Ligne directrice

Objet : Gestion du risque lié aux tiers

Catégorie : Saines pratiques commerciales et limites prudentielles

Nº : B-10 Date : Avril 2023

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, offrir des services ou obtenir des biens à l'appui de leurs propres opérations ou de leur stratégie commerciale.

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

Le Bureau du surintendant des institutions financières (BSIF) s'attend à ce que l'IFF gère efficacement les risques associés à toute entente avec un tiers, et souligne que l'IFF demeure responsable de l'ensemble des activités, fonctions et services impartis à un tiers.

À cette fin, les IFF doivent fournir au BSIF, à la demande de celui-ci, des renseignements relatifs aux ententes commerciales et stratégiques qu'elles ont conclues avec des tiers, à la gestion du risque et aux environnements de contrôle, et ce, afin d'appuyer les activités de surveillance et de supervision[1]. Le BSIF s'attend à être informé rapidement des lacunes importantes qui viennent menacer la capacité de l'IFF à effectuer des activités essentielles en raison d'une entente avec un tiers.

Quoiqu'il en soit, les pouvoirs de surveillance du BSIF ne doivent être, en aucun cas, 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.

[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*.

Elle s'applique à toutes les IFF, à l'exclusion des succursales de banques étrangères et des succursales de sociétés d'assurance étrangères[2]. Les attentes du BSIF à l'égard des succursales de banques étrangères et des succursales de sociétés d'assurance étrangères sont énoncées dans la ligne directrice E-4, *Entités étrangères exploitant une succursale au Canada*.

A2. Application de la ligne directrice

Les ententes des IFF avec des tiers revêtent plusieurs formes; elles peuvent couvrir des services essentiels pour l'IFF, des services de soutien secondaires ou des accords stratégiques où aucun service n'est réellement fourni, par exemple. Le BSIF s'attend à ce que les IFF tiennent compte du risque et de la criticité lorsqu'elles examinent les ententes avec des tiers, et ce, dans le but de déterminer le degré de rigueur à appliquer quant aux attentes énoncées dans la présente ligne directrice. Par exemple, un plan de sortie ou d'urgence ne sera peut-être pas nécessaire pour une entente à faible risque, pas plus que le risque lié à la sous-traitance ne sera un facteur important dans la gestion de toute entente avec un tiers. De même, il ne sera peut-être pas nécessaire de soumettre une entente à faible risque et de courte durée à un examen juridique.

Afin d'appliquer la présente ligne directrice de manière prudente, il est essentiel de cerner le type et le niveau de risque découlant de chaque entente avec un tiers (y compris les ententes de sous-traitance) pour que l'IFF puisse gérer chaque entente avec un tiers avec le degré d'intensité approprié.

Par conséquent, le BSIF s'attend à ce que l'IFF soit consciente du risque et la criticité de toutes ses ententes avec des tiers et qu'elle applique la présente ligne directrice en fonction :

- du risque et de la criticité caractérisant chaque entente avec un tiers;
- de sa taille, de sa nature, de sa portée, de la complexité de ses activités et de son profil de risque.

Le BSIF reconnaît que les contrats avec des tiers ne sont pas tous négociables et que certaines ententes avec des tiers ne font peut-être pas l'objet d'un contrat. La section 3.1 a donc été ajoutée à la présente ligne directrice pour tenir compte de ces situations. Même si la possibilité de gérer le risque lié aux tiers par l'entremise des modalités d'un contrat peut être limitée dans ces cas, le BSIF s'attend néanmoins à ce que l'IFF gère le risque en misant sur le suivi, des mesures de continuité des activités, la planification d'urgence et d'autres mécanismes de résilience, le cas échéant.

A3. Définitions

Selon le National Institute of Standards and Technology (NIST) des États-Unis, la « **transférabilité infonuagique** » s'entend de [TRADUCTION] « la capacité de faire passer des

[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*.

données d'un système de nuage à un autre ou d'installer et d'exploiter des applications sur différents systèmes de nuage à un coût acceptable[3]. »

Le « **risque de concentration** » revêt deux formes. Le *risque de concentration propre à l'institution* s'entend du risque de perte ou de préjudice pour l'IFF résultant du recours excessif à un seul tiers, sous-traitant ou territoire pour de multiples activités. Le *risque de concentration systémique* découle du fait de concentrer la prestation de services à plusieurs IFF sur un tiers ou un territoire[4].

