5.2

Réglementation et lignes directrices

5.2 RÉGLEMENTATION ET LIGNES DIRECTRICES

5.2.1 Consultation

Aucune information.

5.2.2 Publication

DÉCISION N° 2026-PDG-0015

Ligne directrice sur la gestion du risque lié aux tiers

Ligne directrice sur la gestion des risques liés à l'impartition

Vu le pouvoir de l'Autorité des marchés financiers (l'« AMF ») d'établir des lignes directrices destinées à tous les assureurs autorisés, à une catégorie seulement d'entre eux ou à une fédération dont de tels assureurs sont membres, conformément à l'article 463 de la *Loi sur les assureurs*, RLRQ, c. A-32.1 (la « LA »);

Vu le pouvoir de l'AMF d'établir des lignes directrices destinées à toutes les coopératives de services financiers, à une catégorie seulement d'entre elles, à des caisses ou à une fédération dont de telles caisses sont membres, conformément à l'article 565.1 de la *Loi sur les coopératives de services financiers*, RLRQ, c. C-67.3 (la « LCSF »);

Vu le pouvoir de l'AMF d'établir des lignes directrices destinées à toutes les institutions de dépôts autorisées, à une catégorie seulement d'entre elles ou aux fédérations dont de telles institutions sont membres, conformément à l'article 42.2 de la *Loi sur les institutions de dépôts et la protection des dépôts*, RLRQ, c. I-13.2.2 (la « LIDPD »);

Vu le pouvoir de l'AMF d'établir des lignes directrices destinées à toutes les sociétés de fiducie autorisées ou à une catégorie d'entre elles seulement, conformément à l'article 254 de la *Loi sur les sociétés de fiducie et les sociétés d'épargne*, RLRQ, c. S-29.02 (la « LSFSE »);

Vu que le pouvoir de l'AMF d'établir une ligne directrice, prévu aux articles 463 de la LA, 565.1 de la LCSF, 42.2 de la LIDPD et 254 de la LSFSE, appartient exclusivement à son président-directeur général, conformément à l'article 24 de la *Loi sur l'encadrement du secteur financier*, RLRQ, c. E-6.1;

Vu la publication pour consultation au Bulletin de l'AMF (le « Bulletin ») le 9 octobre 2025 [(2025) B.A.M.F., vol. 22, n°40, section 5.2.1] du projet de *Ligne directrice sur la gestion du risque lié aux tiers* (la « Nouvelle ligne directrice »);

Vu les modifications apportées au projet de Nouvelle ligne directrice à la suite de cette consultation;

Vu que la Nouvelle ligne directrice intègre les attentes de l'AMF qui se retrouvaient dans la *Ligne directrice sur la gestion des risques liés à l'impartition* (l'« Ancienne ligne directrice »);

Vu que la Nouvelle ligne directrice prendra effet le 1er avril 2027 et que, de manière concordante, il est nécessaire de révoquer l'Ancienne ligne directrice à cette date;

Vu le deuxième alinéa de l'article 463 de la LA, le troisième alinéa de l'article 565.1 de la LCSF, le deuxième alinéa de l'article 42.2 de la LIDPD et le deuxième alinéa de l'article 254 de la LSFSE selon

lesquels l'AMF publie à son Bulletin les lignes directrices qu'elle établit après en avoir transmis une copie au ministre des Finances (le « Ministre »);

Vu le projet de Nouvelle ligne directrice proposé par la Direction principale de l'encadrement et de la résolution ainsi que la recommandation du surintendant des institutions financières d'établir celle-ci;

En conséquence :

L'AMF établit la *Ligne directrice sur la gestion du risque lié aux tiers,* dont le texte est annexé à la présente décision, et en autorise la publication au Bulletin après en avoir transmis une copie au Ministre.

L'AMF révoque la *Ligne directrice sur la gestion des risques liés à l'impartition*.

La *Ligne directrice sur la gestion du risque lié aux tiers* prend effet le 1er avril 2027 et remplace, à cette date, la *Ligne directrice sur la gestion des risques liés à l'impartition*.

Fait le 24 mars 2026.

Yves Ouellet
Président-directeur général

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 la *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.

La Ligne directrice fait suite à la consultation publique qui s'est déroulée du 9 octobre au 19 décembre 2025.

