5.2

Réglementation et lignes directrices

5.2 RÉGLEMENTATION ET LIGNES DIRECTRICES

5.2.1 Consultation

Ligne directrice sur la gestion du risque lié aux tiers

(*Loi sur les assureurs*, RLRQ, c. A-32.1, art. 463)
(*Loi sur les coopératives de services financiers*, RLRQ, c. C-67.3, art. 565.1)
(*Loi sur les institutions de dépôts et la protection des dépôts*, RLRQ, c. I-13.2.2, art. 42.2)
(*Loi sur les sociétés de fiducie et les sociétés d'épargne*, RLRQ, c. S-29.02, art. 254)

L'Autorité des marchés financiers (l'« AMF ») publie pour consultation le projet de *Ligne directrice sur la gestion du risque lié aux tiers* (la « ligne directrice »). Cette ligne directrice est applicable aux assureurs autorisés, aux coopératives de services financiers, aux sociétés de fiducie autorisées et aux institutions de dépôts autorisées.

Le projet de ligne directrice vise à favoriser une gestion saine et prudente du risque lié aux tiers et ultimement à rehausser la résilience des institutions financières.

Les personnes intéressées à soumettre leurs commentaires sont invitées à les fournir au plus tard le **19 décembre 2025**. Il est à noter que les commentaires seront rendus publics à défaut d'avis contraire de l'AMF à cet effet.

Le projet de ligne directrice est publié ci-après et est également accessible sur le site Web de l'AMF sous la rubrique « Consultations publiques » aux sections « Assurances et planification financière » et « Institutions de dépôts ».

Soumission des commentaires

Les commentaires doivent être soumis à :

Me Philippe Lebel
Secrétaire et directeur général des affaires juridiques Autorité des marchés financiers
Place de la Cité, tour PwC
2640, boulevard Laurier, bureau 400
Québec (Québec) G1V 5C1
Télécopieur : (514) 864-8381
consultation-en-cours@lautorite.qc.ca

Renseignements additionnels

Des renseignements additionnels peuvent être obtenus en s'adressant à :

Julie St-Laurent
Conseillère experte – Risques non-financiers
Direction de l'encadrement prudentiel et des simulations
Téléphone : (418) 525-0337, poste 4524
Numéro sans frais : 1 877 525-0337
julie.st-laurent@lautorite.qc.ca

Le 9 octobre 2025

Autorité des marchés financiers

PROJET

Octobre 2025

Ligne directrice sur la gestion du risque lié aux tiers

Table des matières

PROJET

1. Introduction

1.1 Environnement et évolution du risque

Les institutions financières[1] font affaire avec des tiers pour la fourniture de biens ou de services en lien avec la prestation de leurs services, leurs opérations ou encore leur stratégie commerciale. Le recours aux tiers et la dépendance envers ceux-ci ont considérablement augmenté en réponse à la transformation numérique et à l'évolution rapide des nouvelles technologies. Cette tendance devrait continuer de s'accentuer, considérant l'environnement en constante mouvance dans lequel évoluent les institutions.

Le recours aux tiers comporte de nombreux avantages, permettant par exemple de faire des gains en termes d'efficacité, de productivité ou de réduction de certains coûts. Cette pratique comporte toutefois des risques pour les institutions, les clients et le système financier en raison de l'absence de contrôle direct des institutions sur les activités qui font l'objet de ce type d'entente.

Les tiers peuvent à la fois amplifier les risques existants et exposer les institutions à de nouveaux risques. De plus, des tendances telles que la concentration des tiers et la complexification, voire l'opacité de la chaîne d'approvisionnement, peuvent, si un risque se matérialise, entraîner des conséquences importantes pour les institutions et leurs clients, allant jusqu'à affecter leur résilience opérationnelle. Pour cette raison, la saine gestion du risque lié aux tiers se veut un pilier de la résilience opérationnelle.

Le terme « risque lié aux tiers » désigne l'ensemble des risques qui découlent des ententes avec des tiers.

1.2 Les fondements de la ligne directrice

La ligne directrice sur la gestion du risque lié aux tiers s'inspire des principes et des orientations publiées notamment par le Comité de Bâle sur le contrôle bancaire (CBCB), l'Association internationale des contrôleurs d'assurance (AICA) ainsi que le Conseil de la stabilité financière (CSF).

Compte tenu de sa nature spécifique, cette ligne directrice s'appuie sur les attentes des lignes directrices formant l'assise de l'encadrement prudentiel[2] ainsi que d'autres lignes directrices plus génériques, notamment la *Ligne directrice sur les saines pratiques commerciales* ainsi que la *Ligne directrice sur la gestion du risque opérationnel*.

Les encadrements connexes, notamment la *Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications* et la *Ligne directrice sur la continuité des activités*, devraient être pris en considération.

PROJET

[1] Dans la présente ligne directrice, les termes « institution » et « institution financière » sont utilisés pour faire référence aux institutions financières visées à la section 1.3 – Champ d'application.

[2] Autorité des marchés financiers, *Ligne directrice sur la gouvernance*, avril 2021; Autorité des marchés financiers, *Ligne directrice sur la gestion intégrée des risques,* mai 2015; Autorité des marchés financiers, *Ligne directrice sur la conformité*, avril 2017.

1.3 Champ d'application

En vertu des pouvoirs habilitants[3] de l'Autorité, cette ligne directrice est applicable aux assureurs autorisés, aux coopératives de services financiers, aux sociétés de fiducie autorisées et aux institutions de dépôts autorisées.

1.4 Objectif

Cette ligne directrice énonce les attentes de l'Autorité à l'égard de la gestion du risque lié aux tiers, lequel contribue à renforcer la résilience opérationnelle des institutions financières.

1.5 Portée et mise en œuvre des attentes

Les attentes énoncées dans cette ligne directrice visent l'ensemble des ententes avec des tiers. Leur mise en œuvre devrait tenir compte de la criticité et du niveau de risque propre à chacune des ententes.

Les attentes ne visent pas à remplacer celles qui pourraient se trouver dans des lignes directrices visant des risques spécifiques.

L'Autorité rappelle que cette ligne directrice, tout comme l'ensemble de son encadrement prudentiel, est basée sur le principe de proportionnalité (taille, nature, complexité et profil de risque de l'institution financière)

2. Terminologie utilisée

Capacité d'un tiers

La capacité d'un tiers comprend l'ensemble des facteurs qualitatifs et quantitatifs pertinents au regard de la sélection d'un tiers.