Un « **plan d'urgence** » comporte une série de mesures à prendre par l'IFF afin de poursuivre ses activités essentielles en cas d'interruption imprévue chez un tiers très important.

La « **criticité** » dénote l'importance pour les activités, la stratégie, la situation financière ou la réputation de l'IFF. Elle souligne les répercussions d'un événement générateur de risque sans égard à la probabilité d'occurrence. La criticité d'une entente est un facteur important dans l'évaluation du risque lié à cette dernière. Une entente est critique si elle prévoit la fourniture de produits ou la prestation d'activités commerciales, de fonctions et de services dont l'interruption pourrait mettre en péril la poursuite des activités, la sécurité ou la solidité de l'IFF qui en bénéficie ou son rôle au sein du système financier, menaçant ainsi sa résilience opérationnelle[5].

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

Un « **plan de sortie** » comporte une série de mesures à prendre par l'IFF en cas de retrait prévu (c.-à-d. sans situation de crise) ou imprévu (c.-à-d. en situation de crise) d'une entente avec un tiers, de même que des seuils de déclenchement du plan dans un cas comme dans l'autre. Voir la section 2.3.5 pour de plus amples renseignements.

L'« **acceptation du risque** » s'entend d'une décision d'accepter un risque identifié et de ne prendre aucune mesure d'atténuation, additionnelle ou non.

Un « **sous-traitant** » est une entité faisant partie de la chaîne contractuelle, des accords externes ou de la chaîne d'approvisionnement du tiers.

Le « **risque lié à la sous-traitance** » découle des ententes commerciales ou stratégiques établies par le tiers, par contrat ou autrement, avec des entités ou des particuliers.

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, à l'exclusion des

[3] 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).
[4] Dans le cas du risque de concentration systémique, l'IFF doit chercher à le comprendre dans toute la mesure possible.
[5] Voir les *Définitions clés liées à la résilience opérationnelle* du BSIF.

ententes avec les clients des IFF (p. ex., les déposants et les titulaires de polices) et des contrats d'emploi, qui sont exclus de cette définition.

Les ententes avec des tiers comprennent notamment :

- les activités, fonctions et services impartis qui, autrement, seraient entrepris par l'IFF elle-même;
- le recours à des experts-conseils professionnels indépendants;
- les courtiers (p. ex., les courtiers hypothécaires, les courtiers d'assurance et les courtiers en dépôt);
- les services publics (p. ex., les sources d'énergie, les télécommunications);
- les infrastructures de marchés financiers[6] (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 produits et 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)[7].

Le « **risque lié aux tiers** » est le risque pour l'IFF découlant du fait qu'un tiers ne fournit pas convenablement les biens, les activités commerciales, les fonctions et les services, ne protège pas adéquatement les données ou les systèmes, ou expose autrement l'IFF à des conséquences défavorables. Les scénarios de risques liés à un tiers pourraient inclure, sans s'y limiter, les cas suivants :

- l'insolvabilité du tiers;
- une interruption des opérations 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);
- les risques d'ordre politique, géographique, juridique, environnemental ou autres qui empêchent le tiers de fournir des services conformément à son entente avec l'IFF;
- l'insolvabilité ou l'interruption de service d'un sous-traitant;
- les risques découlant de l'interconnexion entre plusieurs tiers et plusieurs IFF;
- la corruption ou la fuite de données de l'IFF[8];

[6] 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.

[7] 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.

[8] 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.

- la perte de données par le tiers.

A4. Résultats

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

1. **Les structures de gouvernance et de responsabilité sont claires; des stratégies et cadres exhaustifs de gestion du risque sont en place.**
2. **L'IFF cerne et évalue les risques posés par les tiers.**
3. **L'IFF gère et atténue les risques posés par les tiers conformément à son cadre de gestion de la propension à prendre des risques.**
4. **Le rendement des tiers est suivi et évalué; on gère les risques et les incidents par anticipation.**
5. **Le programme de gestion du risque lié aux tiers de l'IFF permet à cette dernière de cerner et de gérer en continu une gamme de relations avec des tiers.**
6. **Les activités liées aux technologies et au cyberrisque menées par des tiers sont transparentes, fiables et sécurisées.**

A5. 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

1. Gouvernance

Résultat : ***Les structures de gouvernance et de responsabilité sont claires; des stratégies et cadres exhaustifs de gestion du risque sont en place.***

1.1 Responsabilités

Principe nº 1 : L'IFF est l'ultime responsable de la gestion du risque découlant de tous les types d'ententes avec des tiers.

