



Bureau du surintendant des institutions financières

[Accueil](#) > [Institutions financières](#) > [Règlementation et consignes](#) > [Directives](#) > [Lignes directrices](#)

> [Ligne directrice sur la gestion du risque lié aux tiers](#)

Ligne directrice sur la gestion du risque lié aux tiers

Le BSIF reporte la date limite de la consultation sur les versions à l'étude des lignes directrices B-10 et B-15

Dans le cadre de son processus de consultation publique sur la [version révisée à l'étude de la ligne directrice B-10, Gestion du risque lié aux tiers](#), et sur la [version à l'étude de la ligne directrice B-15, Gestion des risques climatiques](#), le Bureau du surintendant des institutions financières (BSIF) prolonge la période de commentaires jusqu'au **30 septembre 2022**.

Le BSIF communiquera à une date ultérieure tout changement au calendrier de publication des versions finales de ces lignes directrices.

Autres supports

- [PDF](#)

Documents d'accompagnement

- [Lettre](#)

Type de publication : Ligne directrice (version à l'étude)

Catégorie : Saines pratiques commerciales et limites prudentielles

N° : B-10

Date : Avril 2022

A. Vue d'ensemble

Les institutions financières fédérales (IFF) concluent des ententes commerciales et stratégiques avec des parties externes (qu'il s'agisse d'entités ou de particuliers) pour s'acquitter de différentes activités et fonctions, et offrir les services à l'appui de leurs propres opérations ou de leur stratégie commerciale.

Ces types d'ententes externes (ou ententes avec des tiers) peuvent s'avérer avantageuses pour l'IFF quand elles permettent de gagner en efficacité, de favoriser l'innovation, de suivre l'évolution des besoins opérationnels et d'améliorer les services. Toutefois, ces ententes peuvent comporter des risques qui peuvent mettre en jeu la résilience opérationnelle et financière de l'IFF.

Le Bureau du surintendant des institutions financières (BSIF) s'attend à ce que les IFF gèrent efficacement les risques et qu'elles soient, en fin de compte, responsables de l'ensemble de leurs activités, fonctions et services, qu'ils soient assurés à l'interne ou par un tiers.

À cette fin, les IFF doivent fournir au BSIF, à la demande de celui-ci, des renseignements relatifs à leurs ententes commerciales et stratégiques avec des tiers, à la gestion du risque et aux environnements de contrôle, afin d'appuyer les activités de surveillance et de supervision¹. Le BSIF s'attend à être informé rapidement des lacunes importantes qui viennent menacer la solidité de l'IFF en raison d'une entente avec un tiers.

Quoi qu'il en soit, les pouvoirs de surveillance du BSIF ne doivent d'aucune manière être restreints, que l'activité soit exécutée à l'interne, qu'elle soit impartie ou qu'elle soit réalisée de toute autre façon par un tiers.

A1. Objet et portée

La présente ligne directrice énonce les attentes du BSIF en matière de gestion des risques associés aux ententes avec des tiers.

Elle s'applique à toutes les IFF, à l'exclusion des succursales de banques étrangères et des succursales de sociétés d'assurance étrangères².

Les IFF doivent se conformer aux attentes énoncées dans la présente ligne directrice en fonction de leur taille, de la nature, de l'étendue et de la complexité de leurs activités et de leur profil de risque.

A2. Définitions

Une « **entente avec un tiers** » s'entend de toute entente commerciale ou stratégique entre la ou les IFF et une ou plusieurs entités ou personnes, par contrat ou autrement (p. ex., une autre forme d'accord ou le comportement des parties). Cette définition exclut les ententes avec les clients des IFF (p. ex., les déposants et les titulaires de polices).

Ces ententes comprennent notamment les éléments suivants :

- les activités, fonctions et services impartis³;
- le recours à des professionnels indépendants;
- les courtiers (p. ex., les courtiers en hypothèques, en assurances et en dépôts);
- les services publics (p. ex., les sources d'énergie, les télécommunications);
- les infrastructures de marchés financiers⁴ (p. ex., les systèmes de paiement, les systèmes de compensation et de règlement, les autres IFF dans les cas où l'IFF n'a pas un accès direct aux infrastructures de marchés financiers);
- les services fournis par les sociétés de portefeuille mères, les sociétés affiliées et les filiales, ou par le biais de coentreprises et de sociétés de personnes;
- d'autres relations commerciales impliquant la fourniture de services ou le stockage, l'utilisation ou l'échange de données (comme les fournisseurs de services d'infonuagique, les fournisseurs de services gérés ou les entreprises technologiques qui fournissent des services financiers)⁵.

Le « **risque lié aux tiers** » est le risque que la résilience opérationnelle et financière, ou la réputation de l'IFF, soit compromise parce qu'un tiers ne fournit pas les biens et les services, ne protège pas les données ou les systèmes, ou n'exécute pas les activités conformément à l'entente. Les scénarios de risques liés à un tiers pourraient inclure, sans s'y limiter, les cas suivants :

- l'insolvabilité du tiers;
- une perturbation opérationnelle chez le tiers causée par des défaillances ou inadéquations attribuables aux personnes, aux procédures ou aux systèmes, ou par des événements externes (p. ex., des cyberincidents);
- l'insolvabilité ou l'interruption de service d'un sous-traitant important⁶;
- les risques d'ordre politique, géographique, juridique, environnemental ou autres qui empêchent le tiers, ou ses sous-traitants importants, de fournir des services conformément à son entente avec l'IFF;
- les risques découlant de l'interconnexion entre plusieurs tiers et plusieurs IFF;
- la corruption ou la fuite de données de l'IFF⁷;
- la perte de données par le tiers.

Le « **risque de concentration** » s'entend du risque de perte ou de préjudice, pour l'IFF ou pour le système financier dans son ensemble, découlant de la dépendance à l'égard d'un petit nombre de tiers fournisseurs ou de sous-traitants, ou de leur concentration géographique. La concentration des fournisseurs tiers ou des sous-traitants, et la concentration géographique pourraient augmenter le risque global pour les IFF et pour le secteur des services financiers comme suit :

- en rendant plus difficile toute substitution d'un tiers;
- en augmentant la probabilité que l'insolvabilité ou une interruption des activités d'un tiers ou de son sous-traitant ait des répercussions sur l'IFF ou sur l'ensemble du secteur des services financiers;
- en exposant l'IFF ou le secteur des services financiers aux effets plus graves des catastrophes naturelles ou d'autres événements externes;
- en réduisant le pouvoir de négociation des IFF avec les tiers lors de la recherche d'une entente favorable à l'institution.