Chaîne d'approvisionnement

Réseau d'entités ou de personnes qui fournissent des infrastructures, des biens, des services ou d'autres intrants utilisés directement ou indirectement pour la fourniture d'un produit ou d'un service à une institution financière en vertu d'une entente avec un tiers.

Criticité d'une entente avec un tiers

La criticité d'une entente qualifie l'importance de cette dernière. Elle reflète l'impact que pourrait avoir une perturbation, un ralentissement ou une interruption de la fourniture d'un produit ou d'un service sur l'institution financière et ses clients. À titre d'exemple, une entente pourrait être considérée comme critique si la perturbation, le ralentissement ou l'interruption sont susceptibles d'entraîner des répercussions importantes sur le fonctionnement de l'institution et/ou sur ses clients, particulièrement si l'entente vise un service commercial important.

[3] *Loi sur les assureurs*, RLRQ, c. A-32.1, art. 463 et 464; *Loi sur les coopératives de services financiers*, RLRQ, c. C-67.3, art. 565.1 et 566; *Loi sur les institutions de dépôts et la protection des dépôts*, RLRQ, c. I-13.2.2, art. 42.2 et 42.3; *Loi sur les sociétés de fiducie et les sociétés d'épargne*, RLRQ, c. S-29.02, art. 254 et 255.

Entente avec un tiers

Toute entente conclue par une institution financière avec une personne ou une autre entité juridique qui vise la fourniture de biens ou de services, qu'elle soit de nature commerciale ou stratégique.

Les ententes avec les tiers incluent notamment :

- les ententes d'impartition;
- le recours à des experts-conseils professionnels indépendants;
- les ententes intragroupes;
- les ententes de distribution;
- d'autres relations commerciales impliquant la fourniture de produits et de services, ou le stockage, l'utilisation ou l'échange de données[4];

Elles excluent :

- les ententes avec les clients (déposants, assurés, etc.);
- les contrats d'emploi.

Entente de distribution

Entente entre une institution financière et une personne qui distribue des produits et services financiers au sens de la *Loi sur la distribution de produits et services financiers*.

Impartition

Délégation à un tiers, sur une période définie, de l'exécution et de la gestion d'une fonction, d'une activité ou d'un processus, dont l'institution financière s'acquitte ou pourrait s'acquitter elle-même. L'impartition est un type d'entente avec un tiers.

Plan de sortie

Un plan de sortie comporte une série de mesures à prendre par l'institution en cas d'une terminaison prévue ou imprévue d'une entente avec un tiers.

Résilience opérationnelle

Capacité d'une institution financière à anticiper, se préparer, faire face et s'adapter aux perturbations dans un environnement changeant pour lui permettre de continuer à mener ses activités et de progresser.

Risque lié aux tiers

Risques auxquels est exposée une institution financière et/ou ses clients lorsqu'elle fait affaire avec un tiers. Le risque lié aux tiers désigne l'ensemble des risques qui découlent des ententes avec ces derniers.

Services commerciaux importants

Service clé offert aux clients, c'est-à-dire un service qui, s'il est perturbé, pourrait causer un préjudice important à ces derniers, menacer la viabilité, la solidité ou la sécurité d'une institution financière, ou encore poser atteinte à l'intégrité des marchés.

[4] Notamment les ententes visant des services infonuagiques ou encore des logiciels.

PROJET

Sous-traitant d'un tiers

Entité qui fait partie de la chaîne d'approvisionnement d'un tiers et qui appuie la fourniture de produits ou de services prévus dans le cadre d'une entente avec une institution financière.

Tiers intragroupe

Tiers qui fait partie du groupe d'une institution financière et qui fournit des produits ou services à des filiales de ce même groupe. Les tiers intragroupes sont ceux ayant un détenteur de leur contrôle commun. Ils peuvent inclure notamment la maison mère, une société de portefeuille, les entités sœurs ou toute autre entité affiliée à l'institution financière.

Tolérance aux perturbations

Niveau maximal de perturbation acceptable d'un service commercial important, au-delà duquel les clients, l'institution financière ou encore le système financier pourraient subir un préjudice important, possiblement irréparable, ou duquel il serait difficile de se remettre. De tels préjudices peuvent inclure des pertes financières, une perte d'accès prolongée à des services ou encore d'autres impacts non financiers, dont les fuites de renseignements personnels.

Les niveaux de tolérance peuvent être mesurés en fonction d'une durée de même qu'à l'aide d'autres indicateurs pertinents.

3. Les risques découlant des ententes avec des tiers

3.1 Risques généraux

Les risques qui découlent des ententes avec des tiers sont de diverses natures, allant du risque financier au risque opérationnel (incluant le risque lié aux données). Ces risques peuvent avoir des impacts importants autant sur l'institution que sur ses clients. Certains risques sont inhérents à l'activité ou au produit qui fait l'objet de l'entente, tandis que d'autres dépendent de la gestion des activités et des risques du tiers impliqué.

3.2 Risques spécifiques

Risque lié à la concentration des tiers

Le risque revêt deux formes :

- Le risque de concentration propre à l'institution découle de la dépendance de celle-ci à un nombre limité de tiers, de façon directe ou indirecte.

  Un risque de concentration au sein d'une même institution pourrait par exemple s'observer dans les situations suivantes :

  (i) la concentration de plusieurs produits ou services fournis par un même tiers dans un processus;

  (ii) la concentration de plusieurs produits ou services fournis par un même tiers au sein d'une même institution ;

PROJET

(iii) la concentration de produits ou de services d'un ou de plusieurs tiers provenant d'une même région géographique; ou

(iv) plusieurs tiers qui dépendent du même sous-traitant.

- Le risque de concentration systémique, quant à lui, découle de la dépendance de plusieurs institutions financières à un ou plusieurs produits ou services fournis auprès d'un seul tiers ou d'un nombre limité de tiers, directement ou indirectement par l'intermédiaire d'un sous-traitant, dont la perturbation ou la défaillance peut entraîner des répercussions systémiques.

Risque lié à la sous-traitance

Les tiers peuvent eux-mêmes recourir à des tierces parties afin d'appuyer la fourniture de produits ou de services prévus dans le cadre d'une entente avec une institution. Cette pratique peut complexifier, voire opacifier la chaîne d'approvisionnement.

