Ligne directrice - version provisoire ou à l'étude

Titre	Résilience opérationnelle et gestion du risque opérationnel - Ligne directrice - version provisoire ou à l'étude (2023)
Catégorie	Saines pratiques commerciales et financières
Date	31 octobre 2023
Secteur	Banques Succursales de banques étrangères Sociétés d'assurance vie et de secours mutuels Sociétés des assurances multirisques Sociétés de fiducie et de prêts
Numéro	E-21

Table des matières

État de la consultation : Fermé

A. Vue d'ensemble

- A1. Lien entre gestion du risque opérationnel et résilience opérationnelle
- A2. Objet et portée
- A3. Application et principe de proportionnalité
- A4. Définitions
- A5. Résultats attendus
- A6. Consignes connexes

1. Gouvernance

- 1.1 La haute direction est responsable de la résilience opérationnelle et de la gestion du risque opérationnel
- 1.2 La résilience opérationnelle et la gestion du risque opérationnel sont intégrées au programme et aux rapports de gestion du risque d'entreprise de l'IFF

- 1.3 Les secteurs d’activité et les fonctions centrales gèrent le risque et font l’objet d’une supervision indépendante

2. Résilience opérationnelle

- 2.1 Recenser les activités essentielles et établir des correspondances
- 2.2 Établissement de niveaux de tolérance aux perturbations des activités essentielles
- 2.3 Mise à l’essai et analyse de scénarios
- 2.4 Renforcement continu de la résilience opérationnelle

3. Gestion du risque opérationnel

- 3.1 Cadre de gestion du risque opérationnel
- 3.2 Propension à prendre des risques opérationnels
- 3.3 Pratiques de gestion du risque opérationnel

4. Domaines liés à la gestion du risque opérationnel qui renforcent la résilience opérationnelle

- 4.1 Gestion de la continuité des activités
- 4.2 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

État de la consultation : Fermé

La période de consultation a pris fin le 5 février 2024. Cette version à l’étude de la ligne directrice sera conservée sur notre site Web jusqu’à la publication de la version finale.

A. Vue d’ensemble

Les institutions financières fédérales (IFF) évoluent dans un environnement de risque complexe et caractérisé par des menaces de plus en plus importantes sur leurs activités essentielles, menaces qui peuvent notamment découler de défaillances des mesures de contrôle, de perturbations des activités de tiers, de pannes des infrastructures, de défaillances technologiques, de cyberincidents, d’incidents géopolitiques, de pandémies ou de catastrophes naturelles. En adoptant une approche rigoureuse et concertée à l’égard de la résilience opérationnelle, l’IFF peut améliorer sa capacité à résister à de tels événements, à s’y adapter et à s’en remettre tout en continuant à exercer ses activités essentielles.

Une IFF peut assurer sa résilience opérationnelle en :

- recensant ses activités essentielles et en établissant des correspondances entre les dépendances internes et externes (p. ex., personnes, systèmes, processus, tiers, installations) nécessaires au soutien de ces activités;
- établissant des niveaux de tolérance aux perturbations à l’égard de ses activités essentielles;
- effectuant des mises à l’essai de scénarios pour évaluer sa capacité à respecter les niveaux de tolérance aux perturbations selon divers scénarios graves, mais vraisemblables;
- instaurant une culture de promotion et de renforcement des comportements qui favorisent la résilience opérationnelle, et en gérant en amont les risques liés à la culture et aux comportements qui peuvent influer sur la résilience.

A1. Lien entre gestion du risque opérationnel et résilience opérationnelle

Une gestion efficace du risque opérationnel passe par le recensement, l’évaluation, le suivi et le signalement des risques opérationnels, et par la mise en place de mesures adaptées en réponse à ces risques. La résilience opérationnelle, quant à elle, repose sur une gestion efficace du risque opérationnel, qui doit idéalement englober des domaines comme la gestion du risque lié aux technologies et du cyberrisque, la gestion du risque lié aux tiers et la gestion de la continuité des activités et, s’il y a lieu, tirer parti des cadres existants en matière de gestion du risque et de gouvernance.

La résilience opérationnelle met l'accent sur l'exécution des activités essentielles de l'IFF de bout en bout, à l'échelle de l'organisation. Par conséquent, à mesure que l'approche de l'IFF à l'égard de la résilience opérationnelle arrive à maturité, la gestion du risque opérationnel qui la sous tend doit passer d'une démarche axée sur les unités opérationnelles à une démarche axée sur l'exécution des activités de bout en bout.

Les organisations résilientes sur le plan opérationnel comprennent que des perturbations peuvent survenir, et qu'elles sont inévitables. Elles réagissent à ces événements perturbateurs, s'y adaptent, s'en remettent et en tirent des leçons.

A2. Objet et portée

La présente ligne directrice énonce les attentes du BSIF en matière de résilience opérationnelle et de gestion du risque opérationnel. Elle s'applique à toutes les IFF, y compris les succursales de banques étrangères et les succursales de sociétés d'assurance étrangères, dans la mesure où il est question de leur capacité à respecter les exigences et les obligations juridiques qui leur sont applicables[1]. Les attentes du BSIF à l'égard des succursales sont énoncées dans la ligne directrice E 4, Entités étrangères exploitant une succursale au Canada.

A3. Application et principe de proportionnalité

Les attentes du BSIF en matière de résilience opérationnelle et de gestion du risque opérationnel sont exprimées sous forme de principes et conçues pour être appliquées de manière proportionnelle, en fonction, par exemple, de l'interrelation d'une IFF avec le système financier.

De fait, les IFF de plus grande taille et plus complexes, notamment celles que le BSIF a désignées comme étant d'importance systémique, exercent souvent des activités dont la perturbation pourrait être préjudiciable à d'autres institutions financières, au système financier ou à l'économie dans son ensemble.

Les IFF de plus petite taille et monogammes, quant à elles, comptent habituellement moins de services, de produits ou de fonctions dont la perturbation menacerait la poursuite de leurs activités. Toutefois, certaines petites institutions offrent des produits spécifiques ou assurent des services ou des fonctions dont l'interruption pourrait porter préjudice à d'autres institutions financières, au système financier ou à l'économie dans son ensemble.