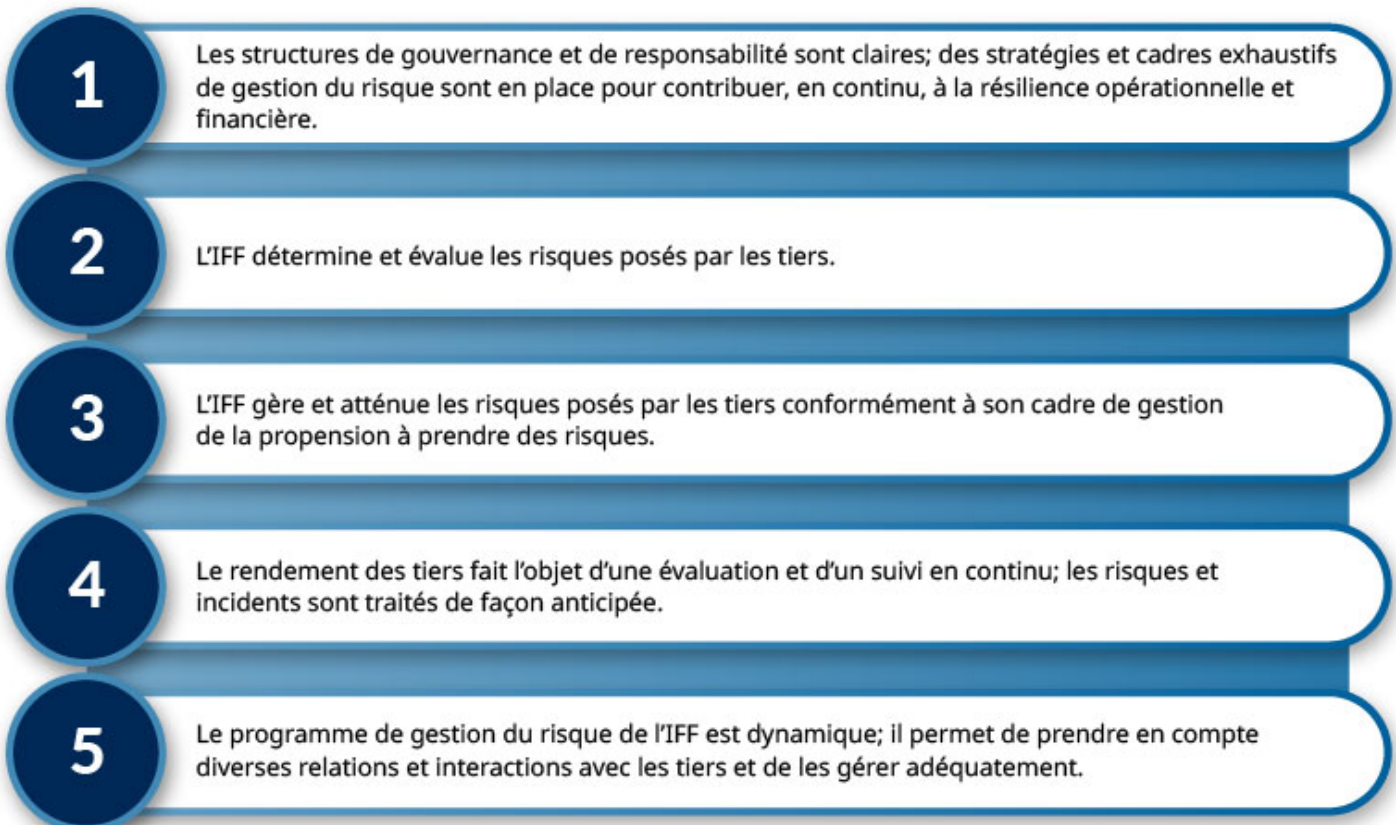
L'« **importance relative** » renvoie à l'incidence potentielle de l'entente avec le tiers sur le profil de risque, les opérations, la stratégie ou la situation financière de l'IFF. Une entente avec un tiers est importante si le tiers exerce une fonction ou un service qui fait partie intégrante d'une opération, fonction ou service significatif de l'IFF. Cela signifie qu'une défaillance de rendement du tiers pourrait causer un préjudice important aux opérations ou à la réputation de l'IFF.

L'importance relative de l'entente avec le tiers constitue un élément essentiel pour l'évaluation des deux éléments suivants :

- le niveau de risque que présente l'entente avec le tiers;
- la résilience opérationnelle et financière globale de l'IFF.

A3. Résultats

La présente ligne directrice présente cinq résultats que les IFF doivent chercher à atteindre lorsqu'elles gèrent le risque lié aux tiers. Ceux-ci contribuent à la résilience opérationnelle et financière de l'IFF et aident à préserver sa réputation.



Description du graphique - Cinq résultats que les IFF doivent atteindre lorsqu'elles gèrent le risque lié aux tiers

1. Les structures de gouvernance et de reddition de compte sont claires, et des stratégies et cadres exhaustifs de gestion du risque sont en place pour contribuer, en permanence, à la résilience opérationnelle et

financière.

2. L'IFF recense et évalue les risques posés par les tiers.
3. L'IFF gère et atténue les risques posés par les tiers conformément à sa propension à prendre des risques.
4. Le rendement des tiers fait l'objet d'une évaluation et d'un suivi constants, et les risques et incidents sont traités de façon anticipée.
5. Le programme de gestion du risque de l'IFF est dynamique; il permet de prendre en compte diverses relations et interactions avec les tiers et de les gérer adéquatement.

A4. Consignes connexes

La présente ligne directrice doit être lue en parallèle avec les lois applicables et les lignes directrices pertinentes du BSIF, notamment la ligne directrice E-21, *Gestion du risque opérationnel*, la ligne directrice B-13, *Gestion du risque lié aux technologies et du cyberrisque* et la ligne directrice *Gouvernance d'entreprise*.

Table des matières

- **A. Vue d'ensemble**
 - **A1. Objet et portée**
 - **A2. Définitions**
 - **A3. Résultats**
 - **A4. Consignes connexes**
- **1. Gouvernance**
 - **1.1. Responsabilités**
 - **1.2. Cadre de gestion du risque lié aux tiers**
- **2. Programme de gestion du risque lié aux tiers**
 - **2.1. Démarche axée sur le risque**
 - **2.2. Détermination et évaluation des risques**
 - **2.3. Gestion et atténuation des risques**
 - **2.4. Suivi et reddition de comptes**
- **3. Ententes spéciales**
 - **3.1. Contrats-types et ententes spéciales**
 - **3.2. Entente avec un tiers quand le tiers est l'auditeur externe**
- **4. Risque lié aux technologies et cyberrisque découlant des ententes avec les tiers**
- **Annexe 1 - Exemples de facteurs à prendre en compte lors de la diligence raisonnable**
- **Annexe 2 - Dispositions minimales des ententes avec des tiers**

1. Gouvernance

Résultat : Les structures de gouvernance et de responsabilité sont claires; des stratégies et cadres exhaustifs de gestion du risque sont en place pour contribuer, en continu, à la résilience opérationnelle et financière.

1.1. Responsabilités

Principe n^o 1 : L'IFF est l'ultime responsable de l'ensemble des activités, fonctions et services qui sont impartis à des tiers et de la gestion des risques liés aux ententes avec ceux-ci.

1.1.1. L'IFF demeure responsable des services impartis à des tiers et de la gestion des risques liés aux ententes et interactions avec ceux-ci

L'IFF dispose de la flexibilité nécessaire pour organiser ses activités de manière à atteindre ses objectifs commerciaux et stratégiques. Toutefois, l'IFF conserve la responsabilité de toutes ses activités, fonctions et services impartis par le biais d'ententes avec des tiers, des données échangées avec eux ou des données auxquelles ils ont accès, ainsi que de la gestion des risques découlant de ces ententes.

La haute direction de l'IFF doit être convaincue que les activités, fonctions et services assurés par les tiers sont menés de manière saine et sûre, et en conformité avec les exigences législatives et réglementaires applicables ainsi qu'avec les politiques, normes et processus internes de l'IFF. Elle doit aussi être convaincue que les ententes avec les tiers sont conformes à la propension de l'institution à prendre des risques et qu'elles sont gérées proportionnellement au niveau de risque et à l'importance relative associés à l'entente.

Consultez la ligne directrice **Gouvernance d'entreprise** du BSIF pour en savoir plus sur les attentes du BSIF à l'égard des conseils d'administration des institutions en ce qui concerne la stratégie opérationnelle, la propension à prendre des risques et les politiques de gestion opérationnelle, de gestion commerciale, de gestion du risque et de gestion de crise.

1.2. Cadre de gestion du risque lié aux tiers

Principe n° 2 : L'IFF doit établir un cadre de gestion du risque lié aux tiers qui définit clairement les rôles, les responsabilités, les politiques et les processus permettant de recenser, de gérer, d'atténuer, de surveiller et de communiquer les risques liés au recours à des tiers.

