Ligne directrice

Titre	Gestion du risque opérationnel et résilience opérationnelle – Ligne directrice
Catégorie	Saines pratiques commerciales et financières
Date	22 août 2024
Secteur	Banques Associations coopératives de crédit Succursales de banques étrangères Succursales de sociétés d'assurance étrangères Sociétés d'assurance vie et de secours mutuels Sociétés des assurances multirisques Sociétés de fiducie et de prêts
No	E-21

Table des matières

A. Vue d'ensemble

- A1. Lien entre la gestion du risque opérationnel et la résilience opérationnelle
- A2. Objet
- A3. Portée
- A4. Application
- A5. Définitions
- A6. Résultats et attentes

1. Gouvernance

- 1.1 Haute direction
- 1.2 Secteurs d'activité et fonctions centrales
- 1.3 Supervision indépendante
- 1.4 Assurance indépendante

2. Gestion du risque opérationnel

- 2.1 Cadre de gestion du risque opérationnel
- 2.2 Propension à prendre des risques opérationnels
- 2.3 Outils de gestion du risque opérationnel
- 2.4. Activités de suivi et rapports

3. Résilience opérationnelle

- 3.1 Recensement et cartographie
- 3.2 Établissement des seuils de tolérance aux perturbations
- 3.3 Tests de scénarios

4. Principaux aspects de la gestion du risque opérationnel qui contribuent à la résilience opérationnelle

- 4.1 Gestion du risque lié à la continuité des affaires
- 4.2 Gestion du risque lié à la reprise après sinistre
- 4.3 Gestion de crise
- 4.4 Gestion du changement
- 4.5 Gestion du risque lié aux technologies et du cyberrisque
- 4.6 Gestion du risque lié aux tiers
- 4.7 Gestion du risque lié aux données

A. Vue d'ensemble

Les institutions financières exercent des activités dans un environnement complexe au rythme trépidant, caractérisé par une intensification des risques pesant sur leurs opérations, notamment sur leur personnel, leurs installations et leurs systèmes. Une saine gestion du risque opérationnel et une bonne résilience opérationnelle améliorent leur capacité à prévenir et à déceler les événements défavorables, à y donner suite et à s'en remettre, tout en assurant la continuité de leurs activités essentielles.

A1. Lien entre la gestion du risque opérationnel et la résilience opérationnelle

La gestion du risque opérationnel consiste essentiellement à cerner et à gérer tout risque susceptible d'influencer les activités des institutions financières. Elle a pour objet de réduire dans toute la mesure du possible la fréquence et l'ampleur des perturbations et des pertes imputables au risque opérationnel.

La saine gestion du risque opérationnel est un aspect fondamental de la résilience opérationnelle, car elle renforce la capacité des institutions financières à résister aux perturbations. Pour sa part, la résilience opérationnelle repose sur l'hypothèse selon laquelle des perturbations vont se produire, de sorte qu'elle met l'accent sur les mesures d'intervention à prendre par les institutions financières dans un tel cas, et sur leur rétablissement de ces dernières, selon une approche holistique, c'est-à-dire une approche qui tient compte de la réalisation de bout en bout de leurs activités essentielles.

A2. Objet

Énoncer les attentes en matière de gestion du risque opérationnel et de résilience opérationnelle.

A3. Portée

La présente ligne directrice s'applique à toutes les institutions financières fédérales, y compris les succursales de banques étrangères et les succursales de sociétés d'assurance étrangères, dans la mesure permise par les exigences et les obligations légales applicables aux activités qu'elles exercent au Canada. Les attentes à l'égard des succursales sont énoncées dans la ligne directrice E 4, Entités étrangères exploitant une succursale au Canada.

A4. Application

L'application de la présente ligne directrice est fonction du risque et est proportionnelle à certains facteurs propres à l'institution, c'est-à-dire :

- sa taille;
- sa stratégie;
- son profil de risque;

- la nature, la portée et la complexité de ses activités;
- son interdépendance, soit qu'une perturbation la touchant pourrait être préjudiciable à d'autres institutions financières, au système financier ou à l'économie dans son ensemble.

A5. Définitions

Risque opérationnel

Le risque opérationnel correspond au risque de pertes attribuables au personnel, à une inadéquation ou à une défaillance des processus ou des systèmes, ou à des événements extérieurs.

Résilience opérationnelle

La résilience opérationnelle correspond à la capacité d'une institution financière à mener ses activités, et tout particulièrement ses activités essentielles, en période de perturbation.

Événement générateur de risque opérationnel

Un événement générateur de risque opérationnel s'entend d'un résultat non intentionnel (perte ou gain) découlant d'un risque opérationnel. Cela comprend notamment les quasi-préjudices (lorsque l'institution financière n'a pas enregistré de perte ou de gain à la suite d'un événement).