Dans tous les cas de figure, la manière dont l'IFF conçoit et met en œuvre son approche à l'égard de la résilience opérationnelle et sa gestion du risque opérationnel doit être proportionnelle à sa taille, à sa nature, à la portée et à la complexité de ses activités, à son profil de risque et à son interrelation avec le système financier.

A4. Définitions

La **résilience opérationnelle** s'entend de la capacité d'une institution à exercer ses activités, notamment ses activités essentielles, en période de perturbation. Sur le plan prudentiel, elle découle d'une gestion efficace du risque opérationnel. La résilience opérationnelle met l'accent sur la préparation, la réactivité, le rétablissement, l'apprentissage et l'adaptation, en tenant pour entendu que des perturbations, y compris des perturbations simultanées, sont inévitables. Elle englobe, entre autres, la résilience au risque lié aux technologies et au cyberrisque.

Le **risque opérationnel** s'entend du risque de pertes attribuables au personnel, à une inadéquation ou à une défaillance des processus et des systèmes internes, ou à des événements extérieurs. Il comprend le risque juridique, mais pas le risque stratégique et le risque d'atteinte à la réputation. La gestion du risque opérationnel englobe les politiques et les procédures qui sont établies pour éviter les pertes attribuables au personnel et aux événements, notamment la fraude interne et externe, le non respect des procédures, des valeurs ou des objectifs internes, ou les comportements contraires à l'éthique.

Un **événement générateur de risque opérationnel** s'entend d'un résultat non intentionnel découlant d'un risque opérationnel, ce qui comprend les pertes et gains opérationnels, qu'ils soient réels ou potentiels, ainsi que les incidents évités de justesse (c. à d. lorsque l'IFF n'a pas enregistré de perte ou de gain explicite attribuables à un incident générateur de risque opérationnel).

Les **activités essentielles** s'entendent des services, des produits et des fonctions d'une IFF qui, s'ils sont perturbés, pourraient mettre en péril la continuité des activités de l'IFF, sa sûreté et sa solidité, ou son rôle au sein du système financier.

Le **risque lié aux données** s'entend du préjudice éventuel ou des conséquences défavorables qui peuvent résulter de la collecte, du stockage, du traitement, de l'utilisation, du partage ou de l'élimination de données. Il englobe le

risque de pertes attribuables à une inadéquation ou à une défaillance des processus, du personnel et des systèmes internes, ou d'événements extérieurs qui touchent les données.

La **tolérance aux perturbations** s'entend du niveau maximal de perturbation découlant d'un risque opérationnel, quel qu'il soit, qu'une IFF est disposée à accepter compte tenu de divers scénarios graves, mais vraisemblables (p. ex., durée d'une panne, réduction des services, perte de données, portée des répercussions sur les clients). Un niveau de tolérance doit être établi pour chaque activité essentielle, en tenant compte des conséquences aggravantes qu'aurait une perturbation simultanée des services, des produits ou des fonctions qui s'y rattachent.

La **mise à l'essai de scénarios** se fonde sur une conjoncture mondiale hypothétique pour définir l'évolution des facteurs de risque influant sur les activités d'une IFF. Généralement, cet exercice concerne l'évolution de plusieurs facteurs de risque ainsi que les effets d'entraînement, c'est-à-dire les autres répercussions qui découlent en toute logique de ces changements et les mesures prises par la direction et les autorités de réglementation pour y faire face. L'horizon temporel d'une mise à l'essai de scénarios est habituellement adapté aux activités et aux risques analysés. Dans le domaine de la résilience opérationnelle, la mise à l'essai de scénarios évaluerait l'efficacité avec laquelle l'IFF parvient à respecter les niveaux de tolérance aux perturbations selon divers scénarios graves, mais vraisemblables.

A5. Résultats attendus

La ligne directrice présente quatre résultats qu'une IFF doit chercher à atteindre sur le plan de la résilience opérationnelle et de la gestion du risque opérationnel.

- L'IFF est en mesure d'exercer ses activités essentielles en période de perturbation.
- La gestion du risque opérationnel est intégrée au programme de gestion du risque à l'échelle de l'entreprise de l'IFF et contribue à la résilience opérationnelle.
- Les risques opérationnels sont gérés en adéquation avec la propension à prendre des risques de l'IFF.
- La résilience opérationnelle repose sur différents domaines liés à la gestion du risque opérationnel comme la gestion de la continuité des activités, 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 et la gestion du risque lié aux données.

A6. Consignes connexes

La présente ligne directrice doit être lue en parallèle avec les lois applicables et les lignes directrices pertinentes du BSIF, notamment les suivantes : Gouvernance d'entreprise, Gestion du risque lié aux tiers (B 10), Gestion du risque lié aux technologies et du cyberrisque (B 13), Gestion de la conformité à la réglementation (E 13), Simulation de crise (E 18) et Entités étrangères exploitant une succursale au Canada (E 4).

1. Gouvernance

Principe 1 : L'approche de l'IFF à l'égard de la résilience opérationnelle et son cadre de gestion du risque opérationnel sont mis en œuvre, régis et transmis au moyen des structures, des stratégies et des cadres qui conviennent.

1.1 La haute direction est responsable de la résilience opérationnelle et de la gestion du risque opérationnel

La haute direction est responsable d'élaborer, de mettre en œuvre et d'assurer la pérennité de l'approche de l'IFF à l'égard de la résilience opérationnelle, d'encadrer la gestion du risque opérationnel, et de veiller à affecter suffisamment de ressources financières, techniques et organisationnelles à ces fins. Les responsabilités et la reddition de comptes à l'égard de la résilience opérationnelle et de la gestion du risque opérationnel doivent être claires à tous les niveaux : secteurs d'activité et fonctions centrales, supervision de la gestion du risque et de la conformité et audit interne. La haute direction doit veiller à ce que les lacunes importantes soient corrigées rapidement et convenablement, et en rendre compte au conseil d'administration dans les meilleurs délais. La haute direction doit par ailleurs promouvoir et renforcer les comportements favorisant la résilience opérationnelle, et gérer en amont les risques liés à la culture et aux comportements qui influent sur la résilience, puisque la culture d'une institution peut avoir des conséquences sur sa capacité à résister aux perturbations opérationnelles et à les atténuer.

Veuillez consulter la ligne directrice Gouvernance d'entreprise pour connaître les attentes du BSIF envers le conseil d'administration d'une IFF en ce qui touche le plan d'affaires, la stratégie, la propension à prendre des risques, la culture, de même que la supervision de la haute direction et des contrôles internes.