1.2.1. Le cadre de gestion du risque lié aux tiers s'applique à l'échelle de l'entreprise, est dynamique et régit le cycle de vie des ententes avec des tiers

L'IFF doit établir un cadre de gestion du risque lié aux tiers qui fournit une vue d'ensemble de ses expositions envers ceux-ci. Le cadre doit tenir compte de la propension de l'IFF à prendre des risques, et il doit être conforme à ses cadres de gestion du risque opérationnel ou d'entreprise.

Le cadre doit être conçu pour couvrir le cycle de vie d'une entente avec un tiers : de la recherche d'un fournisseur, y compris la diligence raisonnable, à la résiliation potentielle de l'entente. Le cadre de gestion du risque lié aux tiers doit indiquer comment l'IFF va recenser, évaluer, gérer, atténuer, surveiller et communiquer les risques liés aux tiers.

Le BSIF s'attend à ce que l'IFF réexamine et actualise ce cadre régulièrement, et à ce qu'elle y apporte des améliorations en fonction de sa mise en œuvre, de son efficacité et des autres leçons apprises (p. ex., les incidents antérieurs).

1.2.2. Le cadre de gestion du risque lié aux tiers reflète différents éléments clés

À tout le moins, il devrait établir et régir les éléments suivants :

- les différentes responsabilités dans la gestion du risque lié aux tiers, y compris celles afférentes aux fonctions de supervision pertinentes;
- des rôles et responsabilités clairs en matière de supervision et de gestion des ententes avec les tiers ainsi que des processus de gestion des risques qui y sont associés;
- la propension à prendre des risques liés aux tiers et son évaluation (p. ex., les limites, les seuils et les principaux indicateurs de risque);
- une méthode d'évaluation du niveau de risque et de l'importance relative des ententes avec les tiers;
- des politiques, normes, systèmes et processus régissant le risque lié aux tiers, qui sont approuvés, régulièrement révisés et mis en œuvre de manière cohérente à l'échelle de l'entreprise;
- des processus et des systèmes permettant de recenser, d'évaluer, de gérer, de surveiller, de mesurer et de communiquer la conformité des tiers aux dispositions contractuelles ou aux ententes de niveau de service, y compris des processus de gestion des exceptions et des incidents;
- des processus permettant de recenser, d'évaluer, de gérer, de surveiller, de mesurer et de communiquer les risques liés aux tiers (y compris le risque lié aux technologies, le cyberrisque, le risque de concentration, le risque lié à la gestion de la continuité des activités, le risque stratégique et le risque financier) en tenant compte de la contribution de l'ensemble des ententes avec des tiers au risque global de l'IFF;

- l'établissement de rapports globaux à l'intention de la haute direction sur l'exposition au risque lié aux tiers et les tendances en la matière, afin d'éclairer le profil de risque actuel et émergent de l'IFF, y compris une liste de fournisseurs classés selon leur niveau de risque et leur importance relative.

2. Programme de gestion du risque lié aux tiers

Le BSIF s'attend à ce que l'IFF gère le risque lié aux tiers d'une manière qui soit proportionnelle au niveau de risque et à la complexité de l'écosystème de tiers auxquels elle a recours. Il s'attend aussi à ce que l'IFF évalue régulièrement ses ententes avec des tiers, et à ce qu'elle soumette celles présentant un risque et une importance relative plus élevés à une évaluation plus fréquente et plus rigoureuse.

Dans le cas des ententes importantes et de celles présentant un risque élevé pour l'IFF, le BSIF s'attend à ce que **toutes** les attentes énoncées à la section 2 soient considérées comme des attentes minimales.

2.1. Démarche axée sur le risque

2.1.1. Les critères d'évaluation du risque sont exhaustifs et évolutifs

Les critères utilisés par l'IFF pour évaluer les risques découlant des ententes avec des tiers doivent être exhaustifs et viser principalement les ententes présentant un risque élevé. Toutefois, ils doivent aussi régir la supervision des autres ententes conformément à la démarche axée sur le risque adoptée par l'IFF. L'institution doit revoir les critères d'évaluation périodiquement afin de s'assurer qu'ils restent adaptés au paysage du risque.

2.1.2. L'IFF détermine l'importance relative des tiers

La détermination de l'importance relative constitue un volet essentiel d'une bonne gestion du risque. L'importance relative d'une entente avec un tiers influence la nature et la fréquence des activités de gestion du risque de l'IFF. Il faut également revoir l'importance relative à intervalles réguliers.

2.1.3. Le niveau de risque et l'importance relative sont évalués

Pour déterminer le niveau de risque et l'importance relative, l'IFF doit tenir compte, entre autres, de ce qui suit :

- le recours à des sous-traitants par le tiers;
- le risque de perte ou de préjudice pour l'IFF dans le cas où le tiers ou un sous-traitant important ne répond pas aux attentes, en raison d'une interruption de service, d'une panne, d'une atteinte à la cybersécurité ou pour toute autre raison;
- la capacité de l'IFF à évaluer les mesures de contrôle chez le tiers et à continuer à satisfaire aux exigences réglementaires et légales à l'égard des activités exercées par le tiers, notamment en cas d'interruption de service;
- la possibilité de remplacer le tiers, y compris la transférabilité des services et la rapidité de leur transfert;
- l'incidence potentielle sur les activités de l'IFF si elle devait se retirer de l'entente avec le tiers et retenir les services d'un autre fournisseur ou s'occuper elle-même de l'activité;
- la santé financière du tiers et le risque potentiel d'obligation d'intervenir, c'est-à-dire que l'IFF est tenue de fournir un soutien financier au tiers ou de reprendre son activité;
- le degré de dépendance de l'IFF ou du secteur à l'égard du tiers ou le degré de concentration (voir la section 2.2.3);
- tout autre risque financier et non financier pertinent lié au recours au tiers.

2.1.4. La rigueur des activités de gestion du risque correspond au niveau de risque et à l'importance relative

La robustesse et la fréquence des activités de gestion du risque lié aux tiers entreprises par l'IFF (p. ex., évaluation du risque, atténuation, suivi, mesure et production de rapports) doivent être proportionnelles au niveau de risque et à l'importance relative associés à l'entente avec le tiers.

2.2. Détermination et évaluation des risques

Résultat : L'IFF détermine et évalue les risques posés par les tiers.

Principe n° 3 : Avant de conclure une entente avec un tiers, et périodiquement par la suite en fonction du niveau de risque et de l'importance de l'entente, l'IFF doit déterminer et évaluer les risques qu'elle représente. Plus précisément, l'IFF doit effectuer des évaluations du risque pour décider de la sélection des tiers, évaluer et réévaluer le risque et l'importance de l'entente, et planifier l'atténuation et la supervision adéquates des risques.

2.2.1. Évaluation du risque

2.2.1.1. L'IFF évalue le risque et l'importance relative de l'entente tout au long de son cycle de vie

Elle doit procéder à des évaluations du risque associé à chaque entente avec un tiers afin de déterminer le risque et l'importance relative de celle-ci, en tenant compte à la fois des risques que pose l'entente et de ceux qu'elle permet d'atténuer (p. ex., le recours à des fournisseurs de différents territoires pour réduire la concentration géographique) et des mesures d'atténuation possibles.

L'IFF effectue de telles évaluations aux moments suivants :

- avant de conclure l'entente avec le tiers (voir section 2.2.2);
- régulièrement tout au long du cycle de vie de l'entente, à une fréquence et selon une portée proportionnelles au niveau de risque et à l'importance relative de l'entente;
- chaque fois qu'il y a un changement important dans l'entente ou chez le tiers (y compris une perturbation chez le tiers ou du service fourni).

Ces évaluations du risque doivent, à tout le moins, permettre ce qui suit :

- déterminer si l'entente est conforme à la propension de l'IFF à prendre des risques liés aux tiers et d'autres risques pertinents;
- établir le niveau de risque et l'importance relative de l'entente;
- élaborer un plan, prévoyant des mesures de suivi et d'atténuation d'une intensité appropriée, afin de gérer l'entente conformément à la propension de l'IFF à prendre des risques.