Activités essentielles

Les activités essentielles englobent les services et les produits d'une institution financière qui, en cas de perturbation, pourraient mettre en péril la continuité des affaires de cette dernière ou sa sûreté et sa solidité, ou encore entraîner un préjudice pour d'autres institutions en raison de l'interdépendance entre l'institution et le système financier.

Équipe de gestion de crise

L'équipe de gestion de crise est généralement un groupe composé de cadres d'une institution financière chargés de prendre des décisions, de coordonner les travaux et d'encadrer l'élaboration et la mise en œuvre de stratégies pour contrer ou atténuer d'éventuelles ou réelles crises susceptibles d'avoir une incidence sur les activités de l'institution, sa réputation ou sa stabilité financière.

Risque lié aux données

Le risque lié aux données s'entend du risque de perte pouvant résulter de la collecte, du stockage, du traitement, de l'utilisation, de la communication ou de l'élimination de données. Ce risque peut être imputable au personnel, à des processus et systèmes inadéquats, ou à des événements extérieurs qui touchent les données.

Test de scénarios

L'expression « test de scénarios » s'entend au sens de la ligne directrice E-18, Simulation de crise. Dans une perspective de résilience opérationnelle, le test de scénarios sert à évaluer la capacité d'une institution à poursuivre ses activités tout en respectant certains niveaux de tolérance aux perturbations, selon divers scénarios graves, mais vraisemblables.

Tolérance aux perturbations

La tolérance aux perturbations correspond au niveau maximal de perturbations découlant d'un événement générateur de risque opérationnel qu'une institution financière est en mesure d'assumer tout en maintenant ses activités essentielles dans le cadre de divers scénarios graves, mais vraisemblables. Cela peut inclure par exemple la durée d'une panne, la réduction des services, la perte de données ou l'ampleur des répercussions sur les clients.

Basculement

On parle de basculement pour désigner la capacité de basculer automatiquement vers un système technologique auxiliaire lorsque le système principal connaît une défaillance.

Entente avec les tiers

Une entente avec les tiers s'entend au sens de la ligne directrice B-10, Gestion du risque lié aux tiers.

A6. Résultats et attentes

1. Les pratiques de gestion du risque opérationnel soutiennent la résilience opérationnelle.
2. Le risque opérationnel est géré en concordance avec la propension à prendre des risques ainsi qu'avec les limites de risque approuvées par l'institution.
3. Les activités essentielles se poursuivent pendant les périodes de perturbations.

Résultat 1 : Les pratiques de gestion du risque opérationnel soutiennent la résilience opérationnelle.

1. Gouvernance

Principe 1 : L'institution dispose d'un cadre de gestion du risque opérationnel et d'une approche de résilience opérationnelle qui sont dûment régis, documentés et mis en œuvre.

1.1 Haute direction

La haute direction est ultimement imputable de l'élaboration, de la mise en œuvre et de la surveillance d'un cadre de gestion du risque opérationnel et d'une approche de résilience opérationnelle efficaces.

Elle est investie des responsabilités suivantes :

- Veiller à ce que des programmes axés sur la gestion du risque opérationnel et sur la résilience opérationnelle soient établis.
- Veiller à ce que des tests et des analyses reposant sur des scénarios soient menés sur une base continue au niveau des secteurs d'activité et, s'il y a lieu, à l'échelle de l'entité.
- Définir clairement les rôles et les responsabilités, et affecter des ressources adéquates.
- Communiquer des renseignements à jour et exacts au conseil d'administration.
- S'assurer que les lacunes opérationnelles font rapidement l'objet d'une évaluation et de mesures correctrices adéquates et durables.
- Veiller à ce que tout dépassement des seuils de tolérance aux perturbations soit signalé aux échelons supérieurs et fasse l'objet de mesures adéquates.
- Promouvoir et favoriser l'adoption d'une culture et de comportements qui appuient la gestion du risque opérationnel et la résilience opérationnelle.
- Outiller les fonctions de gestion du risque et de conformité afin qu'elles puissent procéder à une remise en question des pratiques et des décisions sans avoir à craindre de représailles.

Consulter la ligne directrice Gouvernance d'entreprise pour prendre connaissance des attentes à l'endroit des conseils d'administration au chapitre des plans d'affaires, des stratégies, de la propension à prendre des risques et de la culture de risque ainsi que de la supervision de la haute direction et des contrôles internes.

1.2 Secteurs d'activité et fonctions centrales

Les secteurs d'activité et les fonctions centrales sont imputables de la gestion du risque opérationnel et doivent contribuer à la résilience opérationnelle. Leurs activités doivent faire l'objet d'une analyse critique indépendante, efficace et dûment étayée.