1.2 La résilience opérationnelle et la gestion du risque opérationnel sont intégrées au programme et aux rapports de gestion du risque d'entreprise de l'IFF

Le BSIF s'attend à ce que l'approche de l'IFF à l'égard de la résilience opérationnelle soit pleinement intégrée à son programme de gestion du risque d'entreprise, qui englobe le risque opérationnel, le risque lié aux technologies et le cyberrisque, le risque lié aux tiers et le risque lié aux données, ainsi que la gestion de la continuité des activités, la reprise après sinistre, la gestion de crise et la gestion du changement.

Dans le cadre de la gestion du risque d'entreprise, des rapports adéquats et exacts sur l'état actuel et l'évolution probable du profil de risque opérationnel de l'IFF et de son approche à l'égard de la résilience opérationnelle doivent être fournis à la haute direction en temps opportun. Des mécanismes efficaces de transmission des dossiers à un échelon supérieur doivent aussi être en place pour signaler les événements opérationnels et les lacunes importantes susceptibles d'influer sur la capacité de l'IFF à exercer ses activités essentielles.

1.3 Les secteurs d'activité et les fonctions centrales gèrent le risque et font l'objet d'une supervision indépendante

Les secteurs d'activité et les fonctions centrales de l'IFF doivent être responsables de la gestion des risques opérationnels auxquels ils sont exposés et contribuer à l'approche de l'IFF à l'égard de la résilience opérationnelle. De son côté, l'IFF doit s'assurer que le jugement et les pratiques de gestion du risque des secteurs d'activité et des fonctions centrales sont soumis à une remise en question indépendante et efficace par la fonction de supervision de la gestion du risque et de la conformité, remise en question qui doit reposer sur un processus dûment étayé. Bien que la taille et la structure de la fonction de supervision de la gestion du risque et de la conformité puissent varier selon la nature, la taille, la complexité des activités, et le profil de risque de l'IFF, cette fonction doit toujours pouvoir remettre en question, sans crainte de représailles, les pratiques et les décisions des secteurs d'activité et des fonctions centrales au chapitre de la gestion du risque.

1.3.1 Les secteurs d'activité et les fonctions centrales sont chargés de gérer la résilience opérationnelle et les risques opérationnels dans le cadre de leurs activités quotidiennes

Puisqu'ils sont responsables de la résilience opérationnelle et de la gestion des risques opérationnels au quotidien, le BSIF s'attend à ce que les secteurs d'activité et les fonctions centrales :

- recensent et évaluent les risques opérationnels inhérents à tous les aspects de leurs activités;
- signalent les événements générateurs de risque opérationnel aux échelons supérieurs conformément aux voies de recours hiérarchique établies;
- établissent des mesures de contrôle et d'atténuation adaptées et testent la conception et l'efficacité de ces mesures;
- recensent et atténuent les risques pour les activités essentielles dans le respect des niveaux de tolérance aux perturbations établis;
- gèrent le risque opérationnel conformément au cadre de gestion de la propension à prendre des risques de l'IFF et à son approche à l'égard de la résilience opérationnelle;
- respectent l'approche de l'IFF à l'égard de la résilience opérationnelle, son cadre de gestion du risque et les politiques qui s'y rattachent;
- offrent régulièrement des séances de formation adéquates au personnel sur la gestion de la résilience opérationnelle et du risque opérationnel.

1.3.2 Une supervision indépendante de la gestion du risque et de la conformité est assurée à l'égard de la résilience opérationnelle et de la gestion du risque opérationnel

Pour favoriser une solide résilience opérationnelle et une gestion efficace du risque opérationnel à l'échelle de l'IFF, une fonction indépendante de supervision de la gestion du risque et de la conformité doit :

- établir et assurer le respect, l'examen et l'amélioration continue de l'approche de l'IFF à l'égard de la résilience opérationnelle et de ses politiques, procédures, processus et outils de gestion du risque opérationnel;
- mettre en place des outils efficaces de production de rapports;

- confirmer que des voies de recours hiérarchique adaptées sont en place, que le suivi de la résilience opérationnelle et du risque opérationnel est bien consigné par écrit, et que les lacunes importantes sont signalées aux échelons supérieurs en temps opportun et avec exactitude;
- favoriser l'intégration de la gestion du risque opérationnel au cadre global de gestion du risque à l'échelle de l'entreprise de l'IFF.

1.3.3 Une assurance indépendante est fournie

La fonction d'audit interne ou une fonction similaire doit fournir une assurance indépendante à la haute direction et au conseil d'administration quant à l'efficacité de l'approche de l'IFF à l'égard de la résilience opérationnelle, et quant au bon fonctionnement des mesures de contrôle, processus et systèmes de gestion du risque opérationnel, à l'échelle de l'entreprise.

2. Résilience opérationnelle

Résultat attendu : L'IFF est en mesure d'exercer ses activités essentielles en période de perturbation.

Pour assurer l'efficacité de son approche à l'égard de la résilience opérationnelle, l'IFF doit comprendre et consigner par écrit ses activités essentielles de bout en bout et être prête à exercer ces activités dans des circonstances graves, mais vraisemblables, dans le respect des niveaux de tolérance aux perturbations.

2.1 Recenser les activités essentielles et établir des correspondances

Principe 2 : L'IFF doit recenser ses activités essentielles et établir des correspondances entre les dépendances internes et externes.

2.1.1 Recenser et évaluer les activités essentielles

L'IFF doit recenser et consigner par écrit les services, produits et fonctions qui, s'ils sont perturbés, pourraient mettre en péril la continuité de ses activités, sa sûreté et sa solidité, ou son rôle au sein du système financier. La décision de désigner une activité comme étant essentielle dépend de la stratégie et du profil de risque de l'IFF et, dans une certaine mesure, de la taille et de la nature de l'institution, de la portée et de la complexité de ses activités, ainsi que de ses interrelations avec d'autres institutions financières.

L'IFF doit évaluer ses activités essentielles sous l'angle de leur capacité de résistance aux perturbations et aux pertes opérationnelles. Aux fins de ces évaluations, il peut être utile de quantifier les pertes financières directes (p. ex., coûts à engager pour pallier et résoudre les défaillances technologiques et autres perturbations) et indirectes (p. ex., atteinte à la réputation, occasions manquées). Selon les résultats de ces évaluations, et compte tenu de la propension à prendre des risques de l'IFF, la haute direction pourrait décider d'ajouter des mesures de contrôle ou de renforcer les mesures existantes, ou d'accepter le risque résiduel.