2.2.2. Diligence raisonnable

Principe n° 4 : L'IFF doit effectuer un examen de diligence raisonnable avant de conclure des contrats ou d'autres formes d'ententes avec un tiers, et continuer d'en mener par la suite selon le niveau de risque et l'importance relative de l'entente.

2.2.2.1. L'IFF établit un processus de diligence raisonnable

L'IFF doit établir des processus de diligence raisonnable concernant les ententes avec des tiers et les appliquer avant la conclusion de toute entente et de façon continue par la suite, y compris des processus documentés de signalement des risques aux échelons supérieurs, d'approbation et d'acceptation.

2.2.2.2. La diligence raisonnable exercée est proportionnelle au niveau de risque et à l'importance relative

L'IFF doit exercer une diligence raisonnable proportionnelle au niveau de risque et à l'importance relative de chaque entente avec un tiers :

- avant de conclure l'entente;
- dans le cadre du processus de renouvellement de l'entente;
- de façon périodique et continue en fonction du niveau de risque et de l'importance relative, ou à chaque modification importante de l'entente avec le tiers, comme un changement apporté à sa nature ou une évolution de son importance relative.

La diligence raisonnable doit tenir compte de tous les facteurs qualitatifs (p. ex., opérationnels) et quantitatifs (p. ex., financiers) pertinents au regard de l'entente avec le tiers. On trouvera une liste non exhaustive de facteurs à prendre en compte à l'*annexe 1* de la présente ligne directrice.

2.2.2.3. L'IFF tient compte de certains points précis avant de conclure une entente avec un tiers à l'extérieur du Canada

Lorsqu'elle envisage de conclure une entente avec un tiers situé à l'extérieur du Canada (ou avec un tiers canadien ayant des sous-traitants importants situés à l'extérieur du Canada), l'IFF doit porter une attention particulière aux exigences juridiques des pays en question, ainsi qu'aux risques potentiels d'ordre politique, juridique, sécuritaire, économique, environnemental, social et autres qui pourraient entraver la capacité du tiers à fournir des services.

2.2.3. Risque de concentration

2.2.3.1. L'IFF évalue le risque de concentration

Pour déterminer le niveau d'atténuation approprié, l'IFF doit évaluer le risque de concentration avant de conclure un contrat ou un accord et en continu par la suite. Les processus établis doivent inclure des mesures raisonnables pour évaluer le risque de concentration sur plusieurs dimensions, notamment celles qui concernent le fournisseur, les sous-traitants et la région d'où ils offrent leurs services. Tout au long du processus, il faut tenir compte de la concentration à l'échelle des fonctions et unités opérationnelles et des entités juridiques de l'IFF, ainsi que dans l'ensemble de l'IFF.

2.2.4. Gestion de la chaîne d'approvisionnement

Principe n° 5 : L'IFF doit évaluer, gérer et surveiller les risques associés aux ententes de sous-traitance conclues par des tiers, y compris leur incidence sur le risque de concentration.

Le risque lié à la sous-traitance découle de la complexité et de l'interdépendance de la chaîne d'approvisionnement du tiers. La sous-traitance diminue la capacité de l'IFF à gérer le risque lié à ces ententes et peut augmenter le risque global que présente le recours à certains tiers.

2.2.4.1. Les risques liés aux pratiques de sous-traitance sont recensés et compris

L'IFF doit évaluer si un important recours à la sous-traitance pourrait compromettre sa résilience opérationnelle et financière advenant une forte perturbation de la chaîne d'approvisionnement du tiers, et si ces répercussions l'emportent sur les avantages que procure l'entente.

Avant de conclure une entente avec un tiers, l'IFF doit déterminer et comprendre les facteurs de risques liés aux pratiques de sous-traitance de celui-ci, y compris, à tout le moins :

- l'ampleur des activités de sous-traitance, y compris s'il y a recours à des sous-traitants importants;
- l'emplacement géographique des sous-traitants et les risques d'ordre politique, sécuritaire, économique, environnemental, social et autres qui y sont associés;
- la capacité des sous-traitants à fournir des services conformes aux normes de rendement et aux mesures de contrôle décrites dans le contrat avec le tiers, y compris en cas d'interruption de service;
- la capacité des sous-traitants à satisfaire aux exigences légales et réglementaires.

2.2.4.2. L'IFF dispose de toute l'information sur le recours aux sous-traitants

L'IFF doit aussi avoir un droit de regard sur le recours à des sous-traitants par le tiers. Pour ce faire, elle peut :

- inclure des dispositions contractuelles qui interdisent le recours à des sous-traitants pour certaines fonctions;
- exiger d'être informée, par écrit et sans tarder, lorsqu'un sous-traitant est engagé, ou remplacé, pour exécuter certaines des fonctions confiées par contrat au tiers;
- se réserver le droit de refuser le recours à un sous-traitant;
- établir des dispositions contractuelles lui permettant d'exiger ou de réaliser un audit du sous-traitant.

2.2.4.3. L'IFF a la preuve que le tiers est capable de gérer le risque lié aux sous-traitants

L'IFF doit s'assurer que le tiers a la capacité de surveiller et de gérer les risques découlant du recours à des sous-traitants, y compris, si possible, par des droits d'audit ou l'accès à des rapports d'audit indépendants.

De plus, elle doit évaluer et prendre en compte l'incidence du recours à des sous-traitants sur le risque de concentration que présentent les ententes avec des tiers (voir 2.2.3 ci-dessus).

2.3. Gestion et atténuation des risques

Résultat : L'IFF gère et atténue les risques posés par les tiers conformément à son cadre de gestion de la propension à prendre des risques.

2.3.1. Accords et contrats

Principe n° 6 : L'IFF doit conclure des ententes écrites qui précisent les droits et les responsabilités de chaque partie.

2.3.1.1. Les responsabilités sont clairement définies dans le texte de l'entente

Le BSIF s'attend à ce que les ententes avec des tiers soient encadrées par un contrat écrit ou un autre type d'accord (p. ex., une entente de niveau de service) qui énonce les droits et les responsabilités de chaque partie et qui a été examiné par le conseiller juridique de l'IFF. Le BSIF reconnaît que certaines ententes avec des tiers ne peuvent être encadrées par un contrat sur mesure et que des ententes peuvent exister même en l'absence de contrat ou d'accord officiel. Voir la section 3 de la présente ligne directrice pour connaître les attentes du BSIF à l'égard de ce type d'ententes avec des tiers.

2.3.1.2. Le tiers doit respecter les dispositions imposées par l'IFF

Pour gérer les risques associés à chaque entente avec un tiers, l'IFF doit structurer son contrat écrit avec celui-ci de manière à pouvoir répondre aux attentes énoncées dans la présente ligne directrice. À tout le moins, le BSIF s'attend à ce que l'IFF inclue, dans les contrats écrits, les dispositions énoncées à l'*annexe 2* de la présente ligne directrice.

2.3.2. Sécurité et mesures de contrôle des données (y compris l'emplacement des données)

Principe n° 7 : Pendant toute la durée de l'entente avec le tiers, l'IFF et le tiers doivent établir et maintenir des mesures appropriées pour protéger la confidentialité, l'intégrité et la disponibilité des documents et des données.

2.3.2.1. Les responsabilités en matière de sécurité des documents et des données sont définies

Les contrats avec des tiers doivent définir les responsabilités de chaque partie en matière de confidentialité, de disponibilité et d'intégrité des documents et des données. Ils doivent établir, entre autres, les points suivants :

- l'étendue des documents et des données à protéger;
- la disponibilité des documents et la facilité de l'accès aux données, sur demande, par l'IFF et le BSIF;
- les mesures de contrôle et le suivi de l'utilisation par le tiers des systèmes et de l'information de l'IFF;
- un énoncé clair des responsabilités de chaque partie dans la gestion de la sécurité des données;
- la partie responsable des pertes pouvant résulter d'une atteinte à la sécurité;
- les exigences de signalement en cas d'atteinte à la sécurité.