La sous-traitance peut avoir un impact direct sur la gestion du risque lié aux tiers. Elle peut exacerber certains risques et accroître la dépendance envers des tiers, augmentant ainsi le risque de concentration.

4. Impact des ententes avec des tiers sur la résilience opérationnelle

La résilience opérationnelle et la gestion du risque lié aux tiers sont étroitement liées. En effet, le recours à des tiers peut affecter la capacité des institutions à anticiper, se préparer, répondre et s'adapter aux perturbations dans un environnement changeant pour leur permettre de continuer à mener leurs activités et à progresser. La matérialisation de certains risques découlant du recours à des tiers peut notamment affecter les activités critiques[5] et les services commerciaux importants, et entraîner des répercussions négatives significatives pour l'institution, ses clients, voire ultimement le système financier.

Considérant le lien entre les attentes de la présente ligne directrice et la résilience opérationnelle, certains concepts de résilience opérationnelle à prendre en considération dans la gestion du risque lié aux tiers y sont introduits.

5. Attentes en matière de gouvernance

L'Autorité s'attend à ce que l'institution financière mette en place une structure de gouvernance robuste permettant une saine gestion du risque lié aux tiers.

5.1 Rôles et responsabilités du conseil d'administration

Le conseil d'administration a la responsabilité ultime de la gestion du risque découlant des ententes avec les tiers. Ce dernier devrait obtenir l'assurance raisonnable que les pratiques sont arrimées à la stratégie de recours aux tiers et à l'appétit pour le risque lié aux tiers de l'institution.

[5] Autorité des marchés financiers, *Ligne directrice sur la gestion de la continuité des activités*, avril 2010.

En sus des attentes déjà émises par l'Autorité[6], le conseil d'administration devrait :

- approuver la stratégie de l'institution concernant le recours aux tiers. Celle-ci devrait être arrimée à l'appétit pour le risque et à la tolérance aux perturbations;
- approuver l'appétit pour le risque lié aux tiers de l'institution financière et les niveaux de tolérance pour l'ensemble de l'institution;
- veiller à ce que la haute direction développe et opérationnalise le cadre de gestion du risque lié aux tiers;
- approuver le cadre de gestion du risque lié aux tiers;
- veiller à ce que la haute direction produise une reddition de comptes périodique concernant la gestion du risque lié aux tiers;
- veiller à ce que la gestion du risque lié aux tiers soit intégrée dans l'ensemble de l'institution.

5.2 Rôles et responsabilités de la haute direction

En sus des attentes déjà émises par l'Autorité[7], la haute direction devrait :

- définir la stratégie de l'institution concernant le recours aux tiers;
- définir l'appétit pour le risque lié aux tiers de l'institution et les niveaux de tolérance pour l'ensemble de l'organisation;
- développer et opérationnaliser un cadre de gestion du risque lié aux tiers qui couvre l'ensemble du cycle de vie des ententes, et dans lequel les rôles et les responsabilités des intervenants sont clairement définis;
- produire une reddition de comptes périodique concernant la gestion du risque lié aux tiers;
- communiquer la stratégie et le cadre de gestion du risque lié aux tiers à l'ensemble des parties prenantes à l'interne et à l'externe;
- assurer le maintien, dans l'institution, d'une expertise et de programmes de formation et de sensibilisation adéquats sur la gestion du risque lié aux tiers;
- faire la promotion d'une saine gestion du risque lié aux tiers.

6. Appétit pour le risque

L'Autorité s'attend à ce que l'institution financière définisse son appétit pour le risque lié aux tiers et établisse des niveaux de tolérance pour en assurer l'opérationnalisation dans l'ensemble de l'organisation.

L'institution devrait définir son appétit pour le risque lié aux tiers, incluant les niveaux de tolérance, afin d'assurer une compréhension commune et exhaustive, dans l'ensemble de l'organisation, du niveau de

[6] Autorité des marchés financiers, *Ligne directrice sur la gouvernance*, avril 2021; Autorité des marchés financiers, *Ligne directrice sur la gestion intégrée des risques*, mai 2015

[7] Autorité des marchés financiers, *Ligne directrice sur la gouvernance*, avril 2021, Autorité des marchés financiers, *Ligne directrice sur la gestion intégrée des risques*, mai 2015.

risque qu'elle est prête à accepter. Ce dernier devrait découler de l'appétit plus global du risque opérationnel.

L'appétit devrait inclure des critères quantitatifs et qualitatifs, et prendre en considération l'ensemble des risques qui découlent des ententes avec des tiers, incluant les risques spécifiques, c'est-à-dire le risque de concentration et le risque lié à la sous-traitance. Comme certains risques qui découlent des ententes avec des tiers peuvent affecter la résilience opérationnelle, la tolérance aux perturbations causées par un tiers devrait également être considérée dans la définition de l'appétit.

L'appétit pour le risque et les niveaux de tolérance devraient être révisés régulièrement afin de refléter l'évolution du risque lié aux tiers et la stratégie de l'institution à cet égard. Il devrait demeurer pertinent et adéquat afin d'orienter les décisions.

7. Cadre de gestion du risque lié aux tiers

L'Autorité s'attend à ce que l'institution financière se dote d'un cadre de gestion du risque lié aux tiers qui couvre l'ensemble du cycle de vie d'une entente.

L'institution devrait mettre en place un cadre de gestion du risque lié aux tiers (le « cadre »). Ce dernier devrait notamment être arrimé au cadre plus global du risque opérationnel et tenir compte de l'appétit pour le risque et de la stratégie de recours aux tiers.

Le cadre devrait établir clairement les rôles et responsabilités en matière de gestion des ententes avec les tiers et de gestion du risque lié aux tiers, être exhaustif et couvrir l'ensemble du cycle de vie d'une entente. Il devrait inclure les politiques, les stratégies et les processus pour assurer une saine gestion du risque, c'est-à-dire l'identification, l'évaluation, le contrôle, l'atténuation et la communication de l'ensemble des risques découlant des ententes avec des tiers.

L'institution devrait mettre à jour le cadre régulièrement afin de s'assurer qu'il demeure pertinent et approprié. Le cadre devrait refléter l'évolution de l'environnement interne et externe et les bonnes pratiques en matière de gestion de risques.