L'IFF doit régulièrement revoir et actualiser le recensement et l'évaluation de ses activités essentielles.

2.1.2 Évaluation globale des activités essentielles et établissement des correspondances

L'IFF doit procéder à une évaluation globale, de bout en bout, des activités essentielles pour établir l'ensemble des correspondances entre les dépendances internes et externes. Les correspondances ainsi établies doivent être suffisamment détaillées pour permettre, d'une part, de recenser les ressources humaines, les technologies, les processus, les informations, les installations et les tiers[2] sur lesquels l'IFF s'appuie pour exercer ses activités essentielles et, d'autre part, de déterminer les interrelations et les interdépendances entre ces éléments. Le niveau de détail de ces correspondances doit être suffisant pour pouvoir déceler les vulnérabilités et faciliter la mise à l'essai et l'analyse de scénarios (voir la section 2.3). L'IFF doit régulièrement revoir et actualiser les correspondances établies entre ses activités essentielles.

2.2 Établissement de niveaux de tolérance aux perturbations des activités essentielles

Principe 3 : L'IFF doit établir des niveaux de tolérance aux perturbations des activités essentielles.

2.2.1 Un niveau de tolérance aux perturbations doit être établi pour chaque activité essentielle recensée

L'IFF doit établir le niveau maximal de perturbation qu'elle est disposée à tolérer pour chaque activité essentielle, selon divers scénarios de menace et événements générateurs de risque graves, mais vraisemblables. À noter qu'il y a une différence entre niveaux de tolérance aux perturbations et propension à prendre des risques opérationnels (voir la section 3.2), et que les niveaux de tolérance doivent généralement être plus élevés. La perturbation d'une activité essentielle peut être mesurée en termes de durée ou d'unité de temps, puis nuancée à l'aide d'autres indicateurs et variables comme le volume des opérations, le nombre de clients touchés ou la valeur de la perte financière.

2.2.2 Les niveaux de tolérance aux perturbations doivent être globaux et tenir compte des dépendances internes et externes

Au moment d'établir les niveaux de tolérance aux perturbations, il faut particulièrement prêter attention aux correspondances globales, de bout en bout, entre les dépendances internes et externes nécessaires à l'exercice des activités essentielles. L'IFF doit tenir compte des conséquences qu'ont les perturbations sur d'autres activités essentielles connexes qui font appel aux mêmes ressources, et de la défaillance possible des systèmes, installations et fournisseurs tiers dont dépendent les activités essentielles.

2.3 Mise à l'essai et analyse de scénarios

Principe 4 : L'IFF doit élaborer des exercices de mise à l'essai de scénarios et mener régulièrement ces exercices au regard des activités essentielles pour évaluer sa capacité à respecter les niveaux de tolérance aux perturbations

selon divers événements générateurs de risque graves, mais vraisemblables.

2.3.1 Les exercices de mise à l'essai de scénarios doivent être prospectifs et permettre d'évaluer les conséquences d'événements générateurs de risque graves

Pour être efficaces, les exercices de mise à l'essai et d'analyse de scénarios de résilience opérationnelle doivent être prospectifs et permettre à l'institution d'évaluer, d'une part, les conséquences que pourraient avoir des événements générateurs de risque graves et, d'autre part, sa capacité à exercer ses activités essentielles dans le respect des niveaux de tolérance aux perturbations établis.

Ces exercices doivent porter sur un ensemble de menaces, risques et événements générateurs de risque opérationnel graves, mais vraisemblables, dont la nature, l'ampleur et la durée sont variables. Voici quelques exemples de ce type d'événements :

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

Au moment d'élaborer ses exercices de mise à l'essai et d'analyse de scénarios, l'IFF doit aussi tenir compte du fait qu'il est possible que des événements perturbateurs interdépendants, simultanés et prolongés surviennent.

La mise à l'essai de scénarios est un processus itératif qui parviendra à maturité et se perfectionnera au fil du temps. L'IFF doit donc prendre en compte les résultats des exercices précédents, les événements antérieurs (internes ou externes) et les incidents évités de justesse dans la conception des exercices de mise à l'essai.

2.3.2 La portée des mises à l'essai de scénarios doit être globale et organisationnelle

La mise à l'essai de scénarios s'appuie généralement sur une approche de bout en bout (ou globale) pour déterminer l'ensemble des conséquences d'une perturbation grave de plusieurs activités, notamment les dépendances internes et externes des activités et tiers essentiels. Les secteurs d'activité et les fonctions centrales

peuvent collaborer avec la fonction de supervision de la gestion du risque et de la conformité et la fonction d'audit interne pour déterminer les risques pertinents à inclure dans chaque scénario et assurer une coordination avec les tiers essentiels afin de mener des exercices de portée plus large. S'il y a lieu, l'IFF doit aussi tenir compte des résultats des exercices de mise à l'essai du plan de continuité des activités (PCA) (voir la section 4.1.3).

2.3.3 La fréquence et l'intensité des mises à l'essai sont proportionnelles au risque et à la criticité

Les exercices de mise à l'essai de scénarios doivent être conçus en fonction de la taille, de la complexité, des activités et du profil de risque de l'IFF, ainsi que de son niveau d'interrelation avec le système financier. Dans la plupart des cas, des exercices doivent être réalisés une fois par an et à chaque fois qu'un changement important est observé dans l'environnement de risque.

2.3.4 Des paramètres de suivi du niveau de perturbation doivent être mis en place

Pendant ces mises à l'essai de scénarios, l'IFF doit suivre l'évolution de ses activités essentielles et déterminer si l'institution respecte les niveaux de tolérance aux perturbations établis. Pour ce faire, l'IFF doit définir des paramètres de suivi et d'évaluation des perturbations des activités essentielles et prendre les mesures correctives nécessaires pour y remédier. L'IFF doit par ailleurs régulièrement évaluer ces paramètres pour s'assurer qu'ils sont adéquats et exhaustifs.