Cet encadrement vise à favoriser une gestion saine et prudente du risque lié aux tiers et ultimement à rehausser la résilience des institutions financières. Les attentes couvrent l'ensemble du cycle de vie des ententes avec des tiers.

La Ligne directrice prendra effet le 1er avril 2027, soit un an après la publication de la version finale. Les ententes conclues à partir de cette date devront tenir compte de l'ensemble de ses dispositions.

Pour ce qui est des ententes conclues avant la prise d'effet, l'AMF juge raisonnable que les institutions financières mettent en œuvre les attentes nécessitant des modifications contractuelles lors du prochain renouvellement. Si un renouvellement a lieu entre la publication et la prise d'effet de la Ligne directrice, l'AMF encourage tout de même les institutions à intégrer les pratiques de saine gestion de risque dans les ententes contractuelles. Pour les ententes de longue durée, une approche basée sur la criticité et le niveau de risque devrait être considérée pour la mise à jour de l'entente.

La Ligne directrice intègre les attentes de l'AMF qui se retrouvaient dans la *Ligne directrice sur la gestion des risques liés à l'impartition*. Par conséquent, et de manière concordante, celle-ci sera révoquée en date du 1er avril 2027.

La Ligne directrice est publiée ci-après et est également accessible sur le site Web de l'AMF « Ligne directrice sur la gestion du risque lié aux tiers ». Les mémoires reçus dans le cadre de la consultation, ainsi qu'un tableau synthèse des principaux commentaires, sont également accessibles dans la section « Consultations terminées » sous « Ligne directrice sur la gestion du risque lié aux tiers ».

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 26 mars 2026

Autorité des marchés financiers

Mars 2026

LIGNE DIRECTRICE SUR LA GESTION DU RISQUE LIÉ AUX TIERS

TABLE DES MATIÈRES

1. Introduction et champ d'application

Les institutions financières font appel à des tiers pour soutenir la prestation de leurs services, leurs opérations ou encore contribuer à leur stratégie commerciale. Le recours aux tiers, de même que la dépendance envers ceux-ci, s'est considérablement accru en réponse à la transformation numérique et à l'évolution rapide des nouvelles technologies. Cette tendance devrait se poursuivre, 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 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.

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 stabilité financière (CSF). Compte tenu de sa nature spécifique, elle s'appuie sur les attentes des lignes directrices formant l'assise de l'encadrement prudentiel[1] 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*.

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

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 dans la mise en œuvre des attentes.

En vertu des pouvoirs habilitants[2] 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 Autorité des marchés financiers, *Ligne directrice sur la gouvernance*, *Ligne directrice sur la gestion intégrée des risques* et *Ligne directrice sur la conformité*.

2 *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.

2. 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 :

- du principe de proportionnalité, c'est-à-dire de la taille, de la nature, de la complexité et du profil de risque de l'institution financière ;
- de la criticité et du niveau de risque propre à chacune des ententes.

Le principe de proportionnalité, ainsi que les notions de criticité et de gestion des risques, sont mentionnés uniquement dans cette section, mais sont applicables à l'ensemble de la ligne directrice.

L'Autorité rappelle que l'institution financière demeure ultimement responsable de l'ensemble des activités, fonctions et services impartis à un tiers tel que prévu dans les lois sectorielles administrées par l'Autorité[3].

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

2.1 Prise d'effet

La Ligne directrice prendra effet le 1er avril 2027, soit un an après la publication. Les ententes conclues à partir de cette date devront tenir compte de l'ensemble de ses dispositions.

Pour ce qui est des ententes conclues avant la prise d'effet, l'AMF juge raisonnable que les institutions financières mettent en œuvre les attentes nécessitant des modifications contractuelles lors du prochain renouvellement. Si un renouvellement a lieu entre la publication et la prise d'effet de la Ligne directrice, l'AMF encourage tout de même les institutions à intégrer les pratiques de saine gestion de risque dans les ententes contractuelles. Pour les ententes de longue durée, une approche basée sur la criticité et le niveau de risque devrait être considérée pour la mise à jour de l'entente.

[3] Ibid.

3. Terminologie

Chaîne d'approvisionnement

Réseau d'entités ou de personnes qui fournissent des infrastructures, des biens ou des services 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 son importance pour l'institution financière. Elle reflète l'impact potentiel de la matérialisation d'un risque à l'égard des produits ou services prévus à l'entente, tant pour l'institution financière que pour ses clients.