En outre, les contrats doivent préciser que les documents et données de l'IFF doivent être constamment séparés de ceux des autres clients, y compris pendant leur transfert ou dans des conditions défavorables (p. ex., interruption de service). Les documents et les données doivent être soumis aux mêmes normes de protection, qu'ils soient chez le tiers ou à l'IFF.

2.3.2.2. Exigences en matière de tenue de documents

La *Loi sur les banques*, la *Loi sur les sociétés d'assurances* et la *Loi sur les sociétés de fiducie et de prêt* (collectivement, les lois régissant les IFF) renferment des exigences relatives à certains documents que les IFF doivent préparer et tenir

à jour⁸. Le BSIF s'attend à ce que les documents soient mis à jour et renferment des données exactes à la fin de chaque jour ouvrable⁹, et à ce qu'ils soient suffisamment détaillés pour permettre :

- au BSIF d'examiner et d'analyser les activités et les affaires de l'IFF;
- au BSIF de gérer les actifs de l'IFF avant la nomination d'un liquidateur, dans le cas où le surintendant prendrait le contrôle des actifs de l'institution;
- au liquidateur de procéder à une liquidation efficace des actifs de l'IFF.

Les documents électroniques doivent pouvoir être reproduits sous une forme écrite intelligible dans un délai raisonnable. Le BSIF s'attend à ce que les documents électroniques soient accessibles et intelligibles sans engager de coûts supplémentaires et en utilisant des applications commerciales facilement accessibles. Pour certains types de renseignements comme les accords de réassurance ou les dossiers sur des activités plus complexes, il se peut que les registres électroniques reproduits ne soient pas suffisants aux fins de l'examen par le BSIF, et les originaux signés pourraient devoir être mis à disposition sur demande.

Les lois régissant les IFF exigent qu'elles conservent des exemplaires des documents à leur siège social ou à tout autre endroit au Canada que leurs administrateurs jugent approprié. Si les documents sont sous forme électronique, des copies complètes doivent être conservées sur un serveur situé aux endroits prévus par les lois régissant les IFF¹⁰.

Certaines IFF ne sont pas tenues de conserver des exemplaires des documents aux endroits susmentionnés au Canada. Dans ces circonstances, elles doivent fournir au BSIF un accès immédiat, direct, complet et continu aux documents conservés à l'étranger¹¹.

2.3.3. Droits à l'information et audit

Principe n° 8 : Les ententes conclues par l'IFF avec des tiers doivent permettre à celle-ci d'obtenir rapidement des renseignements exacts et complets qui l'aideront à superviser le rendement des tiers et les risques. L'IFF doit aussi avoir le droit de réaliser un audit indépendant d'un tiers ou d'en faire effectuer un.

2.3.3.1. Le tiers fournit des renseignements et des rapports à l'IFF

Le contrat avec le tiers doit préciser le type de renseignements que celui-ci doit transmettre à l'IFF et la fréquence de communication. Cela comprend des rapports qui permettront à l'IFF de déterminer si les indicateurs de rendement sont satisfaisants et de disposer de tout autre renseignement nécessaire à son programme de suivi, y compris les indicateurs de risque (voir la section 2.4).

2.3.3.2. Le tiers signale les événements qui pourraient avoir une incidence importante sur l'IFF

Le contrat doit contenir des exigences et des procédures garantissant que le tiers signale à l'IFF, sans délai, les événements susceptibles d'avoir une incidence importante sur les risques et la prestation du service.

2.3.3.3. Le rendement du service et les mesures de contrôle sont évalués, et des droits d'audit sont institués, s'il y a lieu

Le contrat doit donner à l'IFF et au BSIF le droit d'évaluer les pratiques de gestion du risque lié au service fourni. Plus précisément, l'IFF et le BSIF doivent être en mesure d'évaluer les risques découlant de l'entente ou de nommer des auditeurs indépendants pour évaluer les pratiques de gestion du risque lié au service fourni et les risques découlant de la relation au nom de l'IFF ou du BSIF. L'IFF et le BSIF doivent également être en mesure d'accéder aux rapports d'audit du service fourni à l'IFF.

L'IFF doit utiliser un éventail de méthodes d'audit et de collecte de renseignements (p. ex., rapports indépendants fournis par des tiers, audits individuels ou collectifs).

2.3.4. Planification de la continuité des activités et mise à l'essai

Principe n° 9 : Le contrat entre l'IFF et le tiers doit prévoir la capacité d'assurer les opérations en cas d'interruption de service, y compris la tenue à jour, la mise à l'essai et l'activation des plans de continuité des activités et de reprise après sinistre. L'IFF doit avoir des plans d'urgence relativement à ses ententes importantes avec des tiers.

2.3.4.1. Les moyens permettant d'assurer la continuité des activités et la reprise après sinistre sont définis et contrôlés

Les contrats avec les tiers doivent exiger que le tiers s'engage à tout le moins à ce qui suit :

- décrire les mesures qu'il prendra pour veiller à la continuité des services en cas de perturbation;
- contrôler régulièrement ses programmes de continuité des activités et de reprise après sinistre qui concernent les services fournis à l'IFF;
- informer l'IFF des résultats des essais;
- remédier à toute déficience importante.

Les plans de continuité des activités et de reprise après sinistre de l'IFF doivent à tout le moins :

- couvrir des situations graves, mais vraisemblables (temporaires ou permanentes), dans lesquelles le tiers risquerait de ne plus pouvoir fournir le service;
- définir des systèmes de sauvegarde et des redondances qui sont proportionnels à l'importance relative du service fourni;
- garantir que l'IFF a en sa possession, en cas d'interruption des services du tiers, tous les documents nécessaires pour lui permettre de poursuivre ses activités, de respecter ses obligations légales et de fournir toute information que peut exiger le BSIF, ou qu'elle peut y accéder facilement¹².

S'il y a lieu, la conception et les essais conjoints des plans de continuité des activités et des plans de reprise après sinistre devraient être envisagés entre le tiers et l'IFF, en fonction de l'importance relative du service.

2.3.5. Stratégie et planification de sortie

2.3.5.1. Des stratégies de sortie sont mises au point pour assurer la continuité des services essentiels

L'IFF doit établir des plans de sortie proportionnels au niveau de risque et à l'importance relative de chaque entente avec un tiers afin de veiller à la continuité des activités de l'IFF en temps normal et en situation de crise. Ces plans doivent être documentés et répondre aux conditions suivantes :

- prévoir les sorties planifiées et non planifiées, telles que le défaut d'un fournisseur ou un arrêt total ou une perturbation prolongée des services, et définir les conditions qui déclencheront l'activation des plans de sortie ou d'urgence;
- prévoir un ensemble d'activités à réaliser lors d'une sortie en situation de crise, par exemple à la suite de la défaillance ou de l'insolvabilité du fournisseur de services (un « guide » pour une sortie en situation de crise);
- prévoir un ensemble d'activités à réaliser lors d'une sortie planifiée et gérée pour des raisons commerciales, de rendement ou stratégiques (un « guide » pour une sortie sans situation de crise);
- prendre en compte les dispositions contractuelles ayant une incidence sur la sortie, telles que les exigences de signalement et les dispositions obligeant le tiers à fournir des services pendant une période prescrite après le signalement de la sortie;
- être suffisamment détaillés (p. ex., d'autres options ou fournisseurs, avec des échéanciers, des coûts, des ressources, les répercussions sur les revenus et des solutions de contournement provisoires) pour permettre une exécution rapide;
- couvrir des scénarios graves, mais vraisemblables, et renfermer des plans documentés pour chaque scénario;
- faire l'objet d'examen réguliers, qui deviennent plus fréquents en cas de changements importants dans les ententes avec les tiers.