Elles sont investies des responsabilités suivantes :

- Se conformer au cadre de gestion du risque opérationnel et à l'approche de résilience opérationnelle de l'institution financière, de pair avec les politiques et procédures connexes.
- Cerner et évaluer tout élément de risque opérationnel, et s'assurer de disposer de contrôles efficaces en tirant parti des outils appropriés.
- Gérer le risque opérationnel conformément au cadre de gestion de la propension à prendre des risques et à l'approche en matière de résilience opérationnelle de l'institution.
- Signaler les événements générateurs de risque opérationnel aux échelons supérieurs selon les modalités appropriées.
- Recenser les activités essentielles et leur attribuer des seuils de tolérance aux perturbations (voir sections 3.1 et 3.2).
- Gérer les risques auxquels peuvent être exposées les activités essentielles, en concordance avec les seuils de tolérance aux perturbations établis.
- Offrir une formation adéquate au personnel en matière de gestion du risque opérationnel et de résilience opérationnelle.

1.3 Supervision indépendante

Les fonctions indépendantes responsables du risque et de la conformité encadrent les activités des secteurs d'activité et des fonctions centrales ayant trait au risque et à la résilience et en fournissent une analyse critique. Elles accomplissent, entre autres, les tâches suivantes :

- Établir le cadre de gestion du risque opérationnel et l'approche de résilience opérationnelle, et surveiller la conformité à ce cadre et à cette approche.
- Réviser les plans d'action établis pour corriger les lacunes cernées.
- S'assurer que des outils d'évaluation et de reddition de comptes appropriés sont élaborés et font l'objet d'un suivi.
- Veiller à ce que les décisions, les mesures et les évaluations soient dûment documentées.
- Veiller à ce que des voies appropriées de signalement aux échelons supérieurs soient établies et que les problèmes importants soient résolus.

1.4 Assurance indépendante

La fonction d'audit interne ou une fonction similaire doit fournir une assurance indépendante à la haute direction et au conseil d'administration concernant l'utilité conceptuelle et l'efficacité des contrôles, des politiques, des procédures et des systèmes destinés à la gestion du risque opérationnel.

Résultat 2 : Le risque opérationnel est géré en concordance avec la propension à prendre des risques et avec les limites de risque approuvées par l'institution.

2. Gestion du risque opérationnel

La gestion efficace du risque opérationnel est essentielle à la résilience opérationnelle.

Principe 2 : L'institution dispose d'un cadre de gestion du risque opérationnel efficace déployé à l'échelle de l'institution.

2.1 Cadre de gestion du risque opérationnel

Un cadre de gestion du risque opérationnel efficace comporte les éléments suivants :

- un énoncé de la propension à prendre des risques opérationnels dûment approuvé et assorti de limites de risque opérationnel;
- des politiques et des procédures faisant l'objet d'examens et de mises à jour périodiques;
- une taxonomie des risques qui comporte des catégories de risques se rapportant au personnel, à une inadéquation ou à une défaillance des processus ou des systèmes, ou à des événements extérieurs;
- des outils d'évaluation et de surveillance des risques et des contrôles.

Principe 3 : L'institution doit établir sa propension à prendre des risques opérationnels, puis s'y conformer.

2.2 Propension à prendre des risques opérationnels

L'énoncé de la propension à prendre des risques opérationnels doit être intégré au cadre de gestion de la propension à prendre des risques, comme il est indiqué dans la ligne directrice Gouvernance d'entreprise du BSIF.

Consulter la ligne directrice Gouvernance d'entreprise pour prendre connaissance des attentes relatives à l'énoncé de la propension à prendre des risques.

L'énoncé de la propension à prendre des risques opérationnels établit les catégories de risque opérationnel et l'ampleur de ces risques que l'institution financière est prête à accepter afin d'atteindre ses objectifs opérationnels. L'énoncé de la propension à prendre des risques opérationnels doit :

- comporter des paramètres de mesure d'ordre qualitatif et quantitatif;
- être prospectif (c'est-à-dire prévoir les risques éventuels);
- établir explicitement les limites de risque.

Les limites de risque opérationnel doivent normalement être inférieures aux seuils de tolérance aux perturbations (voir section 3.2).

Les cadres, les politiques et les procédures doivent mentionner les situations où l'institution dépasse ou est près de dépasser ses seuils de propension à prendre des risques, que ces situations soient attribuables à l'évolution des risques, à des événements particuliers, à des transactions proposées, à des modifications du modèle d'affaires ou à d'autres raisons. Dans de tels cas, une décision sera requise : accepter, éviter ou atténuer le risque, ou réévaluer la propension à prendre des risques et les limites de risque.

Les réévaluations périodiques de la propension à prendre des risques opérationnels et des limites de risque opérationnel doivent porter notamment sur les points suivants :

- les changements relatifs à l'environnement externe, aux volumes d'affaires ou aux activités;
- la qualité de l'environnement de contrôle;
- l'efficacité des stratégies d'atténuation du risque;
- les événements générateurs de risque opérationnel qu'a connus l'institution;
- la fréquence, l'ampleur ou la nature des dépassements des seuils de propension à prendre des risques.