2.3.5 Des rapports sur la mise à l'essai et l'analyse de scénarios sont fournis à la haute direction

Les rapports doivent comprendre des évaluations de la résilience, préciser si les activités essentielles ont été menées dans le respect des niveaux de tolérance aux perturbations établis, et inclure une analyse des lacunes, des possibilités d'amélioration en matière de gestion des événements générateurs de risque opérationnel et des plans en vue de corriger les défaillances dans les meilleurs délais.

2.4 Renforcement continu de la résilience opérationnelle

L'IFF doit se concentrer sur ses activités essentielles au moment d'élaborer et de mettre en place son approche à l'égard de la résilience opérationnelle. Sachant que les paysages de risque, les contextes économiques et les stratégies d'affaires évoluent constamment, l'IFF doit sans cesse améliorer et renforcer son approche. Elle doit aussi

tenir compte du fait que les niveaux de criticité peuvent changer et que les répercussions en matière de risque peuvent s'accumuler dans plusieurs domaines. Une approche bien établie à l'égard de la résilience opérationnelle ne s'arrête pas aux activités essentielles, mais englobe d'autres activités, processus, fonctions et services qui pourraient avoir des effets importants sur l'IFF, les déposants, les titulaires de police ou les clients.

3. Gestion du risque opérationnel

Résultat attendu : La gestion du risque opérationnel est intégrée au programme de gestion du risque à l'échelle de l'entreprise de l'IFF et contribue à la résilience opérationnelle.

Le risque opérationnel est inhérent à tous les produits, toutes les activités, tous les processus et tous les systèmes. Par conséquent, la gestion de ce type de risque est déterminante pour assurer l'efficacité du programme de gestion du risque de l'IFF et de son approche à l'égard de la résilience opérationnelle.

Principe 5 : L'IFF doit établir un cadre de gestion du risque opérationnel à l'échelle de l'entreprise.

3.1 Cadre de gestion du risque opérationnel

Le BSIF s'attend à ce que l'IFF établisse un cadre de gestion du risque opérationnel (CGRO) adapté au principe de proportionnalité. Un CGRO exhaustif comprend généralement les éléments suivants :

- un énoncé de la propension à prendre des risques opérationnels qui précise des limites et des seuils d'acceptation du risque mesurables;
- des politiques et des procédures de gestion du risque opérationnel qui sont régulièrement évaluées et révisées conformément aux principes d'amélioration continue;
- une taxonomie des risques opérationnels standard permettant d'assurer l'uniformité de l'emploi des termes propres à ce type de risque à l'échelle de l'entreprise;

- des outils et des méthodes d'évaluation du risque opérationnel permettant notamment d'évaluer le risque inhérent et l'efficacité relative des mesures de contrôle, et d'estimer le risque résiduel;
- des outils de suivi du risque opérationnel.

3.2 Propension à prendre des risques opérationnels

Principe 6 : L'IFF doit établir sa 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 à l'échelle de l'entreprise de l'IFF, comme l'indique la ligne directrice Gouvernance d'entreprise du BSIF.

3.2.1 L'énoncé de la propension à prendre des risques opérationnels expose clairement les types de risques et fixe des limites d'acceptation du risque quantifiables

L'énoncé de la propension à prendre des risques doit exposer clairement la nature et les types de risques opérationnels que l'IFF est disposée à accepter dans le cadre de ses activités courantes, et inclure un élément mesurable assorti de limites ou de seuils d'acceptation du risque.

3.2.2 La propension à prendre des risques opérationnels est examinée régulièrement

La propension à prendre des risques opérationnels ainsi que les limites et les seuils qui s'y rapportent doivent être régulièrement examinés pour s'assurer qu'ils sont en adéquation avec le profil de risque de l'IFF et les risques encourus. Ces examens peuvent prendre en considération :

- les changements dans l'environnement externe;
- les augmentations ou diminutions importantes des activités ou des volumes;
- la qualité de l'environnement de contrôle;
- l'efficacité des stratégies de gestion ou d'atténuation du risque;
- l'expérience de l'IFF à l'égard des événements générateurs de risque opérationnel;

- la fréquence, le volume ou la nature des cas de non-respect des limites ou des seuils de la propension à prendre des risques.

3.3 Pratiques de gestion du risque opérationnel

Résultat attendu : Les risques opérationnels sont gérés en adéquation avec la propension à prendre des risques de l'IFF.

Principe 7 : L'IFF doit veiller à ce que l'ensemble des risques opérationnels soient recensés et évalués au moyen de pratiques de gestion du risque opérationnel appropriées.

3.3.1 Recensement et évaluation des risques

3.3.1.1 Des outils sont employés pour établir le profil de risque de l'IFF.

L'IFF doit régulièrement recenser et évaluer ses produits, activités, processus et systèmes essentiels pour veiller au respect de sa propension à prendre des risques opérationnels.

L'IFF doit par ailleurs mettre en place des outils et des pratiques efficaces pour comprendre et gérer son profil de risque opérationnel et les risques encourus, de manière à promouvoir la résilience opérationnelle. Voici des exemples de ces outils :

- évaluations des risques et des contrôles (ERC);
- indicateurs de risque clés (IRC);
- analyses des données sur les événements générateurs de risque opérationnel (EGRO).

Si cette liste présente les outils les plus couramment utilisés pour recenser, évaluer et suivre les risques opérationnels, elle n'est pas exhaustive. Il faut tenir compte de la taille et de la nature de l'IFF, de la complexité de ses activités, de sa stratégie, de son profil de risque et de l'environnement de risque pour déterminer les outils qu'il convient d'employer.

3.3.1.2 Des évaluations des risques et des contrôles sont effectuées

Pour veiller à bien comprendre le risque opérationnel inhérent à l'ensemble de ses produits, activités, processus et systèmes essentiels à l'échelle de l'entreprise, l'IFF doit utiliser un outil d'autoévaluation comme une ERC pour gérer efficacement les différents risques opérationnels. L'autoévaluation doit s'appliquer à divers niveaux, s'il y a lieu, tout en tenant compte du principe de proportionnalité et du niveau de criticité.

L'IFF doit se servir des ERC pour évaluer les risques opérationnels ainsi que la conception et l'efficacité des mesures de contrôle et d'atténuation. Ces ERC doivent tenir compte de l'environnement actuel et être de nature prospective. L'IFF doit revoir ces ERC lorsqu'elle entreprend un changement important (voir la section 4.4) ou à la suite d'un important événement générateur de risque opérationnel.

