approche fonctionnelle du cadre de surveillance des paiements de détail, la surveillance par la Banque quant à ces objectifs se limiterait aux activités de paiement de détail des FSP (et ne s'appliquerait pas à leurs autres activités) et porterait plus particulièrement sur les données et les systèmes utiles à leur exécution. Ces précisions clarifient-elles suffisamment le champ d'application des objectifs? Si non, quels autres renseignements seraient utiles?

b) Comment votre organisation détermine-t-elle ce qu'est un niveau « raisonnable » de disponibilité des services?
c) Est-ce que des facteurs externes (ex. : exigences d'autres autorités réglementaires, contrats commerciaux avec d'autres FSP, participation à d'autres systèmes) influent sur les cibles de votre organisation ou sur sa capacité à atteindre les objectifs précités?

Détermination

2) La Banque a entendu dire que, pour les FSP, les événements et risques opérationnels (en général) les plus préoccupants étaient :

   - les défaillances opérationnelles, dont les problèmes de logiciels ou de matériel informatique, qui nuisent à la disponibilité des services;
   - les incidents de sécurité des données ou de cybersécurité qui peuvent compromettre l'intégrité ou la confidentialité des systèmes ou des données.

   a) Cette liste est-elle exhaustive?
   b) Quelles sources de risque opérationnel sont les plus préoccupantes? (ex. : menaces externes ou internes; défaillances associées à un tiers?)
3) Les normes courantes de sécurité de l'information et de cybersécurité recommandent de recenser les actifs essentiels à protéger absolument. Quelle méthode votre organisation emploie-t-elle pour déterminer quels actifs sont essentiels à ses activités?

Protection

4) La Banque sait que les ressources disponibles pour atténuer le risque opérationnel ne sont pas illimitées. Comment les FSP s'y prennent-ils pour établir leurs priorités d'investissement dans les mesures de protection contre les risques connus?
   a) En quoi cet ordre de priorité influe-t-il sur le choix entre des mesures de protection, de détection ou de réaction?
   b) La hiérarchisation des priorités d'investissement dans les mesures de protection contre les risques oblige-t-elle votre organisation à choisir entre la confidentialité, l'intégrité et la disponibilité? Si oui, comment arrive-t-elle à déterminer quel objectif est plus important qu'un autre?
5) Dans le document de juillet, il était question de protéger la confidentialité et l'intégrité des données utilisées, transmises ou stockées, comme dans les normes courantes de sécurité de l'information et de cybersécurité.
   a) Quels sont les défis que votre organisation rencontre lorsqu'il s'agit de protéger la confidentialité et l'intégrité des données pendant la transmission?
   b) Comment les responsabilités de la protection des données en cours de transmission sont-elles établies et coordonnées entre les parties d'une chaîne de paiement?

Intervention et reprise des activités

6) Comment votre organisation envisage-t-elle la planification de la continuité des opérations? Quels types de scénarios son plan prévoit-il?
7) Comment votre organisation reprendrait-elle ses activités en cas de compromission de ses données ou systèmes?
8) Ressources humaines et financières : Dans le cadre de sa planification de la continuité des opérations, votre organisation estime-t-elle les ressources humaines et financières que peut nécessiter la mise en application du plan de continuité des opérations dans divers scénarios?
   a) Si oui, comment fait-elle ces estimations?

b) A-t-elle conclu des ententes lui donnant accès aux ressources financières nécessaires pour intervenir au cas où un événement important perturberait ses activités?
c) Comment veille-t-elle à la fiabilité de l'accès à ces ressources humaines et financières en situation de crise, surtout si elle compte sur un tiers pour les fournir?

Questions pour réponse écrite

Lors des séances du Comité, la Banque souhaite axer les discussions sur les questions qui précèdent. Pour mieux connaître les pratiques de gestion du risque opérationnel des membres du Comité, elle demande aux membres de répondre par écrit aux questions qui suivent en donnant des précisions sur leurs pratiques respectives.

Votre réponse aux questions est volontaire, mais les renseignements recueillis aideront la Banque et le ministère des Finances à mieux connaître les diverses pratiques en usage dans l'écosystème des paiements de détail et à en tenir compte, si possible, dans la conception du cadre de surveillance. Votre participation est donc grandement appréciée. **Merci d'envoyer vos réponses au plus tard le vendredi 4 septembre.**

La confidentialité des renseignements reçus sera maintenue conformément au cadre de fonctionnement du Comité[1].