1.1.1 L'IFF demeure responsable des services impartis à des tiers et gère les risques liés aux ententes 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 des activités, fonctions et services impartis à des tiers, des données échangées avec eux ou des données auxquelles ils ont accès, ainsi que de la gestion du risque 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 des tiers sont conformes à la propension de l'institution à prendre des risques et qu'elles sont gérées proportionnellement au niveau de criticité et de risque de 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 nº 2 : L'IFF doit établir un cadre de gestion du risque lié aux tiers qui définit clairement les responsabilités, les fonctions, 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 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.

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 de façon périodique pour veiller à ce qu'il soit pertinent et approprié, et à ce qu'elle y apporte continuellement 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 établit des responsabilités, des politiques et des processus pour cerner, suivre et gérer le risque lié aux tiers y compris, au besoin :

- les différentes responsabilités dans la gestion du risque lié aux tiers, y compris celles afférentes aux fonctions de supervision;
- des rôles et responsabilités clairs en matière de supervision et de gestion des ententes avec des 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 la criticité des ententes avec des tiers;
- des politiques pour gérer le risque lié aux tiers, qui sont approuvées, régulièrement révisées et mises 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 :
    - un répertoire des tiers selon le niveau de risque et la criticité;
    - 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;
    - les risques liés aux tiers découlant des différentes ententes (y compris le risque lié aux technologies, le cyberrisque, le risque lié à la sécurité de l'information, le risque de concentration, le risque lié à la gestion de la continuité des activités, le risque stratégique et le risque financier);
    - l'exposition globale au risque lié aux tiers et les tendances en la matière, afin d'éclairer le profil de risque actuel et émergent de l'IFF.

2. 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 des 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 criticité plus élevés à une évaluation plus fréquente et plus rigoureuse de même qu'à une gestion plus robuste du risque.

Dans le cas des ententes critiques 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 afin de déterminer avec précision le risque que pose chacune de ces ententes. L'institution doit revoir les critères d'évaluation périodiquement afin de s'assurer qu'ils restent adaptés au paysage du risque.

La criticité est une variable clé de l'évaluation du risque et peut être utilisée pour adapter les évaluations du risque. Afin de déterminer le niveau de criticité, l'IFF doit tenir compte, le cas échéant :

- de la gravité de la perte ou du préjudice qu'elle subirait si le tiers ou le sous-traitant ne répond pas aux attentes en raison de son insolvabilité ou de l'interruption de ses activités;
- de la possibilité de remplacer le tiers, y compris la transférabilité des services et la rapidité de leur transfert;
- de la mesure dans laquelle le tiers ou le sous-traitant assure le soutien d'une activité essentielle de l'IFF;
- de 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.

2.1.2 Le niveau de risque des ententes avec des tiers est évalué

Pour déterminer le niveau de risque, l'IFF doit tenir compte, le cas échéant :

- de la probabilité que le tiers ou le sous-traitant ne réponde pas aux attentes en raison de son insolvabilité ou de l'interruption de ses activités;
- de la capacité de l'IFF d'évaluer les contrôles du tiers et de continuer de respecter les exigences réglementaires et législatives en lien avec les activités exécutées par le tiers, particulièrement lors de perturbations;
- de la santé financière du tiers et du risque d'obligation d'intervenir, c'est-à-dire que l'IFF est tenue de fournir un soutien financier au tiers;
- du recours du tiers à des sous-traitants et de la complexité de la chaîne d'approvisionnement;
- du degré de dépendance de l'IFF à l'égard de tiers dont le risque de concentration est élevé;
- des pratiques du tiers et de ses sous-traitants visant la gestion de l'information, les données, la cybersécurité et la protection de la vie privée;
- de tout autre risque financier et non financier pertinent lié au recours au tiers.