Les impacts peuvent être de différentes natures (p. ex. continuité des affaires, réglementaires, traitement équitable des clients, financiers, réputationnels, etc.).

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[4].

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[5] ;

Elles excluent :

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

[4] Les ententes avec des tiers portent généralement sur des produits ou des services, mais elles peuvent également prendre d'autres formes. C'est notamment le cas des ententes stratégiques qui peuvent viser, à titre d'exemple, un partenariat.

[5] Par exemple, les ententes visant des services infonuagiques ou encore des logiciels.

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*[6].

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.

Résilience opérationnelle

Capacité d'une institution financière à anticiper, se préparer, faire face et s'adapter aux perturbations dans un environnement changeant, afin de continuer à mener ses activités, de progresser et d'en tirer des apprentissages.

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 porter atteinte à l'intégrité des marchés.

Sous-traitant d'un tiers

Personne ou entité faisant partie de la chaîne d'approvisionnement d'un tiers et appuyant la fourniture de produits ou de services prévus dans le cadre d'une entente avec une institution financière. Les sous-traitants incluent les tiers de premier niveau, c'est-à-dire les sous-traitants directs des tiers, mais n'y sont pas limités.

Tiers intragroupe

Tiers qui fait partie du groupe d'une institution financière. Les tiers intragroupes sont ceux ayant un détenteur de leur contrôle commun[7]. Ils peuvent inclure notamment la maison mère, une société de portefeuille, les entités sœurs ou toutes autres entités affiliées à l'institution financière.

6 RLRQ, c. D-9.2.

7 Les notions de contrôle sont définies dans les différentes lois sectorielles administrées par l'Autorité.

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 d'autres impacts non financiers, y compris les fuites de renseignements personnels.

Les niveaux de tolérance peuvent être exprimés en termes de durée ou à l'aide d'autres indicateurs pertinents.

Risque lié à la concentration des tiers

Le risque revêt deux formes :

1. 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 :

   - concentration de plusieurs produits ou services fournis par un même tiers dans un processus ;
   - concentration de plusieurs produits ou services fournis par un même tiers au sein d'une même institution ;
   - concentration de produits ou de services d'un ou de plusieurs tiers provenant d'une même région géographique ; ou
   - plusieurs tiers qui dépendent du même sous-traitant.

2. Le risque de concentration systémique découle de la dépendance de plusieurs institutions à un ou plusieurs produits ou services fournis par un seul tiers ou par un nombre limité de tiers, directement ou indirectement par l'entremise de sous-traitants, 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 est susceptible d'exacerber certains risques et d'accroître la dépendance envers des tiers, augmentant ainsi le risque de concentration.

Le risque lié à la sous-traitance peut découler des sous-traitants directs du tiers, sans toutefois s'y limiter. Il peut également découler d'autres tiers de la chaîne d'approvisionnement.

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. La matérialisation de certains risques découlant du recours à des tiers peut affecter les activités critiques[8] et les services commerciaux importants, et entraîner des répercussions négatives significatives pour l'institution, ses clients, voire ultimement le système financier. Ainsi, la saine gestion du risque lié aux tiers constitue un pilier de la résilience opérationnelle.

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

5. Ententes de distribution

Les attentes énoncées dans la présente ligne directrice sont complémentaires à celles formulées dans d'autres lignes directrices, notamment celle sur les saines pratiques commerciales. Elles visent une gestion globale des risques.

Compte tenu de la nature spécifique de ce type d'entente, il revient à l'institution financière d'adapter ses critères d'évaluation de la criticité pour mieux refléter les caractéristiques propres aux ententes de distribution. Comme pour toute entente avec un tiers, l'institution devrait adapter ses mesures de gestion des risques en tenant compte de la criticité et du niveau de risque que représente l'entente de distribution.

6. 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.

6.1 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[9] ainsi qu'à l'appétit pour le risque lié aux tiers de l'institution.

---

8 Autorité des marchés financiers, *Ligne directrice sur la gestion de la continuité des activités*.

9 La stratégie de recours aux tiers définit le cadre stratégique du recours aux tiers et est étroitement liée à l'appétit pour le risque. Elle peut notamment préciser les limites du recours aux tiers, les types de

En sus des responsabilités qui lui sont généralement dévolues[10], l'Autorité s'attend à ce que le conseil d'administration :

- approuve la stratégie concernant le recours aux tiers;
- approuve l'appétit pour le risque lié aux tiers et la tolérance aux perturbations causées par des tiers ;
- obtienne l'assurance raisonnable que la gestion du risque lié aux tiers est arrimée à la stratégie de recours aux tiers, à l'appétit pour le risque de l'institution, ainsi qu'aux cadres plus larges de gestion des risques[11].