Principe 4 : L'institution doit bien cerner et évaluer les risques opérationnels au moyen de méthodes et d'outils adéquats.

2.3 Outils de gestion du risque opérationnel

Les risques opérationnels doivent faire l'objet d'analyses périodiques dans le but de s'assurer qu'ils demeurent en deçà du seuil de propension à prendre des risques opérationnels, et qu'ils sont bien recensés et gérés. À cette fin, l'institution doit utiliser des outils appropriés, par exemple :

- des évaluations du risque et des contrôles;
- des indicateurs de risque clés;
- des analyses des données sur les événements générateurs de risque opérationnel;
- des analyses de scénarios.

2.3.1 Évaluations du risque et des contrôles

L'institution doit utiliser un outil d'autoévaluation, tel que l'évaluation du risque et des contrôles, pour exécuter les tâches suivantes :

- recenser les risques opérationnels inhérents;
- recenser et évaluer les contrôles connexes afin de déterminer le risque opérationnel résiduel.

Le recours à une autoévaluation du risque et des contrôles ou à un outil similaire sert à déterminer si le risque résiduel se situe à l'intérieur des limites de risque opérationnel établies. Si le risque résiduel excède ces limites, l'institution financière doit élaborer et mettre en œuvre des plans d'action prévoyant les mesures suivantes :

- réévaluation de l'adéquation des limites de risque opérationnel;
- prise d'autres mesures pour atténuer le risque opérationnel dans toute la mesure du possible;
- acceptation explicite de la portion du risque opérationnel qui excède les limites établies.

Le risque opérationnel résiduel doit faire l'objet de réévaluations périodiques, par exemple lors d'un changement important (voir section 4.4) ou à la suite d'un événement générateur de risque opérationnel important.

2.3.2 Indicateurs de risque clés

Les indicateurs de risque clés sont des outils servant à évaluer et à surveiller les principaux facteurs de risque opérationnel, et à déterminer si l'institution financière réalise ses activités en respectant ses limites de risque opérationnel. De tels indicateurs peuvent être établis à la lumière des résultats des évaluations du risque et des contrôles (voir section 2.3.1), des événements générateurs de risque opérationnel (voir section 2.3.3) ou d'autres sources d'information. Les indicateurs de risque clés doivent se situer à différents niveaux de l'institution, notamment au niveau des secteurs d'activités et de l'institution dans son ensemble.

Les indicateurs de risque clés peuvent être aussi bien avancés (en amont) que retardés (en aval). Les indicateurs avancés servent à discerner les expositions à des risques ainsi que les risques émergents. Les indicateurs retardés permettent de mieux repérer les lacunes dans les contrôles. Tous ces indicateurs doivent être assortis de protocoles de signalement aux échelons supérieurs lorsque le risque est en voie d'atteindre – ou a déjà dépassé –

les seuils établis. Ces signalements doivent donner lieu à la prise de mesures d'atténuation du risque par la direction.

2.3.3 Données sur les événements générateurs de risque opérationnel

Lorsqu'un événement générateur de risque opérationnel entraîne un dépassement des seuils établis, les données sur cet événement doivent être consignées afin de répondre aux questions suivantes :

- Quelle est la cause première de l'événement générateur de risque opérationnel?
- Est-ce que l'événement générateur de risque opérationnel est réel, potentiel ou un quasi-préjudice?
- Quelles sont les expositions sous-jacentes à la catégorie de risque opérationnel ayant contribué à l'événement?
- Quelles mesures convient-il de prendre pour corriger les lacunes ou les défaillances des contrôles?

2.3.4 Analyses de scénarios

Les analyses de scénarios ont pour but de cerner d'éventuels événements générateurs de risque opérationnel, de mesurer leurs répercussions possibles, de repérer les lacunes dans les contrôles et d'étayer l'élaboration de mesures d'atténuation. Ces analyses sont axées sur les sources de risque opérationnel et sur l'exposition à ce risque. Elles doivent reposer sur des techniques adéquates et être menées, à la fois, au niveau des secteurs d'activité et de l'institution dans son ensemble. De plus, elles doivent tenir compte d'un ensemble de scénarios graves, mais vraisemblables.

Les analyses de scénarios doivent constituer un processus itératif qui se perfectionnera constamment au fil du temps. Dans le cadre de la préparation des prochaines analyses de scénarios, l'institution doit tenir compte des résultats des analyses précédentes, des événements passés (internes et externes) ainsi que des quasi-préjudices.

Les résultats des analyses de scénarios peuvent être utiles dans le cadre des tests de scénarios axés sur la résilience opérationnelle (voir section 3.3).