Le fait de mener des ERC devrait aider l'IFF à déterminer si son exposition au risque résiduel respecte les limites et seuils applicables, conformément à sa propension à prendre des risques opérationnels. Si le risque résiduel dépasse les limites et les seuils applicables, l'IFF doit soit prendre des mesures correctives soit accepter formellement le risque (c. à d. consigner par écrit pourquoi le risque est accepté, ainsi que l'approbation connexe), et envisager de réexaminer ou de rajuster les limites et les seuils en fonction de sa propension à prendre des risques opérationnels. L'IFF doit suivre et soumettre à une remise en question indépendante tout plan d'action découlant d'ERC pour veiller à ce que les améliorations nécessaires soient bien mises en œuvre et à ce qu'elles soient efficaces. Les plans d'action relatifs à des risques résiduels importants, à des lacunes dans les mesures de contrôle clés ou à des non-respects marqués doivent être traités en priorité.

3.3.1.3 Des indicateurs de risque clés sont établis et appliqués

Les IRC sont des paramètres qui servent à évaluer et à suivre les principaux facteurs d'exposition au risque opérationnel. On établit habituellement des indicateurs avancés et des indicateurs retardés à partir de données provenant d'évaluations du risque (comme les ERC) et d'événements internes et externes. Les indicateurs retardés doivent donner un aperçu des lacunes dans les mesures de contrôle, tandis que les indicateurs avancés s'appliquent aux risques encourus et aux risques émergents. Les IRC doivent être associés à des protocoles de recours hiérarchique permettant de cerner les tendances en matière de risque et de sonner l'alarme lorsque les niveaux de risque se rapprochent des limites ou des seuils, ou qu'ils les dépassent. Ces signes d'alerte doivent

inciter l'IFF à prendre les mesures d'atténuation qui s'imposent.

L'IFF doit mettre en place des IRC aux niveaux appropriés de l'organisation pour favoriser une gestion en amont du risque opérationnel.

3.3.1.4 Les données sur les événements générateurs de risque opérationnel sont consignées et analysées

L'IFF doit avoir mis en place des systèmes et des processus permettant de consigner et d'analyser les données sur les événements générateurs de risque opérationnel internes importants (c. à d. ceux pour lesquels un seuil interne applicable a été dépassé), ainsi que des mesures de contrôle (séparation des tâches et vérification) pour assurer l'intégrité des données.

S'agissant des événements générateurs de risque opérationnel importants, le BSIF s'attend à ce que l'IFF en détermine la cause profonde et à ce qu'elle prenne des mesures correctives de sorte que des événements similaires puissent être évités ou suffisamment bien gérés à l'avenir. Les rapports et les analyses connexes doivent être soumis à des mécanismes d'approbation et de recours hiérarchique adéquats et à une remise en question efficace, et reposer sur les répercussions potentielles ou observées de l'événement. Il faut déterminer :

- si le risque correspond à un incident réel, potentiel ou évité de justesse;
- la catégorie de risque opérationnel sous-jacente, selon la taxonomie établie;
- les lacunes et les défaillances des mesures de contrôle qui peuvent être atténuées;
- les mesures à prendre pour corriger les lacunes et les défaillances des mesures de contrôle.

3.3.2 Suivi et signalement

Principe 8 : L'IFF doit mener des activités de suivi continues des différents risques opérationnels pour déceler les lacunes dans les mesures de contrôle et les éventuels non-respects des limites ou des seuils, fournir des rapports en temps opportun et signaler les lacunes importantes aux échelons supérieurs.

3.3.2.1 Suivi des risques opérationnels continu et fondé sur le risque

Le BSIF s'attend à ce que l'IFF mène des activités de suivi continues dans le cadre de ses travaux de gestion du risque opérationnel pour se préparer à d'éventuelles menaces et à des changements du paysage de risque, et y réagir. Ces activités de suivi doivent :

- être fondées sur le risque et être renforcées dans le cas des domaines de risque élevé;
- être menées régulièrement, et dès que des changements sont observés dans l'environnement opérationnel ou le paysage de risque de l'IFF;
- inclure un ensemble complet de paramètres permettant d'évaluer le respect de la propension à prendre des risques opérationnels et des seuils et limites approuvés;
- être prospectives;
- reposer sur des données (p. ex., risques résiduels, lacunes des mesures de contrôle, événements observés, audits internes).

3.3.2.2 Des rapports exhaustifs sur le profil de risque opérationnel et les lacunes sont transmis aux échelons supérieurs, s'il y a lieu

La haute direction doit recevoir en temps opportun des rapports sur les activités de suivi continues des différents risques opérationnels menées par l'IFF, à l'échelle des unités et des fonctions opérationnelles, s'il y a lieu, et particulièrement si elle décèle d'importantes lacunes. Les rapports et analyses doivent inclure :

- une évaluation complète du profil global de risque opérationnel de l'IFF;
- les résultats des activités de suivi, y compris les paramètres ou les indicateurs formels qui sont utilisés pour cerner et signaler les cas de non-respect des limites ou des seuils de risque opérationnel;
- les lacunes importantes, les répercussions et les mesures correctives qui ont été prises;
- la consignation par écrit des raisons pour lesquelles le risque est accepté et les approbations connexes;
- des mécanismes de recours hiérarchique en temps opportun, surtout pour les expositions importantes au risque.

3.3.3 L'IFF améliore continuellement ses pratiques de gestion du risque opérationnel

Au vu de l'évolution de l'environnement de risque dans un écosystème financier interrelié où tout va très vite, l'IFF doit s'efforcer d'améliorer continuellement ses pratiques de gestion du risque opérationnel. Par exemple, si les pratiques manuelles traditionnelles ne fournissent plus une assurance suffisante, l'IFF doit envisager d'investir dans l'innovation, dans l'automatisation et dans des activités de gestion du risque opérationnel en temps réel pour renforcer continuellement sa résilience opérationnelle.

4. Domaines liés à la gestion du risque opérationnel qui renforcent la résilience opérationnelle

Résultat attendu : La résilience opérationnelle repose sur différents domaines liés à la gestion du risque opérationnel comme la gestion de la continuité des activités, 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 et la gestion du risque lié aux données.