Cadre

1) Votre organisation se sert-elle d'indicateurs quantitatifs pour définir ses objectifs de fiabilité et d'efficacité opérationnelles (ex. : délai de reprise visé, point de reprise visé, taux de disponibilité)? Si oui :
   a) Quels sont ces indicateurs?
   b) Des membres ont-ils adopté des indicateurs quantitatifs concernant la préservation de l'intégrité ou de la confidentialité? Si oui, lesquels?
   c) Quelles cibles sont fixées pour chacun des indicateurs?
   d) Quels sont les facteurs pris en compte dans l'établissement de ces cibles?
      i) Quels facteurs externes influent sur les cibles (ex. : autres règlements, obligations d'inscription à un système, objectifs d'autres tiers)?
   e) Ces cibles sont-elles communiquées aux clients ou à d'autres tiers?

Détermination

2) Processus de détermination et d'analyse des sources de risque opérationnel, dont les suivants :
   - Autoévaluation des risques
   - Analyse de l'efficacité du contrôle
   - Analyse des événements de risque internes et externes
   - Analyse de scénarios
   - Modélisation quantitative de l'exposition
   - Veille prospective

---

[1] En d'autres termes, la Banque s'engage à garder confidentiels tous les renseignements qu'elle obtient, sauf s'ils sont du domaine public ou si leur divulgation est exigée par la loi, y compris la *Loi sur l'accès à l'information*, qui énonce les motifs pour lesquels la Banque peut refuser de communiquer l'information de tiers. Si la Banque reçoit une demande d'accès à des informations fournies par un membre, elle consulte ce dernier pour s'assurer d'avoir une bonne compréhension du niveau de sensibilité de l'information. Le membre a alors l'occasion d'expliquer les motifs justifiant le caractère confidentiel des informations demandées.

a) Votre organisation utilise-t-elle l'un ou l'autre de ces processus? Certains manquent-ils de pertinence? Votre organisation a-t-elle recours à d'autres pratiques?
b) À quelle fréquence votre organisation emploie-t-elle ces processus?

Protection

3) Les contrôles de sécurité physique et de sécurité de l'information (y compris la cybersécurité) sont, en termes généraux, les contrôles liés aux éléments suivants : accès aux systèmes et aux données (ex. : principe du droit d'accès minimal, séparation des tâches, contrôle et surveillance des comptes, journaux d'accès); identification et authentification des utilisateurs et des appareils; formations de sensibilisation à la sécurité; analyse, surveillance et tenue de journaux d'audit; rapprochement; protection des supports; sécurité et filtrage de sécurité du personnel; protection automatisée des systèmes et des communications (ex. : contrôle des ports réseau, défense de périmètre, chiffrement); intégrité des systèmes et de l'information (ex. : protection contre les maliciels, surveillance de l'intégrité des logiciels); gestion des vulnérabilités; tests de pénétration; intervention en cas d'incident de sécurité et gestion connexe; accès physique et surveillance; prévention de l'erreur humaine (ex. : principe du double regard); contrôle de l'alimentation électrique, des télécommunications et de l'environnement; protection contre les incendies; processus de gestion des changements; contrôle des accès et gestion des fournisseurs.
   a) Est-ce que certains des contrôles énumérés ne concernent pas votre organisation? Si oui, veuillez expliquer pourquoi.
   b) Y a-t-il des mesures de protection que votre organisation considère comme absolument indispensables?

Détection

4) Quels sont les principaux processus ou contrôles que votre organisation utilise pour détecter d'éventuelles compromissions de l'intégrité de données, de renseignements ou de systèmes?
   a) Quels contrôles utilise-t-elle pour détecter les compromissions de données, de renseignements ou de systèmes qui résultent d'un risque opérationnel physique?
5) Est-ce que votre organisation surveille et consigne les tentatives de cyberattaques?
   a) Si oui, que fait-elle de ces renseignements?
   b) Si non, pourquoi ne le fait-elle pas?
6) Votre organisation participe-t-elle à des réseaux ou à des groupes d'échange sur les cybermenaces? Connaissez-vous des groupes du genre dans le secteur des paiements de détail, que leurs participants soient nombreux ou non?