Principe 5 : L'institution doit continuellement suivre le risque opérationnel et en rendre compte en vue de repérer les lacunes dans les contrôles ainsi que les possibles dépassements des seuils de propension à prendre des risques et des limites de risque.

2.4. Activités de suivi et rapports

2.4.1 Activités de suivi

L'institution doit mener des activités de suivi sur une base continue pour mieux se préparer aux éventuels changements touchant le risque opérationnel et être plus à même d'agir s'ils se matérialisent. Les activités de suivi doivent notamment porter sur le respect de l'énoncé de la propension à prendre des risques opérationnels, des limites de risque et des seuils de tolérance aux perturbations (voir section 3.2). Elles doivent être fondées sur le risque, de sorte que les activités comportant un risque élevé fassent l'objet d'une surveillance resserrée.

Les travaux de suivi doivent faire appel à un ensemble complet de paramètres de mesure. L'institution peut aussi utiliser des outils de gestion du risque opérationnel pour appuyer les activités de suivi du risque et déterminer au besoin les mesures correctrices.

2.4.2 Reddition de compte et signalement aux échelons supérieurs

Les mécanismes de reddition de compte et de signalement aux échelons supérieurs doivent faire en sorte que la haute direction et le conseil d'administration disposent de rapports en temps opportun, et qu'ils soient tenus informés de tout point important révélé par les outils de gestion du risque opérationnel voir (section 2.3), notamment dans les situations suivantes :

- des lacunes et des problèmes importants sont relevés;
- les limites de risque sont presque atteintes ou sont dépassées;
- les risques résiduels sont expressément acceptés.

Les rapports doivent comprendre une évaluation agrégée du profil de risque, basée sur des données actuelles et prospectives, et inclure des mesures correctrices s'il y a lieu.

L'institution doit aussi présenter à la haute direction et au conseil d'administration les résultats des analyses de scénarios (voir section 2.3.4) et des tests de scénarios (voir section 3.3). L'information ainsi fournie doit comprendre les éléments suivants :

- l'analyse des lacunes;
- l'évaluation de la résilience opérationnelle, notamment la question de savoir si les activités essentielles peuvent être maintenues tout en respectant les seuils de tolérance aux perturbations établis (voir section 3.2);
- des plans de mesures correctrices.

Résultat 3 : Les activités essentielles sont maintenues pendant une période de perturbations.

3. Résilience opérationnelle

La résilience opérationnelle exige une bonne connaissance des activités essentielles et du processus d'exécution de ces activités de bout en bout, à l'intérieur des seuils de tolérance aux perturbations, dans des circonstances graves, mais vraisemblables.

Bien qu'il soit de mise d'accorder au départ la priorité aux activités essentielles, l'approche en matière de résilience opérationnelle, à mesure qu'elle gagne en maturité, devrait s'étendre à d'autres activités susceptibles d'avoir des répercussions importantes sur l'institution financière.

Principe 6 : L'institution doit recenser et évaluer ses activités essentielles et cartographier les interdépendances internes et externes.

3.1 Recensement et cartographie

L'institution doit recenser ses activités essentielles, puis évaluer sa capacité à les maintenir en cas de perturbations. Elle doit ensuite réexaminer et mettre à jour périodiquement ces évaluations, notamment les estimations relatives aux pertes financières directes et indirectes pouvant découler des perturbations.

Après avoir recensé ses activités essentielles, l'institution doit cartographier ces activités pour faire ressortir les interdépendances internes et externes.

La cartographie doit :

- tenir compte des activités essentielles de bout en bout;
- refléter le personnel, les technologies, les processus, les renseignements, les installations et les tiers, de même que leurs interdépendances ou les liens entre eux;
- être axée sur les mesures requises afin de pouvoir exercer les activités essentielles;
- révéler les vulnérabilités, ce qui pourra être utile dans le cadre des tests de scénarios axés sur la résilience opérationnelle (voir section 3.3).

Lorsqu'une institution établit qu'un tiers remplit un rôle essentiel, elle doit obtenir suffisamment d'information afin de pouvoir évaluer sa résilience.

Principe 7 : Des seuils de tolérance sont établis pour les perturbations aux activités essentielles.

3.2 Établissement des seuils de tolérance aux perturbations

Un seuil de tolérance aux perturbations correspond au niveau maximal de perturbations découlant d'un événement générateur de risque opérationnel qu'une institution financière est en mesure d'assumer tout en maintenant ses activités essentielles dans le cadre de divers scénarios graves, mais vraisemblables

Les seuils de tolérance aux perturbations diffèrent de la propension à prendre des risques et sont généralement supérieurs à cette dernière. En effet, la propension à prendre des risques reflète le niveau de risque qu'une

institution est prête à assumer pour atteindre ses objectifs d'affaires, tandis que la tolérance aux perturbations correspond au niveau maximal de perturbations qu'une institution peut tolérer lors d'une crise.