2.1.3 La rigueur des activités de gestion du risque correspond au niveau de risque et à la criticité

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

2.2 Détermination et évaluation du risque

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

Principe nº 3 : Avant de conclure une entente avec un tiers, et périodiquement par la suite, l'IFF doit déterminer et évaluer le risque que l'entente représente. L'évaluation du risque doit être proportionnelle à la criticité de l'entente. Plus précisément, l'IFF doit effectuer des évaluations du risque pour sélectionner les tiers, évaluer ou réévaluer le risque et la criticité de l'entente, et prévoir l'atténuation et la supervision adéquates du risque.

2.2.1 Évaluation du risque

2.2.1.1. **L'IFF évalue le risque et la criticité de l'entente tout au long de son cycle de vie.** Elle doit effectuer des évaluations pour chaque entente avec un tiers afin de déterminer le risque et la criticité de celle-ci, en tenant compte à la fois des risques que pose l'entente, de ceux qu'elle permet d'atténuer (p. ex., le recours à des fournisseurs de différents territoires réduirait le risque lié à la concentration géographique, mais accroîtrait les risques géopolitiques et juridiques) et des mesures d'atténuation du risque. Lorsqu'un tiers est soumis à la réglementation ou à la surveillance du gouvernement, l'IFF peut en tenir compte dans son évaluation du risque.

L'IFF effectue de telles évaluations du risque 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, y compris au moment du renouvellement, à une fréquence appropriée et selon une portée qui témoigne de la criticité de l'entente;
- chaque fois qu'il y a un changement substantiel 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 cadre avec la propension de l'IFF à prendre des risques (risques liés aux tiers et autres risques pertinents);
- documenter la criticité de l'entente;
- établir le niveau de risque de l'entente;

- élaborer un plan, prévoyant des mesures de suivi et d'atténuation d'une intensité appropriée, afin de gérer l'entente selon la propension de l'IFF à prendre des risques.

2.2.2 Diligence raisonnable

Principe nº 4 : L'IFF doit faire preuve de diligence raisonnable, et ce, avant de conclure des contrats ou d'autres formes d'ententes avec des tiers, et régulièrement par la suite, en fonction du niveau de risque et de criticité 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, notamment des processus documentés de signalement des risques aux échelons supérieurs, d'approbation et d'acceptation.

2.2.2.2. **La diligence raisonnable dont l'IFF fait preuve est proportionnelle au niveau de risque et de criticité.** L'IFF doit effectuer un contrôle de diligence raisonnable proportionnel au niveau de risque et de criticité 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 criticité, ou à chaque modification substantielle de l'entente avec le tiers, comme un changement apporté à sa nature ou une évolution de sa criticité.

Le contrôle de 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'égard des ententes critiques et à risque élevé 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 ayant une présence géographique à l'extérieur du Canada (ou avec des sous-traitants ayant une présence géographique à l'extérieur du Canada), l'IFF doit analyser les obligations légales des pays concernés, ainsi que les risques 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 et les sous-traitants ainsi que 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. Dans toute la mesure possible, l'IFF doit aussi évaluer le risque de concentration systémique.

2.2.4 Risque lié à la sous-traitance

Principe nº 5 : L'IFF est responsable de la détermination, du suivi et de la gestion des risques liés aux accords de sous-traitance conclus par ses tiers.

2.2.4.1. **Les risques engendrés par les pratiques de sous-traitance sont recensés et compris.** L'IFF doit évaluer les risques attribuables aux sous-traitants de tiers qui pourraient avoir une incidence sur l'institution.

Avant de conclure une entente avec un tiers, l'IFF doit recenser et comprendre les pratiques de sous-traitance de celui-ci, y compris :

- le nombre de sous-traitants et leur criticité;
- le caractère adéquat et la performance du programme de gestion du risque lié aux tiers du tiers lui-même, notamment l'assurance que les exigences importantes – qu'elles aient trait au rendement ou qu'elles soient d'ordre juridique ou réglementaire – cadrent avec le contrat conclu avec l'IFF;
- l'incidence des ententes de sous-traitance sur le risque de concentration de l'IFF (voir la section 2.2.3 ci-dessus).