8. Attentes en matière de gestion du risque lié aux tiers

La gestion du risque lié aux tiers comprend différentes étapes qui suivent le cycle de vie d'une entente avec un tiers. Le schéma qui suit illustre ces étapes.

Les attentes en matière de gestion des risques sont présentées ci-après en fonction de ces étapes.

PROJET

8.1. Gestion du risque selon la criticité et le niveau de risque d'une entente

L'Autorité s'attend à ce que l'institution financière gère le risque lié aux tiers tout au long du cycle de vie d'une entente, et ce, proportionnellement à la criticité et au niveau de risque de celle-ci.

L'institution devrait gérer le risque lié aux tiers proportionnellement à la criticité et au niveau de risque de chacune des ententes. Celles qui présentent une criticité ou un niveau de risque élevé devraient être soumises à une réévaluation plus fréquente et plus exhaustive de même qu'à une gestion plus robuste du risque.

8.2. Identification et évaluation des risques liés à une entente envisagée

L'Autorité s'attend à ce que l'institution financière détermine la criticité de toute entente envisagée avec un tiers et évalue les risques qui en découlent en fonction de critères formalisés.

L'institution qui envisage d'avoir recours à un tiers devrait évaluer la criticité d'une entente envisagée, c'est-à-dire celle du produit ou du service pour lequel elle envisage avoir recours à un tiers. Elle devrait également évaluer les risques inhérents à l'entente, et ce, avant même l'étape de la sélection du tiers.

À cette fin, l'institution devrait se doter de critères exhaustifs et formalisés. Elle devrait revoir ces critères régulièrement afin de s'assurer qu'ils demeurent pertinents, c'est-à-dire qu'ils reflètent l'évolution de l'environnement de risque et les changements propres à l'institution.

Comme la gestion du risque devrait être proportionnelle à la criticité et au niveau de risque d'une entente avec un tiers, l'institution devrait faire ces évaluations pour chacune des ententes envisagées.

8.2.1. Évaluation de la criticité d'une entente

Pour évaluer la criticité d'une entente envisagée, l'institution pourrait par exemple considérer des critères tels que :

- l'importance financière ou stratégique de l'entente;
- la nature et la complexité du produit ou du service qui fera l'objet de l'entente;
- la criticité du processus visé par l'entente (par exemple, s'il s'agit d'un processus commercial important);
- la tolérance aux perturbations de l'institution en lien avec le produit ou le service visé par l'entente;
- la nature et la sensibilité des données ou des informations à partager avec le tiers;
- les systèmes à partager avec le tiers;
- la possibilité de remplacer le tiers, y compris la transférabilité des services et la rapidité de leur transfert.

PROJET

8.2.2. Évaluation des risques inhérents

L'institution devrait évaluer l'ensemble des risques que pose une entente envisagée avec un tiers, c'est-à-dire les risques inhérents pour elle-même et ses clients. La criticité d'une entente devrait être prise en compte lors de cette évaluation.

L'ensemble des risques inhérents attribuable à l'entente envisagée devrait être pris en compte, incluant ceux que le recours au tiers est susceptible d'atténuer, notamment :

- le risque stratégique;
- le risque de réputation;
- les risques liés aux nouvelles technologies;
- les risques opérationnels;
- le risque de concentration;
- le risque lié à la sous-traitance.

Les impacts potentiels sur les clients et sur le traitement équitable de ceux-ci devraient être considérés dans le cadre de l'évaluation des risques inhérents.

8.2.3. Utilisation des résultats de l'évaluation de la criticité et des risques inhérents

L'institution devrait s'assurer que la criticité et le niveau de risque d'une entente envisagée sont arrimés à son appétit pour le risque lié aux tiers, à sa stratégie de recours aux tiers ainsi qu'à sa tolérance aux perturbations.

Les résultats de l'évaluation de la criticité et des risques constituent des intrants importants pour les différentes étapes de gestion des risques d'une entente en permettant :

- d'évaluer la suffisance de l'environnement de contrôle de l'institution aux fins d'intégration de l'entente et d'identifier des mesures additionnelles requises, le cas échéant;
- d'orienter la diligence raisonnable à effectuer avant de conclure une entente avec un tiers;
- d'identifier les clauses contractuelles pertinentes à intégrer à l'entente;
- d'identifier les activités à intégrer à la surveillance en continu de l'entente et leur fréquence;
- de planifier la terminaison de l'entente.

8.3. Sélection d'un tiers

L'Autorité s'attend à ce que l'institution financière fasse preuve de diligence raisonnable avant de conclure une entente avec un tiers.

L'institution devrait faire preuve de diligence raisonnable avant de conclure une entente avec un tiers. À cette fin, elle devrait se doter de processus d'évaluation et de sélection des tiers. Ces processus devraient inclure les approbations requises et les critères d'escalade aux différents paliers hiérarchiques.

PROJET

La diligence raisonnable faite dans le cadre de l'évaluation d'un tiers devrait notamment permettre à l'institution de :

- déterminer le niveau de risque global associé à une entente avec un tiers;
- s'assurer qu'une entente avec un tiers est arrimée à sa stratégie de recours aux tiers, à son appétit pour le risque lié aux tiers ainsi qu'à sa tolérance aux perturbations;
- déterminer dans quelle mesure et de quelle manière elle pourra identifier, évaluer, contrôler et suivre de manière adéquate les risques associés à l'entente avec un tiers en continu (intrants pour déterminer les dispositions contractuelles et les éléments qui devront faire l'objet d'une surveillance en continu).

L'évaluation du tiers devrait notamment viser les dimensions suivantes :

- la capacité du tiers à fournir les produits ou les services prévus à l'entente;
- la saine gestion des risques qui découlent de l'entente, incluant la résilience opérationnelle du tiers;
- l'analyse coûts-bénéfices.

La diligence raisonnable devrait être proportionnelle au niveau de risque et à la criticité d'une entente. Dans le cas d'une entente critique ou à risque élevé, certains critères minimaux devraient être utilisés lors de l'évaluation d'un tiers. L'Annexe 1 présente des critères qui, dans une perspective de saine gestion du risque, devraient minimalement être utilisés pour les ententes critiques ou à risque élevé.