2.4. Suivi et reddition de comptes

Résultat : Le rendement des tiers fait l'objet d'une évaluation et d'un suivi en continu; les risques et incidents sont traités de façon anticipée.

Principe n° 10 : L'IFF doit faire le suivi de ses ententes avec des tiers afin de vérifier la capacité de ces derniers à continuer de respecter leurs obligations et à gérer les risques de façon efficace.

2.4.1. Supervision du fournisseur tiers

2.4.1.1. L'IFF fait le suivi de ses ententes avec des tiers

L'IFF doit faire le suivi de ses ententes avec des tiers pour s'assurer que les services sont fournis conformément aux modalités de celles-ci et que les tiers en question demeurent en bonne santé financière.

Le suivi doit également porter sur la supervision régulière des risques actuels et émergents et des acceptations des risques¹³ ainsi que sur la conformité de l'entente avec le tiers aux politiques et procédures de l'IFF en matière de risque et aux attentes du BSIF. Le suivi doit porter sur l'entente en tant que telle, de même que sur l'unité opérationnelle, le segment, la plateforme et l'entreprise globalement.

L'étendue et la fréquence du suivi doivent être proportionnelles au niveau de risque et à l'importance relative de l'entente avec le tiers.

2.4.1.2. Les indicateurs confirment que le risque résiduel reste dans les limites de la propension à prendre des risques

L'IFF doit établir des processus pour vérifier régulièrement que le risque résiduel de ses ententes avec des tiers, individuellement et globalement, demeure dans les limites de sa propension à prendre des risques. Pour faciliter l'atteinte de ce résultat, l'IFF doit établir des indicateurs et des seuils connexes, et les inclure dans la reddition des comptes afin d'alerter la haute direction dès lors qu'un seuil est sur le point d'être franchi. Elle doit aussi prévoir les conditions qui déclencheraient le signalement de la situation aux échelons supérieurs.

2.4.2. Gestion des incidents et signalement

Principe n° 11 : L'IFF et le tiers doivent mettre en place des processus documentés afin de détecter, enquêter, signaler, suivre et résoudre les incidents pour veiller à la résilience opérationnelle et financière continue et pour maintenir les niveaux de risque dans les limites de la propension de l'IFF à prendre des risques.

2.4.2.1. Le tiers a mis en place des processus de gestion des incidents clairement définis

Dans le cadre d'un programme efficace de gestion du risque lié aux tiers, l'IFF doit s'assurer que ceux-ci suivent des processus clairement définis et documentés pour déceler les incidents (y compris ceux concernant des sous-traitants), enquêter à leur sujet, transmettre l'information aux échelons supérieurs, prendre des mesures correctives efficaces et en aviser l'IFF rapidement si ces incidents peuvent se répercuter directement ou indirectement sur la capacité du tiers à fournir les biens ou les services prévus au contrat.

2.4.2.2. Les exigences du tiers en matière de déclaration et de signalement des incidents aident l'IFF à se conformer aux exigences du BSIF en matière de signalement d'incidents

L'IFF doit s'assurer que ses ententes écrites avec des tiers renferment les dispositions voulues pour permettre à l'IFF de se conformer à ses exigences de déclaration en vertu du préavis du BSIF intitulé [Signalement des incidents liés à la technologie et à la cybersécurité](#). Ces dispositions pourraient inclure, entre autres, l'obligation de signaler rapidement à l'IFF les incidents liés à la technologie et les cyberincidents (chez le tiers ou le sous-traitant), y compris la transmission d'informations sur chaque incident conformément au préavis.

2.4.2.3. L'IFF met en place un processus interne de gestion des incidents

L'IFF doit avoir des processus internes clairement définis pour assurer la gestion efficace des incidents survenus chez les tiers et leur signalement aux échelons supérieurs, et pour effectuer un suivi ultérieur des mesures correctives. Les processus établis doivent définir clairement les responsabilités à tous les niveaux de l'IFF et les conditions qui déclencheraient le signalement aux échelons supérieurs au sein de l'IFF.

2.4.2.4. Les incidents font l'objet d'une enquête et d'une analyse, et les résultats sont communiqués

Pour s'assurer que les mesures correctives sont suffisantes, l'IFF doit demander au tiers d'effectuer une analyse des causes fondamentales et de communiquer les résultats de tout incident, en fonction de sa gravité et de son incidence potentielle sur l'IFF. De plus, l'IFF doit effectuer, s'il y a lieu, sa propre analyse des causes fondamentales. Elle doit également effectuer le suivi des mesures correctives.

3. Ententes spéciales

Résultat : Le programme de gestion du risque de l'IFF est dynamique; il permet de prendre en compte diverses relations et interactions avec les tiers et de les gérer adéquatement.

3.1. Contrats-types et ententes spéciales

Les contrats sur mesure peuvent être des outils efficaces pour atténuer le risque lié aux tiers. Cependant, il n'est pas rare que les IFF reçoivent ou utilisent des produits ou des services de fournisseurs (services publics, fournisseurs de services Internet, infrastructures de marchés financiers et autres) selon des modalités prédéfinies dans des contrats-types. Or, la capacité d'adapter les modalités de tels contrats est limitée.

3.1.1. Les services assurés par des tiers comportent des risques même s'ils ne sont pas l'objet d'un contrat

L'absence d'une entente écrite¹⁴ n'exclut pas l'existence d'une relation avec un tiers. Même si l'IFF n'a pas toujours de liens directs avec tous les tiers avec lesquels elle interagit, ceux-ci peuvent néanmoins présenter des risques.

3.1.2. L'IFF gère le risque lié aux tiers avec lesquels elle n'a pas conclu de contrat ou avec lesquels elle a conclu des contrats-types

Dans les situations où un contrat ou accord type ou non officiel appuie l'entente, le BSIF s'attend toujours à ce que l'IFF ait un programme de gestion du risque lié aux tiers qui couvre la relation et qui est proportionnel au niveau de risque et à l'importance relative de la relation avec le tiers. En pareil cas, pour attribuer une cote de risque finale à ces ententes, l'IFF doit évaluer le risque en tenant compte des risques inhérents, des mesures de contrôle et d'atténuation et d'autres facteurs.

Parmi les mesures de contrôle et d'atténuation que l'IFF peut envisager, mentionnons l'élaboration de redondances, de solutions de contournement, de mesures de continuité des activités et d'autres mécanismes de résilience.

3.2. Entente avec un tiers quand le tiers est l'auditeur externe

Les ententes avec l'auditeur externe peuvent donner lieu à des conflits d'intérêts.

3.2.1. Les auditeurs externes respectent les normes d'indépendance lorsqu'ils fournissent des services à titre de tiers

Avant d'obtenir des services de conseil en gestion de la part de son auditeur externe, l'IFF doit s'assurer que ce dernier se conformera aux normes de la profession comptable canadienne sur l'indépendance des auditeurs ainsi qu'à toute autre exigence applicable en matière d'indépendance des auditeurs en ce qui a trait aux services devant être rendus par l'auditeur externe.

3.2.2. L'IFF n'obtient pas de services actuariels ou d'audit interne de son auditeur externe, sauf sous certaines conditions

À moins qu'il ne soit raisonnable de conclure que les résultats du service ne seront pas visés par l'audit des états financiers de l'IFF, cette dernière ne doit pas obtenir les services suivants de son auditeur externe :

- Tout service actuariel¹⁵.
- Tout service d'audit interne lié aux contrôles comptables internes, aux systèmes financiers ou aux états financiers de l'IFF. Cela n'empêche pas l'auditeur externe de fournir un service ponctuel pour évaluer un poste ou un programme distinct si le service ne correspond pas essentiellement à l'impartition d'une fonction d'audit interne.