Les seuils de tolérance aux perturbations doivent tenir compte des répercussions que d'éventuelles perturbations pourraient avoir sur les éléments suivants :

- les autres activités essentielles de l'institution financière qui font appel aux mêmes ressources;
- les systèmes, les installations et les fournisseurs tiers dont dépendent les activités essentielles;
- les autres institutions financières, le système financier et l'économie dans son ensemble.

Lorsqu'une institution financière fixe un seuil de tolérance aux perturbations, elle doit garder à l'esprit que le volume ou l'exécution des activités essentielles peut varier selon le moment de la journée et selon la période de l'année.

Consulter la ligne directrice B-10, Gestion du risque lié aux tiers, pour prendre connaissance des attentes en matière de risque lié aux tiers.

Principe 8 : Les tests de scénarios doivent servir à évaluer périodiquement la capacité de l'institution à maintenir ses activités essentielles, à l'intérieur des seuils de tolérance aux perturbations établis, dans l'éventualité de perturbations graves, mais vraisemblables.

3.3 Tests de scénarios

La réalisation périodique de tests de scénarios aide à mieux comprendre les circonstances où les seuils de tolérance aux perturbations seraient dépassés (voir section 3.2). Ces tests vont au-delà de l'analyse de scénarios de risque opérationnel, qui servent à déterminer les potentiels événements générateurs de risque opérationnel, leurs répercussions ainsi que les contrôles et les mesures d'atténuation connexes (voir section 2.3.4).

L'institution doit tester un ensemble de scénarios graves, mais vraisemblables, y compris des scénarios qui se déroulent simultanément et d'autres qui portent sur une période plus longue. Voici des exemples de scénarios possibles :

- pannes de courant;
- défaillances technologiques de grande ampleur;
- perturbations touchant des services essentiels de tiers;
- cyberincidents;
- catastrophes naturelles;
- pandémies.

Les tests de scénarios reposent généralement sur une approche de bout en bout afin de déterminer l'ensemble des répercussions sur de multiples secteurs d'activité. Ils tiennent aussi compte des interdépendances internes et externes. En fonction du degré de criticité, différentes méthodologies de tests doivent être utilisées, par exemple des exercices de table, des simulations et des tests de systèmes en situation réelle.

Les secteurs d'activité, les fonctions centrales, les fonctions de gestion du risque et de conformité ainsi que la fonction d'audit interne ou une fonction similaire peuvent formuler des recommandations utiles et collaborer à la conception et aux tests des scénarios.

Le cas échéant, l'institution financière devrait aussi mener des exercices de plus vaste portée en coordination avec des tiers essentiels.

La fréquence et l'intensité des tests doivent être proportionnelles à la criticité des activités et au niveau de risque auquel elles sont exposées. Lorsque l'environnement de risque connaît des changements importants, les tests devraient être menés plus fréquemment, y compris en dehors du cycle régulier.

Le test de scénarios est un processus itératif qui devrait parvenir à maturité et se perfectionner au fil du temps. Les résultats des tests passés serviront à élaborer les tests à venir.

4. Principaux aspects de la gestion du risque opérationnel qui contribuent à la résilience opérationnelle

Voici différents aspects clés rattachés à la gestion du risque opérationnel qui servent à renforcer la résilience opérationnelle :

- la gestion du risque lié à la continuité des affaires;
- la gestion du risque lié à la reprise après sinistre;
- la gestion de crise;
- la gestion du changement;
- la gestion du risque lié aux technologies et du cyberrisque;
- la gestion du risque lié aux tiers;
- la gestion du risque lié aux données.

Il convient de préciser que cette liste n'est pas exhaustive. Au fil de l'évolution de l'environnement de risque, d'autres domaines de risque pourraient apparaître ou venir à occuper une place plus importante dans une optique de résilience opérationnelle.

Le respect des attentes exposées dans la suite de la présente ligne directrice aidera à atteindre les résultats énoncés aux points 1 à 3 ci-devant.

4.1 Gestion du risque lié à la continuité des affaires

La gestion du risque lié à la continuité des affaires est un processus qui consiste, d'une part, à établir des plans dans l'éventualité d'une perturbation touchant les activités, et d'autre part, à assurer le rétablissement à la suite d'une telle perturbation. Elle doit faire partie intégrante de la résilience opérationnelle et renforcer cette dernière. Elle devrait également en venir, avec le temps, à passer des processus opérationnels aux activités essentielles considérées de bout en bout.

La gestion du risque lié à la continuité des affaires doit comprendre :

- la réalisation d'analyses des répercussions sur les activités;
- l'élaboration et le test des plans de continuité des affaires.