6.2 Rôles et responsabilités de la haute direction

En sus des responsabilités qui lui sont généralement dévolues[12], l'Autorité s'attend à ce que la haute direction :

- définisse l'appétit pour le risque lié aux tiers de l'institution et les niveaux de tolérance permettant son opérationnalisation ;
- développe et opérationnalise un cadre de gestion du risque lié aux tiers qui couvre l'ensemble du cycle de vie des ententes ;
- produise une reddition de comptes régulière sur la gestion du risque lié aux tiers permettant d'informer le conseil d'administration en temps opportun ;
- communique la stratégie et le cadre de gestion du risque lié aux tiers à l'ensemble des parties prenantes concernées, y compris les employés et les tiers intragroupes ;
- assure le maintien au sein de l'institution, d'une expertise et de programmes de formation et de sensibilisation adéquats sur la gestion du risque lié aux tiers.

7. 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

services pouvant ou non faire l'objet d'une telle entente, ainsi que les conditions pouvant entraîner la terminaison d'une entente.

10 Autorité des marchés financiers, *Ligne directrice sur la gouvernance*.

11 Les institutions devraient utiliser leur structure de gouvernance existante pour l'approbation des politiques de gestion des risques liés aux tiers.

12 Ibid.

l'institution, du niveau de risque qu'elle est prête à accepter. Ce dernier devrait découler de l'appétit 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 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 recours aux tiers de l'institution.

8. 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.

Le cadre de gestion du risque lié aux tiers (le « cadre ») 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 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, et qu'il reflète l'évolution de l'environnement interne et externe ainsi que les bonnes pratiques en matière de gestion des risques.

9. 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.

9.1 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.

L'institution devrait évaluer la criticité d'une entente envisagée, c'est-à-dire celle du produit ou du service pour lequel elle prévoit recourir à un tiers. Elle devrait également évaluer les risques inhérents à l'entente envisagée, et ce, avant même l'étape de la sélection du tiers. L'évaluation des risques à cette étape est un outil qui pourrait permettre à l'institution de prendre des décisions éclairées quant au choix de confier ou non un produit ou un service à un 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 lié aux tiers devrait être proportionnelle à la criticité et au niveau de risque d'une entente, l'institution devrait faire ces évaluations pour chacune des ententes envisagées.

Les résultats de l'évaluation de la criticité et des risques constituent des intrants importants aux différentes étapes de gestion des risques d'une entente.

9.1.1 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'impact financier 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.

9.1.2 Évaluation des risques inhérents

L'institution devrait évaluer les risques que pose une entente envisagée avec un tiers, c'est-à-dire les risques inhérents pour elle-même et ses clients. Cette évaluation devrait être complétée par celle spécifique à un tiers au moment de la sélection. L'ensemble des risques inhérents attribuables à l'entente envisagée devrait être pris en compte, incluant ceux que le recours à un tiers est susceptible d'atténuer.

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.

9.2 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 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.

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 ;
- 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.

L'évaluation du tiers devrait par exemple porter sur des dimensions telles que :

- 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.

L'Annexe 1 présente des exemples de critères qui, dans une perspective de saine gestion du risque, devraient 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 tenir compte des risques réglementaire, juridique, politique, économique et autres qui pourraient entraver la capacité du tiers à respecter l'entente.

9.3 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 à l'égard du tiers. Elle devrait permettre à l'institution d'obtenir l'information nécessaire pour gérer adéquatement le risque lié aux tiers.

À cet effet, une saine gestion du risque devrait amener l'institution à intégrer à ses ententes des éléments tels que :

- 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 des répercussions importantes sur les risques et la prestation des services, notamment la gestion des incidents.
- le droit à l'audit, par l'institution ou par un auditeur indépendant.

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. Dans une perspective de saine gestion du risque, ces dispositions devraient 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.

Bien que les ententes avec des tiers devraient être formalisées par écrit, l'Autorité reconnaît qu'en certaines circonstances, des ententes peuvent être conclues avec un tiers en l'absence du respect de ce formalisme. L'absence d'entente écrite ne signifie pas qu'il n'y a pas d'entente avec le tiers ou de risque lié à ce dernier. Les ententes non écrites sont également incluses dans la portée de la ligne directrice.