4. Risque lié aux technologies et cyberrisque découlant des ententes avec les tiers

Le BSIF est conscient que le risque lié aux technologies et le cyberrisque découlant des ententes avec les tiers représentent d'importants facteurs de vulnérabilité pour une IFF. En plus des attentes minimales formulées plus haut, l'IFF doit envisager de mettre en œuvre des mécanismes de contrôle supplémentaires pour gérer le risque lié aux technologies et le cyberrisque découlant de ses ententes avec des tiers.

4.1. Des rôles et responsabilités clairs sont définis à l'égard des mécanismes de contrôle du risque lié aux technologies et du cyberrisque

Conformément aux attentes énoncées plus haut, et réitérées à l'annexe 2, le fait de définir des rôles et responsabilités clairs entre l'IFF et le tiers est essentiel pour gérer le risque et réduire l'ambiguïté entre les parties. Au moment de définir les responsabilités afférentes à ces mécanismes de contrôle, l'IFF doit tenir compte du risque que présente l'entente et de l'importance relative de celle-ci. Au besoin, l'IFF doit décrire plus en détail les rôles, responsabilités et procédures qui s'appliquent à chaque partie lorsqu'il s'agit de gérer la configuration des produits et des systèmes.

4.2. Les tiers se conforment aux normes de l'IFF en matière de risque lié aux technologies et de cyberrisque

Si le risque et l'importance relative l'exigent, l'IFF doit établir des processus pour s'assurer que les tiers qui présentent des niveaux élevés de risque respectent les normes de l'IFF – ou les normes sectorielles établies – en matière d'atténuation du risque, particulièrement dans les domaines de la gestion de l'accès et des données (sécurité et protection)¹⁶.

4.3. Des exigences qui s'appliquent à l'infonuagique sont établies

L'IFF doit élaborer des exigences propres à l'infonuagique pour veiller à une adoption planifiée et stratégique de cette technologie. Ces exigences particulières doivent permettre d'optimiser l'interopérabilité tout en respectant la propension déclarée de l'IFF à prendre des risques. Elles doivent également renforcer les normes et contrôles existants de l'IFF, notamment au chapitre de la protection des données, de la gestion des clés cryptographiques et de la gestion des conteneurs.

Ces exigences doivent s'accompagner d'une gouvernance de l'infonuagique solide pour assurer une supervision et un suivi adéquats de la conformité aux pratiques de gestion du risque de l'IFF, de même qu'une concordance avec la stratégie technologique générale.

4.4. La transférabilité du nuage¹⁷ est prise en considération

En plus de planifier des stratégies de sortie judicieuses (voir la section 2.3.5), l'IFF doit tenir compte de la transférabilité lorsqu'elle conclut une entente avec un fournisseur de services d'infonuagique, et lors du processus de conception et de mise en œuvre de l'infonuagique.

L'IFF doit envisager des stratégies (p. ex., un environnement à nuages multiples) pour gagner en résilience et atténuer le risque de concentration lié aux fournisseurs de services d'infonuagique.

Annexe 1 – Exemples de facteurs à prendre en compte lors de la diligence raisonnable

Avant de conclure une entente (écrite ou non) avec un tiers, et en continu par la suite, l'IFF doit effectuer une diligence raisonnable. À tout le moins, la diligence raisonnable doit couvrir les facteurs non exhaustifs suivants :

- a. l'expérience, la compétence technique et la capacité du tiers à mettre en œuvre et à soutenir les activités qu'on lui a confiées, y compris, le cas échéant, l'expérience, la compétence technique et la capacité des sous-traitants importants;
- b. la solidité financière du tiers pour mener à bien son mandat, conformément à l'entente;
- c. la conformité du tiers aux lois, règles, règlements et consignes réglementaires applicables au Canada et dans d'autres territoires de compétence pertinents;

- d. le risque potentiel d'atteinte à la réputation qui est associé à la relation avec le tiers ou à ses services, y compris l'existence d'un litige, d'une enquête ou d'une plainte, récents ou en cours, contre le tiers;
- e. la solidité des programmes, des processus et des mesures de contrôle interne du tiers relatifs à la gestion du risque ainsi que le cadre applicable à la reddition des comptes (l'IFF doit déterminer si ceux-ci cadrent avec ses processus et contrôles de gestion du risque);
- f. la capacité du tiers à :
 - gérer le risque lié aux technologies et le cyberrisque conformément aux attentes énoncées dans la ligne directrice B-13 du BSIF intitulée *Gestion du risque lié aux technologies et du cyberrisque*;
 - fournir à l'IFF des renseignements suffisants et opportuns pour qu'elle puisse se conformer à ses exigences de déclaration en vertu du préavis du BSIF intitulé *Signalement des incidents liés à la technologie et à la cybersécurité*;
- g. la solidité des programmes de sécurité de l'information du tiers, y compris leur conformité aux programmes de l'IFF;
- h. l'évaluation de la capacité du tiers à fournir des services essentiels en cas d'interruption de service, d'après ses plans de continuité des activités et de reprise après sinistre, y compris la qualité de ces plans, et la fréquence et les résultats des essais;
- i. la dépendance du tiers à l'égard des sous-traitants, et sa capacité à les gérer;
- j. l'incidence de l'entente avec le tiers, y compris avec ses sous-traitants, sur le risque de concentration;
- k. le lieu à partir duquel le tiers et ses sous-traitants importants exercent leurs activités;
- l. la capacité et la facilité à remplacer le tiers par un autre tiers et les répercussions de cette substitution sur les activités de l'IFF;
- m. la transférabilité des applications et services fournis par le tiers à un autre tiers ou à l'IFF;
- n. la couverture d'assurance du tiers;
- o. les objectifs d'affaires, les politiques de ressources humaines, les philosophies de service et la culture d'entreprise du tiers, ainsi que leur concordance avec ceux de l'IFF;
- p. les risques d'ordre politique ou juridique potentiels liés au territoire de compétence du tiers ou de tout sous-traitant important.

Annexe 2 – Dispositions minimales des ententes avec des tiers

Cette annexe contient une liste non exhaustive de dispositions que les IFF devraient inclure dans des ententes signées avec des tiers (en les adaptant aux circonstances de l'entente) :

- a. **Nature et portée de l'entente** : Le contrat doit préciser la nature et la portée de l'entente, y compris les dispositions sur la fréquence, la teneur et les modalités des services en question, la durée du contrat et l'endroit à partir duquel les services sont fournis.
- b. **Rôles et responsabilités** : Le contrat doit clairement établir les rôles et les responsabilités de l'IFF et du tiers, et de tout sous-traitant important du tiers, y compris pour la gestion du risque lié aux technologies et du cyberrisque, et des mesures de contrôle y afférentes.
- c. **Recours à des sous-traitants** : Le contrat doit établir des paramètres pour le recours aux sous-traitants et exiger que le tiers avise l'IFF de toute impartition en sous-traitance afin que cette dernière puisse effectuer une diligence raisonnable, et évaluer et gérer le risque lié aux sous-traitants et toute incidence potentielle d'un changement de service.
- d. **Établissement des frais** : Le contrat doit définir la base de calcul des frais relatifs aux services fournis.