Intervention et reprise des activités

7) En cas d'incident opérationnel, qu'est-ce qui amènerait votre organisation à mener une enquête poussée? Par exemple, votre organisation a-t-elle fixé d'avance des seuils ou des éléments déclencheurs? Si oui, quels sont-ils?
   a) Sur quoi porte l'enquête?
   b) Arrive-t-il à votre organisation de consulter des experts externes dans le cadre de ses enquêtes?
8) Votre organisation a-t-elle des seuils de transmission des incidents aux échelons supérieurs?
   a) Comment les fixe-t-elle?
   b) Quel est le processus de transmission?

Évaluation et tests

9) À quels genres de tests votre organisation soumet-elle ses mesures de contrôle du risque opérationnel?
    a) De quels facteurs votre organisation tient-elle compte pour déterminer la portée et la profondeur des tests?
    b) À quelle fréquence les tests ont-ils lieu?
    c) Qui les effectue?
10) Votre organisation teste-t-elle son ou ses plans de continuité des opérations?
    a) Les tests simulent-ils des scénarios précis?
    b) Quelles parties prenantes (internes et externes) participent aux tests?
    c) À quelle fréquence les tests ont-ils lieu?
11) Le cadre de gestion du risque opérationnel de votre organisation fait-il l'objet d'audits? Si oui :
    a) Comment l'étendue de ces audits est-elle définie?
    b) À quelle fréquence les audits ont-ils lieu?
    c) Qui les effectue (auditeurs internes ou externes)?

Mandataires

12) Votre organisation fait-elle appel à des mandataires pour fournir des services de paiement? Si oui, veuillez répondre aux questions ci-dessous.
13) Quels sont les principaux risques opérationnels que représentent les mandataires pour votre organisation?
14) Comment votre organisation veille-t-elle à ce que les mandataires gèrent ces risques, le cas échéant? Par exemple :
    a) Soumet-elle les mandataires à des politiques, à des normes ou à des niveaux de service minimaux?
    b) Comment ces parties sont-elles informées des normes en question?
    c) Comment votre organisation s'assure-t-elle que les mandataires honorent leurs obligations?
15) Comment votre organisation s'assure-t-elle que les mandataires (s'il y a lieu) sont capables de détecter et de signaler les problèmes opérationnels?
16) Vos mandataires doivent-ils respecter différentes normes de gestion du risque opérationnel selon le territoire où ils se trouvent?
    a) Si oui, quelles sont les conséquences sur la manière dont votre organisation gère le risque opérationnel associé au recours à des mandataires?

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

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

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

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

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

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

Principes	Concepts susceptibles de figurer dans une loi, un règlement ou une ligne directrice	Exemples d'autres normes pertinentes
qu'après des changements importants[2].	Éléments de la gestion du risque opérationnel qu'il faut évaluer et tester (p. ex., plan de continuité des opérations, contrôles de cybersécurité, autres politiques, tests et évaluations des contrôles de protection et de détection ainsi que mécanismes d'intervention). Méthodes de conception et d'exécution des tests. Fréquence des tests, des audits et des examens : • Si certains processus doivent être testés tous les ans (p. ex., plan de continuité des opérations; possibilité de tester chaque année des parties différentes du plan), d'autres peuvent l'être moins souvent. • Les éléments du cadre de gestion du risque opérationnel peuvent être audités sur une période fixe. • Le cadre de gestion du risque opérationnel doit être examiné tous les ans. Le FSP doit choisir entre procéder lui-même aux tests, audits et examens ou les confier à un tiers.	risques liés aux TIC et à la sécurité
7. Un FSP devrait avoir un plan de continuité des activités qui prend en compte les événements représentant un risque important d'interruption des activités. Le plan devrait être conçu de manière à protéger les renseignements et les données de paiement des utilisateurs finaux et à	Le FSP doit surveiller et détecter les incidents opérationnels. But d'un plan de continuité des opérations : • Servir de plan structuré et clair pour réagir aux éventuels incidents, y compris ceux qui portent lourdement atteinte à la confidentialité, à l'intégrité ou à la disponibilité des activités de paiement de détail du FSP ou des systèmes informatiques, des données ou des renseignements facilitant ses fonctions de paiement.	Principe 17.6 des PIMF Orientations de l'ABE sur la gestion des risques liés aux TIC et à la sécurité

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

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