L'Autorité reconnaît également que certaines ententes avec des tiers ne peuvent être encadrées par un contrat sur mesure. Ce type d'entente est abordé à la section 11.

9.4 Suivi en continu de l'entente

9.4.1 Respect de l'entente et gestion du risque lié aux tiers

L'Autorité s'attend à ce que l'institution financière assure une surveillance de ses ententes avec des tiers tout au long de la relation d'affaires.

L'institution devrait mettre en place des mesures afin de gérer le risque lié aux tiers, notamment :

- s'assurer du respect des modalités de l'entente ;
- confirmer l'application des pratiques de gestion des risques du tiers évaluées à l'étape de la sélection ;
- s'assurer de la saine gestion des incidents survenus chez les tiers en lien avec l'entente[13] ;
- faire la reddition de la performance des tiers, incluant les irrégularités, si applicable.

Les mesures visant à assurer une saine gestion du risque comprennent des mécanismes de détection (alertes, incidents, changements), ainsi que des activités de suivi périodique structurées.

Les risques pris en compte lors de la sélection du tiers devraient notamment être intégrés aux suivis, de même que ceux ayant émergé depuis la conclusion de l'entente. Ces suivis devraient permettre à l'institution de traiter et d'escalader les incidents ainsi que les cas de non-respect des modalités du contrat, y compris ceux liés à la performance du tiers.

9.4.2 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 ou lors de changements ou d'événements importants, par exemple :

- un incident majeur ou répété chez le tiers ;

[13] 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.

- 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 ;
- 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.).

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. 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 comptes produite à l'intention de la haute direction et du conseil d'administration.

9.5 Terminaison de l'entente

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

9.5.1 Développement de stratégies de sortie

L'institution devrait développer et maintenir à jour des stratégies de sortie. Celles-ci devraient couvrir la terminaison imprévue, c'est-à-dire une stratégie de sortie d'urgence, ainsi que 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, par exemple :

- 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, qui décrivent l'approche générale que l'institution adoptera lors d'une terminaison d'une entente avec un tiers, devraient être appuyées par des plans de sortie qui en précisent les modalités.

Les stratégies de sorties et les plans associés devraient être réévalués régulièrement, entre autres lors d'un changement important à une entente avec un tiers, pour s'assurer de leur faisabilité, notamment en termes de budget, de ressources, d'infrastructures ou de tout autre facteur pertinent.

9.5.2 Intégration de dispositions concernant les 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 et des actifs physiques dans un délai raisonnable et dans un format permettant la poursuite des activités ;
- les dispositions relatives aux données ;
- 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.

9.6 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 au sein d'une institution comporte plusieurs dimensions, notamment :

- la concentration d'un même tiers au sein d'un processus ;
- la concentration d'un même tiers au sein de l'institution ;
- la concentration géographique des tiers.

La concentration systémique devrait également être évaluée, dans la mesure du possible, en fonction de l'information disponible.

9.7 Risque lié à la sous-traitance

L'Autorité s'attend à ce que l'institution financière gère les risques liés à la sous-traitance découlant de ses ententes conclues avec des tiers.

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

- recenser les sous-traitants ayant une incidence importante sur les services ou produits prévus à l'entente ;
- 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.

L'institution devrait inclure le risque lié à la sous-traitance à la surveillance d'une entente avec un tiers. À cet effet, des dispositions devraient être intégrées aux ententes contractuelles afin d'obtenir des engagements des tiers relatifs à la saine gestion des risques liés à leurs propres tiers, ou encore afin que l'institution soit avisée dans diverses situations concernant les sous-traitants (voir l'Annexe 2).

L'institution pourrait également, afin d'atténuer ses risques, inclure, par exemple, 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.

9.8 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[14] ;
- 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 des rôles et responsabilités de chaque partie dans la gestion de la sécurité des données.

Les données devraient être soumises aux mêmes mesures de protection, qu'elles soient conservées par le tiers ou par l'institution[15].

9.9 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

[14] 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.

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

opérationnels sévères, mais plausibles. L'institution devrait également exiger du tiers qu'il mette en œuvre un tel plan de continuité des affaires.

9.9.1 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.