Lorsqu'elle envisage de conclure une entente avec un tiers à l'extérieur du Canada (ou si une entente comporte des sous-traitants à l'extérieur du Canada), l'institution devrait être vigilante et tenir compte des risques réglementaire, juridique, politique, économique et autres qui pourraient entraver la capacité du tiers à respecter l'entente.

8.4. Conclusion de l'entente

L'Autorité s'attend à ce qu'une entente avec un tiers soit formalisée et qu'elle renferme les dispositions nécessaires pour assurer une gestion saine et prudente du risque lié aux tiers.

Une entente avec un tiers devrait être encadrée par un contrat écrit qui définit clairement les rôles et responsabilités, les droits et obligations et les attentes de l'institution et du tiers. Elle devrait permettre à l'institution d'obtenir l'information nécessaire pour assurer une surveillance en continu de l'entente et gérer adéquatement le risque lié aux tiers.

À cet effet, l'institution devrait notamment intégrer à ses ententes :

- le droit à l'audit, par l'institution ou par un auditeur indépendant;
- le droit de l'institution d'évaluer les pratiques de gestion de risque du tiers;
- les types de renseignements à transmettre par le tiers et la fréquence de communication;
- les exigences et les processus visant le signalement d'événements susceptibles d'avoir une incidence importante sur les risques et la prestation des services, notamment la gestion des incidents.

L'Annexe 2 présente les dispositions qui devraient généralement se retrouver dans les ententes contractuelles avec des tiers, et ce, en fonction de la nature, de la criticité et du niveau de risque de l'entente. Toutefois, dans une perspective de saine gestion du risque, ces dispositions devraient minimalement être intégrées aux ententes avec des tiers critiques ou à risque élevé.

Les dispositions comprises dans les ententes avec des tiers ne devraient pas interférer avec la capacité de l'institution de gérer efficacement ses activités, non plus qu'elles ne devraient porter atteinte aux pouvoirs de surveillance de l'Autorité.

L'Autorité reconnaît que certaines ententes avec des tiers ne peuvent être encadrées par un contrat sur mesure. Ce type d'entente est abordé à la section 10 – Contrats d'adhésion.

8.5. Surveillance en continu de l'entente

8.5.1. Surveillance en continu du respect de l'entente

L'Autorité s'attend à ce que l'institution financière surveille en continu ses ententes avec des tiers afin de s'assurer du respect de ces dernières et de la gestion adéquate du risque lié aux tiers.

L'institution devrait surveiller en continu toute entente avec un tiers afin de :

- s'assurer du respect des modalités de l'entente;
- confirmer l'application des pratiques et des mesures évaluées à l'étape de la sélection;
- s'assurer de la saine gestion des incidents en lien avec l'entente survenus chez les tiers[8];
- faire la reddition de la performance des tiers, incluant les irrégularités, si applicable.

Dans le cadre de la surveillance en continu, l'institution devrait mettre en place des processus utilisant un éventail de méthodes d'audit et de collecte d'informations. Les risques pris en compte lors de la sélection du tiers devraient notamment être intégrés aux suivis, de même que ceux qui auraient émergé depuis la conclusion de l'entente. La surveillance en continu devrait permettre à l'institution de traiter et d'escalader les incidents et les cas de non-respect des modalités du contrat (incluant la performance du tiers).

L'étendue et la fréquence de la surveillance en continu devraient être proportionnelles au niveau de risque et à la criticité de l'entente avec le tiers. Une entente critique ou à risque élevé devrait faire l'objet d'une surveillance plus fréquente et exhaustive.

[8] Les incidents doivent être gérés conformément au *Règlement sur la gestion et le signalement des incidents de sécurité de l'information de certaines institutions financières et des agents d'évaluation du crédit* (RLRQ, c. A-8.2, r. 0.1) lorsqu'applicable.

8.5.2. Réévaluation de la criticité et du niveau de risque

L'Autorité s'attend à ce que l'institution financière réévalue régulièrement la criticité et le niveau de risque d'une entente avec un tiers.

La criticité et le niveau de risque d'une entente avec un tiers peuvent évoluer tout au long du cycle de vie de celle-ci. Par conséquent, l'institution devrait en faire l'évaluation régulièrement, notamment lors de la survenance d'un des événements suivants :

- un incident majeur ou répété chez le tiers;
- des pratiques du tiers qui ne respectent pas l'entente ou les attentes de l'institution;
- une récurrence de plaintes reçues à l'endroit du tiers ou des services ou produits fournis;
- le renouvellement de l'entente;
- un changement important dans l'environnement interne de l'institution;
- un changement important à l'entente;
- un changement important chez le tiers (changement organisationnel, localisation des services, introduction de nouvelles technologies, etc.);
- un changement dans l'environnement externe de l'institution ou du tiers (politique, économique, social, juridique et financier, etc.).

Les informations recueillies dans le cadre de la surveillance en continu devraient être utilisées pour réévaluer le niveau de risque d'une entente.

8.5.3. Niveau de risque de l'entente dans les limites de l'appétit pour le risque

L'institution devrait avoir en place des mécanismes afin de s'assurer que le niveau de risque d'une entente avec un tiers demeure dans les limites de son appétit pour le risque lié aux tiers. Les mécanismes devraient inclure les critères nécessitant l'escalade à la haute direction et au conseil d'administration.

Pour ce faire, l'institution devrait se doter d'indicateurs afin de suivre les niveaux de tolérance établis pour le risque lié aux tiers. Ces indicateurs devraient être intégrés à la reddition de compte produite à l'intention de la haute direction et du conseil d'administration.

Le suivi des niveaux de tolérance devrait être fait individuellement pour chacune des ententes avec un tiers, mais également pour l'ensemble des ententes avec un même tiers.

PROJET

8.6. Terminaison de l'entente

L'Autorité s'attend à ce que l'institution financière développe, maintienne et teste des stratégies de sortie pour assurer la terminaison ordonnée d'une entente avec un tiers.

8.6.1. Développement de stratégies de sortie

L'institution devrait développer, maintenir à jour et tester ses stratégies de sortie. Celles-ci devraient couvrir les scénarios suivants :

- la terminaison imprévue, c'est-à-dire une stratégie de sortie d'urgence;
- la terminaison prévue pour des raisons commerciales, stratégiques ou autres, c'est-à-dire une terminaison planifiée.