La résilience opérationnelle repose sur une gestion efficace du risque opérationnel. Outre les pratiques élémentaires de gestion du risque opérationnel décrites à la section 3, il existe des domaines liés à la gestion du risque opérationnel qui renforcent la résilience opérationnelle en mettant l'accent sur la préparation, la réactivité, le rétablissement, l'apprentissage et l'adaptation. Les domaines ayant une incidence considérable sur l'atteinte de la résilience opérationnelle englobent la gestion de la continuité des activités, 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 et la gestion du risque lié aux données.

4.1 Gestion de la continuité des activités

La gestion de la continuité des activités (GCA) de l'IFF doit être intégrée à l'approche de l'institution à l'égard de la résilience opérationnelle et contribuer à cette résilience, de sorte que l'IFF puisse se préparer globalement à un

événement perturbateur, et y réagir. Les attentes du BSIF à l'égard de la gouvernance de la GCA cadrent avec celles visant la gouvernance du risque opérationnel et de la résilience opérationnelle de manière plus générale. Plus précisément :

- la haute direction doit veiller à ce que des ressources humaines et financières suffisantes soient affectées à l'élaboration, à la mise en œuvre et à la supervision de la GCA;
- les responsabilités et obligations redditionnelles à l'égard de la GCA doivent être clairement attribuées;
- les rapports présentés à la haute direction doivent inclure l'état de mise en œuvre de plans précis en ce qui touche la continuité des activités, les rapports d'incidents, les résultats et l'analyse des mises à l'essai et les plans d'action qui s'y rattachent en vue de renforcer la GCA de l'IFF et son approche à l'égard de la résilience opérationnelle;
- les politiques et procédures de GCA doivent être mises en œuvre à l'échelle de l'entreprise.

4.1.1 Analyse des répercussions sur les activités

L'analyse des répercussions sur les activités (ARA) est l'une des premières étapes de l'élaboration de la GCA de l'IFF. Les ARA servent à recenser les domaines et dépendances essentiels (p. ex., fonctions, produits, services, technologies, systèmes, ressources, tiers, infrastructures) et les objectifs de rétablissement s'y rapportant (p. ex., délais, données, volumes). Les ARA visent à évaluer les risques et les répercussions possibles de divers événements perturbateurs et doivent être régulièrement revues et actualisées. Elles permettent de déterminer et d'évaluer les répercussions d'une perturbation ainsi que les limites maximales à l'égard des objectifs de rétablissement avant que ne surviennent des conséquences graves.

4.1.2 Plans de continuité des activités

Des plans de continuité des activités (PCA) efficaces permettent à l'institution de se préparer à des événements perturbateurs, d'y réagir, de s'en remettre, d'en tirer des leçons et de s'y adapter. Les PCA de l'IFF doivent favoriser la continuité dans la prestation des services, l'offre des produits et l'exécution des fonctions (et plus particulièrement s'ils constituent des activités essentielles) lors de divers événements, allant d'incidents relativement mineurs aux incidents les plus graves, mais vraisemblables, et tenir compte du fait qu'il est possible que des événements interdépendants et simultanés surviennent.

Voici des exemples de bonnes pratiques au chapitre des PCA :

- établir des protocoles décisionnels internes de déclenchement des PCA;
- établir des protocoles de communication interne et externe;
- attribuer des fonctions à l'égard de la gestion des perturbations des activités essentielles;
- fixer des objectifs en matière de rétablissement, y compris des niveaux (p. ex., activités courantes) et des délais;
- définir des procédures pour prendre en compte les résultats des mises à l'essai et apporter des améliorations stratégiques aux plans;
- analyser les répercussions des événements et définir des stratégies de rétablissement;
- prendre des mesures pour former et sensibiliser le personnel afin qu'il puisse réagir et s'adapter;
- prendre des précautions pour garantir la sécurité du personnel de l'IFF pendant l'événement;
- prévoir des plans de relève en cas d'absence imprévue ou de perte de personnel clé pendant l'exécution du plan ou immédiatement après l'événement générateur de risque.

4.1.3 Mise à l'essai des plans de continuité des activités

La mise à l'essai des PCA fournit l'assurance qu'un plan bien conçu est en place pour réduire autant que possible les répercussions d'une perturbation, conformément au programme de GCA et aux objectifs de rétablissement définis dans le cadre des ARA. La fréquence et le type de mise à l'essai des PCA doivent être adaptés aux répercussions potentielles selon les ARA et la propension à prendre des risques de l'IFF.

L'IFF doit effectuer des mises à l'essai pour déceler les lacunes potentielles des PCA dans diverses circonstances défavorables. En plus de contribuer à l'amélioration continue, la mise à l'essai est essentielle pour favoriser la prise de conscience de la haute direction et d'autres employés clés, et les aider à comprendre leurs fonctions dans le cadre du PCA pendant des événements générateurs de risque.

La mise à l'essai des PCA peut aussi éclairer la mise à l'essai et l'analyse de scénarios, contribuant ainsi à une vue d'ensemble des activités essentielles à l'échelle de l'entreprise dans le cadre de l'approche de l'IFF à l'égard de la résilience opérationnelle (voir la section 2.3).

4.2 Reprise après sinistre

La planification de la reprise après sinistre contribue à adopter une posture de préparation et à prévoir d'éventuelles mesures en cas d'événements générateurs de risque graves, comme une perte d'infrastructure technologique (p. ex., des serveurs de données). Le plan de reprise après sinistre doit indiquer les fonctions des employés, ainsi que les protocoles de déclenchement du plan.

Veuillez consulter la ligne directrice B 13, Gestion du risque lié aux technologies et du cyberrisque, pour connaître les attentes du BSIF en ce qui touche la reprise après sinistre.

4.3 Gestion de crise

L'IFF doit établir un plan de gestion de crise pour garantir une réponse efficace, coordonnée et rapide en cas de crise ou d'urgence de taille attribuable à des facteurs internes ou externes. Pour assurer des communications efficaces, accélérer le rétablissement et réagir de manière décisive, l'IFF doit envisager de désigner un organe central chargé de gérer une crise, comme un groupe de gestion de crise ou une structure équivalente.

L'IFF doit aussi songer à mettre au point des protocoles de communication de crise interne et externe pour s'assurer de communiquer les meilleures informations disponibles aux bonnes parties prenantes dans les meilleurs délais. Pendant une crise, une communication efficace contribue à assurer la sécurité des employés, à limiter la perturbation des activités, à atteindre les objectifs de rétablissement et à maintenir la confiance du public envers l'institution.