9.9.2 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[16]. 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 par le tiers 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.

16 Autorité des marchés financiers, *Ligne directrice sur la gestion de la continuité des activités*.

9.10 Traitement équitable des clients

L'Autorité s'attend à ce que l'institution financière prenne en considération le 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[17].

Lors de l'évaluation des risques liés à une entente envisagée, elle devrait tenir compte des impacts sur les clients (fuite de données, perturbation des services, etc.).

Selon la nature de l'entente, l'institution pourrait intégrer des mesures spécifiques visant le traitement équitable des clients, par exemple :

Lors de la sélection d'un tiers :

- 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 :

- intégrer des attentes en matière de traitement équitable des clients afin d'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 de l'expérience des clients et des enjeux en matière de traitement équitable des clients.

Enfin, lors de la surveillance de l'entente :

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

10. Répertoire des ententes avec des tiers

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

Une vue d'ensemble des ententes conclues avec des tiers est indispensable à une gestion saine et prudente du risque. À cette fin, l'institution devrait tenir des répertoires de ses

[17] Cette section exclut les ententes de distribution dont les attentes en matière de traitement équitable des clients sont déjà définies dans la *Ligne directrice sur les saines pratiques commerciales*.

ententes avec des tiers. Les ententes critiques devraient, quant à elles, faire l'objet d'un registre centralisé.

L'institution devrait intégrer dans ses répertoires les éléments clés permettant d'identifier les interconnexions entre les ententes et de gérer adéquatement les risques qui en découlent, par exemple :

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

Les registres devraient être mis à jour régulièrement, notamment lors de changements importants aux ententes 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.

11. Contrats d'adhésion ou difficilement négociables

L'Autorité reconnaît que certaines ententes avec des tiers peuvent être standardisées ou sont difficilement négociables.

Lorsque l'institution ne peut mettre en œuvre certaines mesures de gestion des risques préconisées par la présente ligne directrice en raison de l'indisponibilité d'informations ou de contraintes propres aux contrats d'adhésion, elle devrait adapter sa gestion des risques en conséquence.

L'institution devrait évaluer le risque que pose ce type de contrat à la sélection, en fonction des informations disponibles, et confirmer qu'il demeure acceptable en fonction de son appétit pour le risque lié aux tiers.

Des mesures compensatoires devraient être mises en place chez l'institution pour gérer le risque lié aux tiers. Elles pourraient inclure, par exemple, un suivi accru de la prestation du tiers, des mesures additionnelles de continuité des activités ou tout autre dispositif de résilience opérationnel jugé approprié.

La stratégie de gestion des risques devrait préciser la manière dont ce type de contrat doit être traité.

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. Dans une perspective de saine gestion du risque, ces critères devraient 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 ;
- la solidité financière ;
- la capacité à respecter les obligations légales et réglementaires ;
- la robustesse de la gestion des risques ;
- la robustesse du processus de gestion des incidents ;
- la capacité à fournir les services critiques durant les perturbations ;
- la capacité à assurer le traitement équitable des clients.

Gestion des risques de l'entente

- le risque d'atteinte à la réputation ;
- les conflits d'intérêts potentiels ;
- la dépendance du tiers à l'égard des sous-traitants ;
- la gestion des risques associés aux dépendances géographiques ;
- l'incidence de l'entente avec le tiers sur le risque de concentration de l'institution ;
- la capacité et la facilité à remplacer le tiers ou à rapatrier les activités ;
- la transférabilité des applications et services à un autre tiers ou à l'institution ;
- la capacité à rapatrier les données, le cas échéant, au sein de l'institution ;
- la couverture d'assurance du tiers ;
- les risques d'ordre politique ou juridique liés au territoire de compétence du tiers ou des sous-traitants ;
- les conditions de résiliation de l'entente 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.

Annexe 2 — Exemples de dispositions contractuelles

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. Dans une perspective de saine gestion du risque, ces dispositions devraient être intégrées aux ententes avec des tiers critiques ou à risque élevé.

- 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 ;
- le droit de l'institution financière d'obtenir de l'information du tiers pour assurer la saine gestion des risques liés à l'entente ;
- les mesures d'évaluation du rendement ;
- la propriété, l'accès et l'utilisation des actifs matériels et de propriété intellectuelle ;
- la gouvernance des données, la propriété et la transférabilité des données ;
- 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 ;
- 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 ;
- 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.