- e. **Mesures de rendement** : Le contrat doit contenir des mesures de rendement qui permettent à chaque partie de déterminer si les engagements qui y sont prévus sont respectés.
- f. **Propriété et accès** : Le contrat doit établir et indiquer à qui appartient chaque actif (intellectuel ou matériel) lié à l'entente avec le tiers, y compris les actifs générés ou acquis dans le cadre de l'entente. Le contrat doit également préciser si, et de quelle manière, le tiers peut utiliser les actifs de l'IFF (p. ex., les données, le matériel, les logiciels, la documentation des systèmes ou la propriété intellectuelle), y compris les utilisateurs autorisés ainsi que le droit d'accès de l'IFF à ces actifs.
- g. **Sécurité des documents et des données** : Le contrat doit régir la confidentialité, l'intégrité, la sécurité et la disponibilité des documents et des données.
- h. **Avis à l'IFF** : Le contrat doit stipuler que le tiers est tenu d'informer l'IFF de ce qui suit :
- i. les incidents ou événements (chez le tiers ou un sous-traitant) qui ont eu ou qui pourraient avoir une incidence sur les services fournis, les clients ou données de l'IFF, ou la réputation de l'IFF;
 - ii. les incidents liés à la technologie et les cyberincidents (chez le tiers ou un sous-traitant) afin de permettre à l'IFF de se conformer à ses exigences de déclaration en vertu du préavis du BSIF intitulé **Signalement des incidents liés à la technologie et à la cybersécurité**;
 - iii. d'importants changements organisationnels ou opérationnels.
- i. **Règlement des différends** : Le contrat doit prévoir un protocole de règlement des différends. Il doit également préciser si le tiers doit continuer d'assurer le service en situation de différend et pendant la période de règlement de celui-ci, de même que l'instance, les lois et les règles qui régiront le règlement du différend.
- j. **Conformité à la réglementation** : Le contrat doit permettre à l'IFF de se conformer à toutes les exigences législatives et réglementaires applicables, y compris, sans s'y limiter, l'emplacement des documents et la confidentialité des renseignements sur les clients.
- k. **Continuité des activités et reprise après sinistre** : Le contrat doit stipuler que le tiers est tenu d'exposer les mesures visant à assurer la continuité des activités en cas d'interruption de service, y compris les attentes en matière d'essais et de rapports et les exigences d'atténuation, ainsi que les exigences applicables au tiers relativement au suivi et à la gestion du risque lié aux technologies et du cyberrisque.
- l. **Défaut et résiliation** : Le contrat doit préciser ce qui constitue un défaut ou un droit de résiliation, indiquer les mesures correctives possibles et permettre de corriger un défaut ou de résilier l'entente. La résiliation doit faire l'objet d'un préavis suffisant et, le cas échéant, les actifs de l'IFF doivent être retournés en temps opportun. Les données et les documents doivent être remis à l'IFF de manière à ce que cette dernière puisse poursuivre ses activités sans engager de frais excessifs.
- Le libellé du contrat ne doit pas empêcher le BSIF, ou toute autre autorité de résolution ou régime d'indemnisation financière, de s'acquitter de leur mandat en période de tensions ou de résolution. Par exemple, le contrat doit, entre autres, rester valide et exécutoire pendant le processus de résolution, à condition que les obligations de paiement soient respectées.
- m. **Assurance** : Le contrat doit stipuler qu'il incombe au tiers d'obtenir et de maintenir une assurance appropriée, de même que d'en communiquer les conditions générales. Il doit aussi stipuler qu'il incombe au tiers d'informer l'IFF en cas de changements importants dans la couverture d'assurance.
- n. **Gestion prudente des risques** : Le contrat doit inclure toute disposition supplémentaire nécessaire pour que l'IFF gère prudemment ses risques conformément à la présente ligne directrice.

-
- 1** Conformément aux exigences afférentes aux renseignements relatifs à la supervision énoncées dans la *[Loi sur les banques](#)*, la *[Loi sur les sociétés d'assurances](#)* et la *[Loi sur les sociétés de fiducie et de prêt](#)*.
 - 2** Les « succursales de banques étrangères » sont des banques étrangères autorisées à exercer leurs activités au Canada par l'exploitation de succursales en vertu de la partie XII.1 de la *Loi sur les banques*. Les « succursales de sociétés d'assurance étrangères » sont des entités étrangères qui sont autorisées à garantir au Canada des risques par l'exploitation de succursales en vertu de la partie XIII de la *Loi sur les sociétés d'assurances*.
 - 3** Une activité, une fonction ou un service imparti est une activité, une fonction ou un service qui est, ou pourrait être, entrepris par l'IFF elle-même, et est un type d'entente avec un tiers.
 - 4** Pour plus de clarté, les attentes en matière de gestion du risque lié aux tiers qui sont énoncées dans la présente ligne directrice ne sont pas destinées à remplacer les activités applicables de gestion du risque de crédit de contrepartie et du risque de marché appliquées aux infrastructures de marchés financiers, mais plutôt à servir de complément à celles-ci.
 - 5** Le BSIF tient compte du fait qu'un cadre approuvé à l'échelle fédérale sera élaboré pour régir la mobilité des données des consommateurs au sein du secteur financier. La présente ligne directrice n'a pas pour but d'empêcher la mise en place ou le fonctionnement d'un tel cadre. Une fois que le cadre aura été conçu, le BSIF pourra fournir des consignes pertinentes au besoin.
 - 6** Dans le présent document, le terme « sous-traitant » fait référence de manière générale à la chaîne d'approvisionnement du tiers.
 - 7** Dans les cas où il y a un échange de données entre l'IFF et un tiers, ou lorsque le tiers a accès aux systèmes de l'IFF, une corruption et une fuite de données peuvent se produire dans les locaux du tiers, de l'IFF ou pendant que les données sont en transit.
 - 8** Voir l'article 238 de la *Loi sur les banques*, l'article 261 de la *Loi sur les sociétés d'assurances* et l'article 243 de la *Loi sur les sociétés de fiducie et de prêt*.
 - 9** Les documents qui sont modifiés à une fréquence moindre que quotidienne sont réputés exacts jusqu'à ce qu'un changement y soit apporté. Par conséquent, les documents doivent être actualisés chaque jour ou selon la fréquence des changements qui leur sont apportés.
 - 10** Voir le paragraphe 239(1) de la *Loi sur les banques*, le paragraphe 262(1) de la *Loi sur les sociétés d'assurances* et le paragraphe 244(1) de la *Loi sur les sociétés de fiducie et de prêt*.
 - 11** Voir le paragraphe 239(3.1) de la *Loi sur les banques*, le paragraphe 262(3.1) de la *Loi sur les sociétés d'assurances* et le paragraphe 244(3.1) de la *Loi sur les sociétés de fiducie et de prêt*.
 - 12** Voir les sections 2.3.2.1 et 2.3.2.2 de la présente ligne directrice.
 - 13** L'acceptation d'un risque renvoie à la décision d'accepter un risque qui a été recensé sans aucune mesure d'atténuation ou sans prendre de mesures d'atténuation supplémentaires.
 - 14** Il est toujours préférable que l'entente soit documentée dans un contrat, mais le BSIF reconnaît qu'il peut y avoir des situations où il est difficile d'obtenir un contrat.

- 15** À cette fin, les services actuariels ont trait à la détermination d'un montant à inscrire dans les états financiers de l'IFF ou à des travaux normalement effectués par son actuaire désigné. Ils ne comprennent pas les services qui consistent à aider l'IFF à comprendre les méthodes, les modèles, les hypothèses et les intrants utilisés ou à conseiller la direction sur les méthodes et les hypothèses actuarielles appropriées qui seront utilisées. Conformément à la ligne directrice E-15, *Actuaire désigné : Dispositions législatives, qualifications et examen par des pairs*, l'IFF peut confier à un actuaire de son cabinet d'audit externe l'examen externe des travaux et rapports de l'actuaire désigné.
- 16** Consulter la ligne directrice B-13, *Gestion du risque lié aux technologies et du cyberrisque* pour connaître les attentes du BSIF en matière de gestion de ces types de risque par les IFF.
- 17** La deuxième version de la publication spéciale du National Institute of Standards and Technology (NIST) *NIST-SP 500-291 – NIST Cloud Computing Standards Roadmap* (feuille de route des normes du NIST en matière d'infonuagique) définit la transférabilité comme la capacité à transférer des données d'un système d'infonuagique à un autre, ou à transférer et à exécuter des applications dans différents systèmes d'infonuagique à un coût acceptable.
-

Date de modification : 2022-07-19