Les protocoles de recours hiérarchique doivent énoncer les critères de signalement des crises (ou d'autres urgences de taille) à la haute direction et les critères de déclenchement du plan de gestion de crise.

Le plan de gestion de crise doit être régulièrement mis à l'essai et communiqué aux secteurs pertinents. Enfin, des analyses doivent être menées à la suite d'une crise pour en tirer des leçons.

4.4 Gestion du changement

En règle générale, l'exposition de l'IFF au risque opérationnel évolue lorsque cette dernière apporte un changement, comme la mise au point de nouveaux produits ou services, la pénétration de nouveaux marchés, l'exercice de nouvelles activités, le déploiement de nouveaux systèmes technologiques ou une modification importante des processus d'affaires. L'IFF doit élaborer et consigner par écrit un processus exhaustif de gestion du changement qui suit l'évolution de l'exposition de l'institution au risque opérationnel pendant tout le cycle de vie du changement qu'elle instaure.

L'IFF doit définir des politiques et des procédures de gestion du changement, ainsi que des plans d'urgence, pour composer avec le risque opérationnel lié aux nouveaux produits, services, activités, marchés, systèmes technologiques et processus d'affaires.

Lorsqu'elle instaure un changement important, l'IFF doit engager un processus de gestion du changement, associé à des plans d'urgence, et doit notamment :

- recenser et évaluer les risques inhérents et résiduels;
- évaluer les mesures de contrôle pertinentes;
- tenir compte des risques liés aux ressources humaines, à la gestion du risque et aux technologies;
- gérer le projet tout au long du cycle de vie du changement, ce qui englobe des mises à l'essai adaptées avant et après la mise en œuvre, et l'utilisation de paramètres appropriés;
- revoir la propension à prendre des risques opérationnels et les limites et seuils s'y rapportant, et apporter tout changement nécessaire à l'évaluation des risques opérationnels liés aux produits, services, activités, marchés, processus ou systèmes existants;
- recenser tout nouveau risque et évaluer toute modification de l'exposition au risque opérationnel, y compris les changements imprévus;
- soumettre le processus de gestion du changement à une évaluation indépendante et à une remise en question efficace.

4.5 Gestion du risque lié aux technologies et du cyberrisque

La défaillance d'une technologie indispensable, l'infiltration d'un système crucial, ou la perte ou la corruption de données pourrait mettre en péril la résilience opérationnelle de l'IFF. Une saine gestion du risque lié aux technologies et du cyberrisque est donc essentielle pour renforcer la résilience opérationnelle. La ligne directrice B 13 du BSIF promeut la mise en place d'une architecture et de systèmes technologiques qui cadrent avec les besoins opérationnels et la tolérance de l'IFF aux perturbations.

Veuillez consulter la ligne directrice B 13, Gestion du risque lié aux technologies et du cyberrisque, pour connaître les attentes du BSIF en ce qui touche la gestion des risques liés aux technologies.

4.6 Gestion du risque lié aux tiers

Les ententes critiques avec des tiers peuvent engendrer des risques. Par exemple, une perturbation des activités d'un tiers ou la perte ou la corruption de données essentielles peut menacer la résilience opérationnelle de l'IFF. Une gestion efficace du risque lié aux tiers contribue donc grandement à la résilience opérationnelle.

Veuillez consulter la ligne directrice B 10, Gestion du risque lié aux tiers, pour connaître les attentes du BSIF en ce qui touche la gestion des risques liés aux ententes avec des tiers.

4.7 Gestion du risque lié aux données

La gestion du risque lié aux données est essentielle pour assurer la résilience opérationnelle dans un environnement interrelié et fondé sur les données. Une gestion efficace du risque lié aux données appuie la supervision et améliore la prise de décisions en veillant à ce que les données soient exactes, complètes, pertinentes, sécurisées et protégées. Une exploitation et un traitement efficaces des données peuvent renforcer la résilience opérationnelle en limitant la probabilité et les répercussions de fuites de données, de pannes des systèmes, ou de perturbations, protégeant ainsi les activités essentielles et la réputation de l'IFF.

Une approche fondée sur le risque en matière de gestion du risque lié aux données doit englober :

- un cadre de gestion des données solide, qui comprend des politiques, des procédures, des normes, des évaluations et des mesures de contrôle;

- une propension à prendre des risques et des paramètres appropriés pour suivre la gestion du risque lié aux données et en rendre compte;
- des fonctions clairement définies à l'égard de la gestion et de la supervision des données;
- des processus permettant de classer et de protéger les données, et d'en assurer l'intégrité, la confidentialité et la disponibilité tout au long de leur cycle de vie, en fonction des risques évalués;
- la capacité de recueillir, de regrouper et de présenter de manière exacte et en temps opportun des données sur le risque à l'échelle de l'entreprise;
- une stratégie bien définie pour ce qui est de l'architecture des données et de l'infrastructure informatique qui favorise la collecte, le regroupement et la présentation des données à l'échelle de l'entreprise aux fins de la prise de décisions;
- des processus de gestion des incidents permettant de réagir à des fuites de données et à d'autres incidents liés aux données;
- la tenue régulière de séances de formation pertinentes à l'intention des personnes responsables de la gestion et de la supervision des données;
- le suivi et l'examen continus des pratiques de gestion du risque lié aux données pour cerner les points à améliorer et apporter les changements qui conviennent.

1 Les « succursales de banques étrangères » s'entendent des banques étrangères autorisées à exercer des activités au Canada par l'exploitation d'une succursale en vertu de la partie XII.1 de la *Loi sur les banques*. Les « succursales de sociétés d'assurance étrangères » s'entendent des entités étrangères qui sont autorisées à garantir au Canada des risques par l'exploitation d'une succursale en vertu de la partie XIII de la *Loi sur les sociétés d'assurances*.

2 Une « entente avec un tiers » s'entend de toute entente commerciale ou stratégique entre l'IFF et une ou plusieurs entités ou personnes, par contrat ou autrement, à l'exclusion des ententes avec les clients de l'IFF (p. ex., les déposants et les titulaires de polices) et des contrats d'emploi, qui sont exclus de cette définition. Voir la ligne directrice B 10, Gestion du risque lié aux tiers.