Une stratégie de sortie d'urgence devrait couvrir un large éventail de motifs, notamment :

- une détérioration des services fournis;
- des faiblesses importantes en matière de gouvernance ou de gestion des risques chez le tiers;
- une perturbation prolongée des services qui ne peut être gérée par d'autres mesures de continuité des activités;
- un incident opérationnel majeur.

Les stratégies de sortie devraient être appuyées par des plans de sortie qui en précisent les modalités, telles que les déclencheurs et les étapes à réaliser.

8.6.2. Intégration de stratégies de sortie aux ententes avec des tiers

L'institution devrait s'assurer que des dispositions concernant les stratégies de sortie, planifiées ou non, sont intégrées à ses ententes avec des tiers afin d'en assurer le bon déroulement. Les dispositions contractuelles suivantes devraient notamment être intégrées :

- les rôles et responsabilités dans le cadre d'une terminaison;
- les périodes de transition pour minimiser le risque de perturbation;
- les processus pour assurer le transfert des actifs intellectuels (p. ex. les données et les applications) et des actifs physiques dans un délai raisonnable et dans un format permettant la poursuite des activités;
- les dispositions relatives aux données (p. ex. archivage, destruction, retrait des accès);
- dans le cas des plans de sortie pour une terminaison non planifiée, la coordination avec un comité de gestion de crise ou d'autres ressources identifiées.

Les stratégies de sortie devraient être réévaluées régulièrement, entre autres lors d'un changement important à une entente avec un tiers.

PROJET

8.7. Risque lié à la concentration des tiers

L'Autorité s'attend à ce que l'institution financière évalue le risque de concentration des tiers qui lui est propre et en tienne compte dans sa gestion du risque.

L'institution devrait évaluer le risque de concentration avant de conclure une entente avec un tiers, et tout au long de son cycle de vie. La concentration des tiers dans une institution comporte plusieurs dimensions, notamment :

- la concentration d'un tiers dans un même processus;
- la concentration d'un tiers dans l'institution;
- la concentration géographique.

La concentration systémique devrait également être évaluée dans la mesure du possible en fonction de l'information disponible (voir la définition donnée dans la section 3.2 – Risques spécifiques).

8.8. Risque lié aux ententes de sous-traitance des tiers

L'Autorité s'attend à ce que l'institution identifie et gère les risques découlant des ententes de sous-traitance conclues par un tiers.

L'institution devrait évaluer les risques liés aux sous-traitants d'un tiers qui pourraient avoir une incidence sur les produits ou services prévus à une entente.

8.8.1. Identification des risques liés à la sous-traitance lors de la sélection d'un tiers

Dans le cadre de l'évaluation d'un tiers, l'institution devrait :

- identifier les sous-traitants et déterminer leur criticité;
- évaluer les pratiques du tiers en matière de gestion des sous-traitants (c'est-à-dire sa gestion du risque lié aux tiers);
- évaluer l'incidence des ententes de sous-traitance sur le risque de concentration de l'institution.

L'institution pourrait demander au tiers de mettre en place des mesures additionnelles si elle juge que le risque lié à la sous-traitance n'est pas géré adéquatement par le tiers.

8.8.2. Suivi des ententes de sous-traitance

L'institution devrait inclure les sous-traitants dans la surveillance en continu d'une entente avec un tiers. Pour ce faire, elle devrait s'assurer d'obtenir l'information nécessaire à la saine gestion du risque lié à la sous-traitance.

Des dispositions devraient être intégrées aux ententes contractuelles avec les tiers afin d'obtenir des engagements sur la saine gestion du risque lié aux tiers ou encore afin que l'institution soit avisée dans diverses situations (voir l'Annexe 2).

PROJET

L'institution pourrait également inclure des dispositions contractuelles :

- qui interdisent le recours à des sous-traitants pour certaines fonctions;
- qui exigent qu'elle soit informée par écrit lors d'une nouvelle entente avec un sous-traitant ou lors d'un remplacement;
- 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.

8.9. Protection des données

L'Autorité s'attend à ce que l'institution financière mette en place les mesures appropriées afin d'assurer la protection des données faisant l'objet d'une entente avec un tiers.

L'institution devrait définir des mesures visant la disponibilité, l'intégrité et la confidentialité des données afin d'assurer la saine gouvernance des données partagées avec le tiers. Des dispositions encadrant ces mesures, notamment en ce qui concerne la responsabilité de chaque partie, devraient être intégrées aux ententes avec les tiers, notamment :

- l'étendue des données à protéger;
- les mécanismes pour détecter les atteintes à la sécurité de l'information chez le tiers;
- les exigences de signalement lors d'un incident de sécurité de l'information, incluant les incidents de confidentialité[9];
- la disponibilité et l'accès aux données par l'institution;
- les mesures de contrôle et le suivi de l'utilisation des systèmes et de l'information de l'institution par le tiers (p. ex. accès aux données);
- un énoncé clair des rôles et responsabilités de chaque partie dans la gestion de la sécurité des données;
- la destruction des données.

Les données devraient être soumises aux mêmes mesures de protection, qu'elles soient conservées par le tiers ou par l'institution[10].

PROJET

[9] Les incidents doivent être gérés conformément au *Règlement sur la gestion et le signalement des incidents de sécurité de l'information de certaines institutions financières et des agents d'évaluation du crédit* (RLRQ, c. A-8.2, r. 0.1) lorsqu'applicable.

[10] Autorité des marchés financiers, *Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications*, février 2020.

8.10. Continuité des activités

L'Autorité s'attend à ce que l'institution financière s'assure que des mesures soient mises en place pour permettre la continuité d'une activité critique dont la réalisation implique une entente avec un tiers.

Les activités critiques qui font l'objet d'une entente avec un tiers, ou encore, qui sont soutenues par une telle entente, devraient être intégrées au plan de continuité des activités de l'institution afin d'assurer un niveau de préparation optimal aux incidents opérationnels sévères, mais plausibles. L'institution devrait également exiger du tiers qu'il mette en œuvre un tel plan de continuité des affaires.