2.2.4.2. **Suivre et gérer le risque lié à la sous-traitance.** L'IFF doit aussi s'assurer d'obtenir, régulièrement, des comptes rendus et des rapports pertinents sur le recours des tiers à des sous-traitants, et ce, afin de bien gérer le risque lié à la sous-traitance. Pour ce faire, selon le niveau de risque et la criticité des services fournis par le tiers, l'IFF peut inclure des dispositions contractuelles :

- qui interdisent le recours à des sous-traitants pour certaines fonctions;
- qui exigent qu'elle soit informée, par écrit et sans tarder, lorsqu'un sous-traitant est engagé, ou remplacé, pour exécuter certaines des fonctions confiées par contrat au tiers;
- qui lui réservent le droit de refuser le recours à un sous-traitant;
- qui lui permettent d'exiger ou de réaliser un audit du sous-traitant.

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 écrits

Principe nº 6 : L'IFF doit conclure des accords écrits qui définissent les droits, les obligations 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., 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. Le BSIF s'attend à ce que l'IFF inclue, dans les contrats écrits portant sur les ententes critiques et à risque élevé, les dispositions énoncées à l'annexe 2 de la présente ligne directrice[9].

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

Principe nº 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 brèche de sécurité des données;
- les exigences de signalement en cas d'une brèche de sécurité des données.

[9] Sauf pour les contrats visés par la section 3.

Le cas échéant, les contrats doivent également préciser que les documents et données de l'IFF doivent être constamment séparés de ceux des autres clients, y compris durant leur transfert ou dans des conditions défavorables (p. ex., interruption de service). Les données et les documents doivent être soumis aux mêmes normes de protection, en fonction du niveau de risque, qu'ils soient conservés par le tiers ou par 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) prévoient des exigences relatives à certains documents que les IFF doivent préparer et tenir à jour[10]. Le BSIF s'attend à ce que les documents soient mis à jour et renferment des données exactes à la fin de chaque jour ouvrable (les documents qui sont modifiés à une fréquence moindre que quotidienne sont réputés être exacts jusqu'à ce qu'un changement y soit apporté), 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 documents électroniques reproduits ne soient pas suffisants aux fins d'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 exemplaires complets doivent être conservés sur un serveur situé aux endroits prévus par les lois régissant les IFF[11].

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'étranger[12].

[10] 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*.
[11] 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*.
[12] 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*.

2.3.3 Droits à l'information et audit

Principe nº 8 : Les ententes conclues par l'IFF avec des tiers doivent permettre à celle-ci d'obtenir rapidement des informations exactes et complètes qui l'aideront à superviser le rendement des tiers et les risques. L'IFF doit aussi avoir le droit de réaliser, elle-même ou en faisant appel à un auditeur indépendant, un audit du tiers.

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 d'évaluer si les indicateurs de rendement sont respectés et de disposer de tout autre renseignement nécessaire à son programme de contrôle, 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 substantielle sur l'IFF.** Le contrat doit contenir des exigences et des procédures garantissant que le tiers signale à l'IFF, dans les meilleurs délais, les événements susceptibles d'avoir une incidence substantielle sur les risques et la prestation des services.

2.3.3.3. **Le rendement des services 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 tests

Principe nº 9 : Le contrat entre l'IFF et le tiers doit prévoir des dispositions afin d'assurer les opérations en cas d'interruption de service, notamment la tenue à jour, les tests 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 critiques avec des tiers.

2.3.4.1. **Les capacités des tiers à assurer la continuité des activités et la reprise après sinistre sont définies et contrôlées.** 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 tests;
- remédier à toute déficience substantielle.

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), y compris les interruptions prolongées ou simultanées, dans lesquelles le tiers risquerait de ne plus pouvoir fournir le service;
- documenter des processus et systèmes de sauvegarde et des capacités de redondance qui sont proportionnels à la criticité du service fourni;
- garantir que l'IFF a en sa possession, en cas d'interruption des services du tiers, tous les rapports 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 facilement[13].

S'il y a lieu, le tiers et l'IFF devraient envisager de concevoir et de tester conjointement les plans de continuité des activités et les plans de reprise après sinistre, en fonction de la criticité du service.