4.1.1 Analyse des répercussions sur les activités

L'analyse des répercussions sur les activités sert à évaluer les risques et les répercussions possibles de différents événements perturbateurs sur les activités. L'analyse doit cerner et mesurer :

- les répercussions des perturbations;
- les limites maximales associées aux objectifs de rétablissement avant que ne surviennent des conséquences graves.

Les analyses des répercussions sur les activités doivent faire l'objet d'examens périodiques et être mises à jour lorsque cela est requis.

4.1.2 Plans de continuité des affaires

Les plans de continuité des affaires énoncent les interventions et les mesures de rétablissement prévues relativement à tout un éventail de perturbations. Ces plans ont pour objet de composer avec des perturbations touchant les personnes et les actifs corporels afin qu'ils puissent rapidement être opérationnels en cas de sinistre.

Un plan de continuité des affaires doit comprendre les éléments suivants :

- les protocoles à suivre pour activer le plan et prendre des décisions;
- la définition des rôles et des responsabilités entourant la gestion des perturbations;
- la désignation du personnel suppléant pour couvrir les absences non prévues;
- la mise en œuvre de mesures pour assurer la sécurité du personnel;
- l'établissement de cibles concernant le degré de rétablissement et les délais connexes;
- des analyses des répercussions sur les activités, des solutions de rechange et des stratégies de rétablissement;
- des plans de communication interne et de communication externe.

L'institution doit offrir au personnel une formation sur les plans de continuité des affaires, notamment l'activation de ces plans et la manière dont les activités seront menées durant la période de perturbations.

4.1.3 Tests du plan de continuité des affaires

Les tests portant sur les plans de continuité des affaires doivent fournir une assurance raisonnable que ces plans sont efficaces. Ils doivent permettre aux membres de la haute direction et au personnel de mieux comprendre leurs rôles et leurs responsabilités à l'égard du plan de continuité des affaires, et de savoir comment elles seront menées durant la période de perturbations.

Les tests doivent englober un ensemble de circonstances graves, mais vraisemblables, et notamment des scénarios où les perturbations :

- durent longtemps;
- surviennent simultanément, de par leur nature;
- touchent des tiers essentiels.

La fréquence des tests et le type de tests doivent être déterminés en fonction des résultats des analyses des répercussions sur les activités et doivent concorder avec la propension à prendre des risques opérationnels. Les tiers essentiels devraient eux aussi démontrer qu'ils ont des pratiques robustes quant à leurs plans de continuité des affaires et des tests de ces derniers. L'institution doit prévoir des processus pour corriger les lacunes révélées par les tests, de même que des plans d'urgence concernant les tiers essentiels.

Les tests des plans de continuité des affaires serviront aussi à renforcer les tests de scénarios et à obtenir une véritable vue d'ensemble, de bout en bout, des activités essentielles à l'échelle de l'institution (voir section 3.3).

> Consulter la ligne directrice B-10, Gestion du risque lié aux tiers, pour prendre connaissance des attentes en matière de risque lié aux tiers.

4.2 Gestion du risque lié à la reprise après sinistre

La gestion du risque lié à la reprise après sinistre aide à se préparer à d'éventuels événements générateurs de risque graves, mais vraisemblables découlant de la mise hors service d'infrastructures technologiques (par exemple des réseaux ou des serveurs de données). Le plan de reprise après sinistre doit préciser les rôles et les responsabilités des employés ainsi que les protocoles d'activation du plan.

Des plans de basculement et des plans de secours doivent être élaborés et testés à l'égard des actifs technologiques qui appuient l'exécution des activités essentielles.

> Consulter la ligne directrice B-13, Gestion du risque lié aux technologies et du cyberrisque, pour prendre connaissance des attentes en matière de reprise après sinistre.

4.3 Gestion de crise

Des modalités de gestion de crise efficaces aident à préserver la sécurité du personnel, à limiter les perturbations, à mener rapidement des interventions coordonnées et à maintenir la confiance du public dans l'institution financière. Une équipe de gestion de crise peut être utile pour maintenir des communications efficaces, accélérer le rétablissement et intervenir efficacement afin de surmonter la crise.

L'institution doit établir un plan de gestion de crise pour pouvoir assurer une intervention coordonnée et rapide en cas de crise attribuable à des facteurs internes ou externes. Ce plan doit comporter les éléments suivants :

- des protocoles de signalement de la situation à la haute direction et au conseil d'administration;
- les critères devant être réunis pour que le plan soit activé;
- des protocoles de communication interne et de communication externe afin de transmettre en temps opportun l'information pertinente aux parties prenantes.

Des analyses rétrospectives doivent être menées à la suite d'une crise pour en tirer des leçons et pour intégrer ces dernières au plan de gestion de crise. De plus, ce plan doit faire l'objet de tests périodiques et être communiqué

aux secteurs d'activité concernés de l'institution ainsi qu'à toute partie externe touchée.