8.10.1. Évaluation et suivi des plans de continuité des activités des tiers

Pour une entente avec un tiers ayant un niveau de criticité élevé, l'institution devrait exiger que ce dernier s'engage notamment à :

- fournir une description du plan de continuité des activités et de la stratégie pour assurer la continuité et la reprise des services prévus dans le cadre de l'entente;
- tester régulièrement ses programmes de continuité des activités et de reprise (incluant la relève informatique) après un incident impliquant les services fournis;
- informer l'institution du résultat des tests et des mesures correctives, le cas échéant, et remédier à toute défaillance importante.

8.10.2. Intégration du risque lié aux tiers dans le plan de continuité des activités de l'institution financière

L'institution devrait tenir compte de ses ententes avec des tiers dans sa stratégie et son plan de continuité des activités[11]. Elle devrait :

- considérer des scénarios où les tiers seraient dans l'impossibilité de fournir le ou les services prévus par l'entente suivant un incident opérationnel sévère, mais plausible;
- faire des tests périodiques des plans de continuité des activités en s'assurant que les mesures identifiées respectent la tolérance aux perturbations de l'institution.

Le tiers et l'institution devraient envisager de concevoir et de tester conjointement les plans de continuité des activités et les plans de reprise après un incident, en fonction de la criticité de l'entente.

PROJET

[11] Autorité des marchés financiers, *Ligne directrice sur la gestion de la continuité des activités*, avril 2010.

8.11. Traitement équitable des clients

L'Autorité s'attend à ce que l'institution financière tienne compte du traitement équitable des clients dans la gestion du risque lié aux tiers, et ce, tout au long du cycle de vie d'une entente.

L'institution devrait intégrer des éléments qui visent le traitement équitable des clients dans sa gestion du risque lié aux tiers.

Lors de l'identification et de l'évaluation des risques liés à une entente envisagée, elle devrait :

- considérer les processus commerciaux importants comme critère pour évaluer la criticité de l'entente;
- considérer l'impact pour les clients dans l'évaluation des différents risques inhérents (fuite de données, perturbation des services, etc.).

Lors de la sélection d'un tiers, elle devrait :

- s'assurer que les pratiques du tiers sont en adéquation avec la culture de l'institution en matière de traitement équitable du client.

Lors de la conclusion d'une entente, elle devrait :

- intégrer des attentes en matière de traitement équitable des clients afin qu'elle puisse évaluer la performance du tiers en la matière;
- inclure, dans les dispositions de l'entente, le droit pour l'institution de recevoir de l'information permettant de brosser un portrait complet de l'expérience des clients et des enjeux en matière de traitement équitable des clients, lorsqu'applicable.

Enfin, lors de la surveillance en continu de l'entente, elle devrait :

- inclure des indicateurs de suivi permettant d'apprécier le traitement équitable des clients dans les ententes, notamment quand le tiers est en contact direct avec les clients.

8.12. Fournisseurs de services infonuagiques

L'Autorité s'attend à ce que l'institution financière intègre des dispositions spécifiques dans ses ententes avec des tiers fournisseurs de services infonuagiques.

L'infonuagique pose des risques importants, notamment en matière de cybersécurité et de sécurité des données. En raison de la nature des risques qui découlent de ce type d'entente, les institutions devraient adapter leur gestion du risque lié aux tiers lorsqu'elles ont recours à des tiers fournisseurs de services infonuagiques.

En plus des attentes formulées dans la présente ligne directrice, les institutions devraient adapter leur cadre de gestion du risque lié aux tiers pour y inclure des éléments spécifiques à ce type d'entente. Elles devraient notamment se référer à la *Ligne directrice sur la gestion des risques liés aux technologies de*

PROJET

l'information et des communications[12], qui précise certaines attentes concernant les services infonuagiques fournis par un tiers.

Les éléments spécifiques devraient se baser sur les meilleures pratiques généralement reconnues dans le domaine.

8.12.1 Dispositions s'appliquant à l'infonuagique

Les institutions devraient intégrer des dispositions spécifiques dans les ententes contractuelles visant des services infonuagiques. Ces dispositions devraient viser à s'assurer que les mesures de contrôle et de sécurité chez le tiers permettent une gestion adéquate des risques. Elles devraient également avoir pour objectif de favoriser l'interopérabilité[13].

8.12.2 Transférabilité infonuagique[14]

En plus de planifier des stratégies de sortie adéquates, l'institution devrait tenir compte de la transférabilité infonuagique lorsqu'elle conclut une entente avec un fournisseur de services infonuagiques. À cette fin, elle devrait évaluer les avantages et les risques liés à la transférabilité infonuagique ainsi que des mesures d'atténuation en l'absence de celle-ci.

Pour atténuer le risque de concentration lié aux fournisseurs de services infonuagiques et ainsi gagner en résilience opérationnelle, l'institution pourrait envisager diverses stratégies, comme un environnement à nuages multiples.

9. Registre des ententes avec des tiers

L'Autorité s'attend à ce que l'institution financière se dote d'un registre centralisé de ses ententes avec des tiers et en assure la mise à jour en continu.

Une vue d'ensemble des ententes avec des tiers est indispensable à une gestion saine et prudente du risque. L'institution devrait tenir un registre centralisé de l'ensemble de ses ententes avec des tiers. Les éléments suivants devraient minimalement y être intégrés :

- le propriétaire de l'entente;
- la criticité de l'entente;
- le niveau de risque de l'entente;
- le ou les processus visés par l'entente chez l'institution ainsi que le niveau de criticité de ces derniers;

[12] Autorité des marchés financiers, *Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications*, 2020.

[13] Capacité des systèmes informatiques hétérogènes à fonctionner conjointement, grâce à l'utilisation de langages et de protocoles communs, et à donner accès à leurs ressources de façon réciproque.

[14] Le National Institute of Standards and Technology (NIST) définit la transférabilité infonuagique comme la capacité de faire passer des 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.

PROJET

- le ou les produits ou services couverts par l'entente;
- l'information sur les sous-traitants du tiers;
- la nature des informations partagées avec le tiers (informations sensibles, renseignements personnels);
- le lieu de prestation des services.

Le registre devrait être mis à jour à régulièrement, notamment lors de changements importants à l'entente, tels que le renouvellement, une modification importante, un changement concernant la criticité, un changement du lieu de prestation des services, ou encore lorsqu'une nouvelle entente de sous-traitance est conclue.

Afin d'assurer une gestion saine et prudente du risque lié aux tiers, les institutions devraient notamment utiliser les informations consignées au registre pour faire ressortir les dépendances et les interconnexions entre les ententes, en particulier celles relatives aux ententes critiques et à risque élevé.