2.3.5 Stratégie et planification de mesures d'urgence et de sortie

2.3.5.1. **Des stratégies d'urgence et de sortie sont mises au point afin d'assurer la continuité des services essentiels.** L'IFF doit établir des plans d'urgence et de sortie proportionnels au niveau de risque et de criticité de chaque entente avec un tiers, et ce, afin de veiller à la continuité des activités de l'IFF en temps normal et en situation de crise. L'IFF doit inclure les éléments suivants dans ses plans documentés pour les ententes critiques ou à risque élevé, et envisager de les intégrer à ses plans visant les ententes à risque plus faible ou moins critiques :

- les éléments qui déclenchent l'activation des plans de sortie ou d'urgence;
- les activités à réaliser afin d'assurer le maintien des activités essentielles en cas d'interruption ou lors d'une sortie dans des circonstances imprévues, comme la défaillance ou l'insolvabilité du fournisseur de services (un « guide » pour une sortie en situation de crise);
- les 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);
- des renvois aux dispositions contractuelles pouvant avoir une incidence sur la sortie, telles que les modalités de notification et les dispositions obligeant le tiers à fournir des services pendant une période prescrite après la notification de la sortie;
- suffisamment de détails (p. ex., d'autres options ou fournisseurs, avec des échéanciers, des coûts, des ressources, l'incidence sur les revenus et des solutions de contournement provisoires) pour permettre une exécution rapide;

[13] Voir les sections 2.3.2.1 et 2.3.2.2 de la présente ligne directrice.

- des plans documentés afin de réagir à des scénarios graves, mais vraisemblables, y compris des interruptions prolongées ou multiples.

Les plans d'urgence et les stratégies de sortie doivent être réévalués et révisés régulièrement, et plus fréquemment lors de changements substantiels dans les ententes avec des tiers.

2.4 Suivi et reddition de comptes

Résultat : ***Le rendement des tiers est suivi et évalué; on gère les risques et les incidents par anticipation.***

Principe nº 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 tiers fournisseur

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 inclure une surveillance régulière des risques actuels et émergents, des acceptations des risques et de la conformité de l'entente avec le tiers à l'égard des politiques et procédures de l'IFF en matière de risque et des attentes du BSIF. Le suivi doit porter sur l'entente en elle-même, mais aussi sur l'unité opérationnelle, le segment, la plateforme et l'entreprise dans son ensemble. L'étendue et la fréquence du suivi doivent être proportionnelles au niveau de risque et à la criticité de l'entente avec le tiers.

2.4.1.2. **Les indicateurs confirment que le risque résiduel ne dépasse pas 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 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 nº 11 *:* L'IFF et le tiers doivent mettre en place des processus documentés qui permettent de détecter, enquêter, signaler, suivre et résoudre efficacement les incidents afin de s'assurer que les niveaux de risque ne dépassent pas 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 détecter 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 avoir des effets, directs ou indirects, sur la capacité du tiers à fournir les biens, les activités commerciales, les fonctions 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 a mis en place un processus interne de gestion des incidents bien défini.** L'IFF doit avoir des processus internes clairement définis qui permettent, d'une part, d'assurer la gestion efficace des incidents survenus chez les tiers et leur signalement aux échelons supérieurs et, d'autre part, d'effectuer, a posteriori, un suivi
des mesures correctives. Les processus établis doivent définir clairement, à tous les niveaux de l'IFF, les responsabilités et les conditions qui déclencheraient le signalement aux échelons supérieurs 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 et adéquates, l'IFF doit demander au tiers d'effectuer une analyse des causes fondamentales de tout incident, en fonction de sa gravité et de son incidence potentielle sur l'IFF, et de lui communiquer les résultats. 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 lié aux tiers de l'IFF permet à cette dernière de cerner et de gérer, en continu, un éventail de relations avec des tiers.***

3.1 Contrats d'adhésion

Les contrats d'adhésion sont ceux établis par des tiers qui prévoient des modalités prédéfinies, laissant peu de marge permettant à l'IFF de négocier et d'adapter ses propres modalités contractuelles. À titre d'exemple, citons les contrats avec les services publics, les fournisseurs de services Internet, les infrastructures de marchés financiers et d'autres.