4.4 Gestion du changement

Le changement peut engendrer des risques opérationnels. Voici quelques exemples de changements importants :

- l'offre de nouveaux produits ou services;
- les acquisitions et les dessaisissements;
- la pénétration de nouveaux marchés;
- la mise en service de nouveaux systèmes technologiques;
- l'apport de modifications importantes aux processus opérationnels.

Les changements importants doivent faire l'objet de processus complets de gestion du changement, et les risques opérationnels doivent être évalués et suivis. Les processus utilisés doivent à la fois régir le risque opérationnel découlant du changement et assurer la gestion efficace du changement proprement dit.

Les processus de gestion du changement doivent être efficaces et concorder avec les attentes générales associées à la gestion du risque opérationnel, attentes qui sont énoncées à la section 2 de la présente ligne directrice.

De plus, l'institution financière doit prendre les mesures suivantes :

- assurer une saine gestion du projet tout au long de son cycle de vie;
- réévaluer la propension à prendre des risques opérationnels et apporter les modifications qui pourraient s'avérer nécessaires en raison du changement;
- mettre en œuvre des plans d'urgence ayant fait préalablement l'objet de tests, dans l'éventualité où le changement est un échec;
- tester le changement au niveau des systèmes et des processus avant son déploiement officiel;
- définir des paramètres de mesure pour évaluer l'efficacité du changement, postérieurement à sa mise en œuvre.

4.5 Gestion du risque lié aux technologies et du cyberrisque

Une défaillance technologique grave, un piratage ou la perte de données sont autant de situations qui peuvent entraîner des perturbations de grande ampleur qui toucheront les activités. Une saine gestion du risque lié aux technologies et du cyberrisque est essentielle pour renforcer la résilience opérationnelle.

Consulter la ligne directrice B-13, Gestion du risque lié aux technologies et du cyberrisque, pour prendre connaissance des attentes relatives au risque lié aux technologies et au cyberrisque.

4.6 Gestion du risque lié aux tiers

Les ententes critiques avec des tiers peuvent miner la résilience opérationnelle d'une institution, par exemple en cas de perturbations touchant les activités des tiers ou à la suite de la perte ou de la corruption de données critiques. Une gestion efficace du risque lié aux tiers constitue dès lors l'un des aspects qui appuient grandement la résilience opérationnelle.

Consulter la ligne directrice B-10, Ligne directrice sur la gestion du risque lié aux tiers, pour prendre connaissance des attentes en matière de risque lié aux tiers.

4.7 Gestion du risque lié aux données

Dans un monde interconnecté et axé sur les données, une gestion efficace du risque lié aux données constitue un volet important de la gestion du risque opérationnel et joue un rôle clé à l'appui de la résilience opérationnelle. Des données indisponibles, de piètre qualité ou divulguées dans le cadre d'une fuite peuvent faire entrave à la prise de décisions, perturber les activités essentielles, entacher la réputation de l'institution et avoir des répercussions sur d'autres institutions financières, sur le système financier et sur l'économie dans son ensemble.

Cela est particulièrement vrai dans le cas des données :

- qui sont rattachées aux activités essentielles;
- qui sont requises pour la prise de décisions;
- qui sont des renseignements personnels;
- qui sont des renseignements exclusifs.

Une gestion efficace du risque lié aux données permet de s'assurer que l'institution dispose de données exactes, complètes, actuelles, sûres et protégées. En outre, la gestion du risque lié aux données doit concorder avec les attentes générales en matière de gestion du risque opérationnel qui sont énoncées à la section 2 de la présente ligne directrice. Elle doit comporter notamment un cadre de gestion du risque lié aux données, incluant une stratégie et un programme de gestion de ce risque.

Le programme de gestion du risque lié aux données doit comprendre les éléments suivants :

- des modalités de gouvernance des données appropriées, assorties de rôles et de responsabilités clairement définis;
- une architecture de données et une infrastructure de technologies de l'information qui appuient la collecte, l'agrégation et la traçabilité des données essentielles ainsi que la reddition de comptes connexe, et ce, à l'échelle de l'institution;
- des processus de classification, d'agrégation et de protection des données;
- des méthodologies servant à garantir l'intégrité, l'adaptabilité, la confidentialité et la disponibilité des données tout au long de leur cycle de vie;
- des processus de signalement aux échelons supérieurs et des procédures d'intervention en cas de fuites de données et d'autres incidents liés aux données;
- des programmes de formation à l'intention des personnes responsables de la gestion et de la surveillance des données.

Consulter la ligne directrice B-13, Gestion du risque lié aux technologies et du cyberrisque, pour prendre connaissance des attentes ayant trait à la classification de l'information et à la protection des données.