10. Contrats d'adhésion

L'Autorité reconnaît que certaines ententes avec des tiers ne peuvent être encadrées par un contrat sur mesure. La conclusion d'une entente de type contrat d'adhésion n'exempte toutefois pas l'institution des attentes de la présente ligne directrice.

Lorsqu'elle conclut une entente de la sorte avec un tiers, l'institution devrait adapter son cadre de gestion du risque lié aux tiers en conséquence. La sélection d'un tiers devrait être faite en fonction des renseignements disponibles et la surveillance en continu, dans la mesure où elle est limitée à ce qui est prévu à l'entente standardisée, devrait quant à elle viser des mesures de continuité des activités[15] chez l'institution ainsi que d'autres mesures permettant de rehausser la résilience opérationnelle.

PROJET

[15] Se référer à la *Ligne directrice sur la continuité des activités*.

Annexe 1 — Exemples de critères permettant l'évaluation d'un tiers

Cette annexe présente des exemples de critères permettant l'évaluation d'un tiers. Ces derniers devraient être pris en considération en fonction de la nature de l'entente, de sa criticité et de son niveau de risque. Toutefois, dans une perspective de saine gestion du risque, ces critères devraient minimalement être utilisés pour les ententes critiques ou à risque élevé.

Capacité d'un tiers

- le modèle d'affaires et sa complexité;
- la réputation et l'expérience;
- les compétences opérationnelles et techniques pour réaliser les activités prévues par l'entente (y compris, le cas échéant, celles des sous-traitants);
- la solidité financière;
- la capacité à respecter les obligations légales et réglementaires qui s'appliquent dans le cadre de l'entente;
- la robustesse de la gestion des risques, incluant les risques opérationnels, dont le risque lié aux tiers, le risque des technologies de l'information et des communications ainsi que le risque lié à la donnée;
- la robustesse du processus de gestion des incidents (sécurité de l'information et risque opérationnel);
- la capacité à fournir les services critiques durant les perturbations en fonction des plans de continuité des activités et des plans de gestion de crise;
- la capacité à assurer le traitement équitable des clients.

Gestion des risques de l'entente

- le risque d'atteinte à la réputation 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 ou le sous-traitant du tiers, si applicable;
- les conflits d'intérêts potentiels;
- la dépendance du tiers à l'égard des sous-traitants;
- la robustesse de la gestion des risques associés aux dépendances géographiques. Ces risques peuvent être liés à l'environnement économique, financier, politique, juridique ou réglementaire du ou des territoires où le service concerné sera fourni;
- l'incidence de l'entente avec le tiers, y compris avec ses sous-traitants, sur le risque de concentration de l'institution financière;
- la capacité et la facilité à remplacer le tiers par un autre tiers ou à rapatrier les activités, et les répercussions de cette substitution sur les activités;
- la transférabilité des applications et services fournis par le tiers à un autre tiers ou à l'institution financière;

PROJET

- la capacité à rapatrier les données, le cas échéant, au sein de l'institution financière;
- la couverture d'assurance du tiers;
- les risques d'ordre politique ou juridique liés au territoire de compétence du tiers ou des sous-traitants.

Coûts-bénéfices

- les conditions de résiliation de l'entente (y compris le coût, le calendrier et les restrictions contractuelles) et la facilité à passer à un autre tiers ou à rapatrier le service ou le produit à l'interne;
- les impacts d'une substitution du tiers pour l'institution financière et pour les clients (liés aux processus de transfert et de terminaison d'une entente d'un tiers).

PROJET

Annexe 2 — Exemples de dispositions contractuelles à intégrer aux ententes avec des tiers

Cette annexe présente les dispositions qui devraient généralement se retrouver dans les ententes contractuelles avec des tiers, et ce, en fonction de la nature, de la criticité et du niveau de risque de l'entente. Toutefois, dans une perspective de saine gestion du risque, ces dispositions devraient minimalement être intégrées aux ententes avec des tiers critiques ou à risque élevé.

- date d'entrée en vigueur, date de renouvellement, et délais de préavis et de terminaison;
- rôles et responsabilités de l'institution financière, du tiers et des sous-traitants, incluant ceux relatifs à la gestion des incidents, à la cybersécurité, aux données, à la résilience et à d'autres configurations techniques;
- les attentes quant au traitement équitable des clients pour évaluer la performance du tiers en la matière;
- le droit de l'institution financière d'obtenir de l'information du tiers pour assurer la saine gestion des risques liés à l'entente (incluant l'information sur les sous-traitants);
- les paramètres du recours aux sous-traitants;
- les mesures d'évaluation du rendement (respect des modalités du contrat);
- la propriété, l'accès et l'utilisation des actifs matériels et de propriété intellectuelle;
- la gouvernance des données (confidentialité, intégrité, sécurité et disponibilité des données);
- la propriété et la transférabilité des données;
- le droit de l'institution de recevoir l'information permettant de brosser un portrait complet de l'expérience des clients et des enjeux en matière de traitement équitable des clients, lorsqu'applicable;
- le droit de l'institution de recevoir de l'information adéquate, complète et en temps opportun, notamment lors :
  - d'un incident opérationnel majeur ou répété (chez le tiers ou un sous-traitant);
  - d'une nouvelle entente avec un sous-traitant ou d'un changement;
  - d'un changement de propriété du tiers;
  - d'un changement organisationnel ou opérationnel important chez le tiers;
  - d'une non-conformité avec les exigences réglementaires ou d'un litige;
- le mécanisme de traitement des plaintes;
- le défaut et la résiliation, incluant le préavis de terminaison de l'entente;
- l'exigence de conformité à la réglementation;
- les modalités de terminaison;
- l'exigence d'un plan de continuité des affaires en cas d'interruption de service, y compris les attentes en matière de tests et de rapports, et de mesures d'atténuation;

PROJET

- la responsabilité du tiers d'obtenir et de maintenir une couverture d'assurance appropriée (telle une cyberassurance) de même que d'en communiquer les conditions générales, incluant lors d'un changement;
- toute disposition supplémentaire requise afin que l'institution financière puisse gérer adéquatement le risque lié aux tiers conformément à la présente ligne directrice.

PROJET

5.2.2 Publication

Aucune information.