3.1.1. **L'IFF gère le risque lié aux tiers avec lesquels elle a conclu des contrats d'adhésion.** Dans les situations où il faut recourir à un contrat d'adhésion, le BSIF s'attend à ce que le programme de gestion du risque lié aux tiers de l'IFF porte sur la relation. L'IFF doit évaluer le risque en tenant compte des risques inhérents, des mesures de contrôle qui visent à les atténuer ainsi que d'autres facteurs et, le cas échéant, accepter les risques que comportent les contrats d'adhésion.

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. Aucun contrat écrit

3.2.1. Les tiers avec lesquels il n'y a pas de contrat écrit posent tout de même des risques.

L'absence d'entente écrite, de contrat formel ou d'accord[14] ne signifie pas qu'il n'y a pas d'entente avec le tiers ou de risque lié à ce dernier. Même s'il est possible que l'IFF n'ait pas de relation directe avec l'ensemble des tiers avec lesquels elle interagit, le BSIF s'attend à ce que le programme de gestion du risque lié aux tiers de l'IFF couvre ces relations.

3.3 Entente avec un tiers quand celui-ci est l'auditeur externe

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

3.3.1. **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.

3.3.2. **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 actuariel[15].

[14] Il est toujours préférable de documenter l'entente au moyen d'un contrat; le BSIF reconnaît toutefois qu'il peut être difficile d'obtenir un contrat dans certaines circonstances.

[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.

- 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 des tiers

Résultat : ***Les activités liées aux technologies et au cyberrisque menées par des tiers sont transparentes, fiables et sécurisées.***

Le BSIF est conscient que le risque lié aux technologies et le cyberrisque découlant des ententes avec des tiers représentent d'importants facteurs de vulnérabilité pour une IFF. En plus des attentes 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 à la gestion du risque, assurer la reddition de comptes 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 la criticité de celle-ci. Au besoin, l'IFF doit détailler davantage les rôles, responsabilités et procédures qui s'appliquent à chaque partie lorsqu'il s'agit de gérer la configuration des actifs technologiques.

4.2 Les tiers se conforment aux normes de l'IFF en matière de risque lié aux technologies et de cyberrisque. Si le risque ou la criticité le requiert, l'IFF doit établir des processus afin de 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 des accès et des données (sécurité et protection)[16].

4.3 Les exigences s'appliquant 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.

[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.

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 infonuagique est prise en considération. En plus de planifier des stratégies de sortie adéquates (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 services infonuagiques. À cette fin, l'IFF doit évaluer les avantages et les risques de la transférabilité ainsi que des mesures d'atténuation en l'absence de transférabilité.

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 (voir la section 2.2.3).

Annexe 1 – Exemples de facteurs à prendre en compte dans le cadre du contrôle de diligence raisonnable

Avant de conclure une entente (écrite ou non) avec un tiers, et en continu par la suite, l'IFF doit effectuer un contrôle de diligence raisonnable proportionnel au risque et à la criticité de l'entente. Dans le cas, à tout le moins, de ses ententes critiques et à risque élevé, le contrôle de diligence raisonnable effectué par l'IFF 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;

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 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, récent 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 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 valeurs, les objectifs commerciaux, le code de conduite, les politiques connexes et la culture du tiers, ainsi que leur concordance avec ceux de l'IFF;

p) les risques d'ordre politique ou juridique liés au territoire de compétence du tiers ou des sous-traitants.

Annexe 2 – Dispositions des ententes avec des tiers

Cette annexe contient une liste non exhaustive de dispositions que les IFF devraient inclure dans des ententes critiques et à risque élevé conclues avec des tiers. Il convient d'envisager l'inclusion de ces dispositions aux ententes avec d'autres tiers, le cas échéant, en fonction du risque et de la criticité de ces ententes.

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, du tiers et des sous-traitants, 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 tout service imparti à un sous-traitant . L'IFF doit pouvoir effectuer un contrôle de diligence raisonnable afin d'évaluer les répercussions du 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. les changements de propriété du tiers;
iv. d'importants changements organisationnels ou opérationnels;
v. les cas de non-conformité substantielle avec les exigences réglementaires (c.-à-d. l'application de la réglementation) ou les litiges.

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 de tests et de rapports, et les mesures d'atténuation nécessaires, 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 couverture d'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.