PROJET

AUTORITÉ DES MARCHÉS FINANCIERS

LIGNE DIRECTRICE SUR LA GESTION DU RISQUE OPÉRATIONNEL

Octobre 2016

TABLE DES MATIÈRES

Préambule

La présente ligne directrice est une indication des attentes de l'Autorité des marchés financiers (l'« Autorité ») à l'égard de l'obligation légale des institutions financières de suivre des pratiques de gestion saine et prudente. Elle porte donc sur l'interprétation, l'exécution et l'application de cette obligation imposée aux institutions financières.

Dans cette optique, l'Autorité privilégie une approche basée sur des principes plutôt que d'édicter des règles précises. Ainsi, du fondement même d'une ligne directrice, l'Autorité confère aux institutions financières la latitude nécessaire leur permettant de déterminer elles-mêmes les stratégies, politiques et procédures pour la mise en œuvre de ces principes de saine gestion et de voir à leur application en regard de la nature, de la taille et de la complexité de leurs activités. À cet égard, la ligne directrice illustre des façons de se conformer aux principes énoncés.

Note de l'Autorité

L'Autorité considère la gouvernance, la gestion intégrée des risques et la conformité (GRC) comme les assises sur lesquelles doivent reposer la gestion saine et prudente et les saines pratiques commerciales d'une institution financière et, conséquemment, les bases sur lesquelles l'encadrement prudentiel donné par l'Autorité s'appuie.

La présente ligne directrice s'inscrit dans cette perspective et énonce les attentes de l'Autorité à l'égard des pratiques en matière de gestion du risque opérationnel.

Champ d'application

La *Ligne directrice sur la gestion du risque opérationnel* est applicable aux assureurs de personnes, aux assureurs de dommages, aux sociétés de gestion de portefeuille contrôlées par un assureur, aux coopératives de services financiers, aux sociétés de fiducie et aux sociétés d'épargne régis par les lois suivantes :

- *Loi sur les assurances*, RLRQ, c. A-32;
- *Loi sur les coopératives de services financiers*, RLRQ, c. C-67.3;
- *Loi sur les sociétés de fiducie et les sociétés d'épargne*, RLRQ, c. S-29.01.

Enfin, cette ligne directrice s'applique tant à l'institution financière qui opère de façon autonome qu'à celle qui est membre d'un groupe financier[1]. Dans le cas des coopératives de services financiers et des sociétés mutuelles d'assurance[2] membres d'une fédération, les normes ou politiques adoptées à leur intention par la fédération doivent être cohérentes, voire convergentes, avec les principes de gestion saine et prudente comme ils sont précisés dans la présente ligne directrice.

Les expressions génériques « institution financière » ou « institution » sont utilisées pour faire référence à toutes les entités visées par le champ d'application.

1 Aux fins d'application de la présente, est considéré comme « groupe financier » tout ensemble de personnes morales formé d'une société mère (institution financière ou *holding*) et de personnes morales qui lui sont affiliées.

2 Les sociétés mutuelles d'assurance sont des assureurs de dommages visés par le champ d'application de la présente ligne directrice.

Prise d'effet et processus de mise à jour

La *Ligne directrice sur la gestion du risque opérationnel* est effective à compter du 1er octobre 2016.

En regard de l'obligation légale des institutions de suivre des pratiques de gestion saine et prudente, l'Autorité s'attend à ce que chaque institution se soit approprié les principes de cette ligne directrice en élaborant des stratégies, politiques et procédures adaptées à sa nature, sa taille, la complexité de ses activités et son profil de risque.

Dans la mesure où une institution a déjà mis en place un tel encadrement, l'Autorité pourra vérifier si cet encadrement permet à l'institution de répondre aux exigences prescrites par la loi.

Cette ligne directrice sera actualisée en fonction des développements en matière de gestion du risque opérationnel et à la lumière des constats effectués dans le cadre des travaux de surveillance menés auprès des institutions financières visées.

Introduction

La gestion du risque opérationnel est un sujet d'intérêt croissant pour le secteur financier depuis près de deux décennies. Le Comité de Bâle sur le contrôle bancaire (le « Comité de Bâle »)[3] a été le précurseur dans le domaine afin de faire connaître ses attentes. L'Association internationale des contrôleurs d'assurance (AICA) prône également une gestion adéquate des risques opérationnels[4]. En réponse à ces préoccupations croissantes des instances internationales, plusieurs juridictions membres de l'Organisation de coopération et de développement économique (OCDE) ont publié leurs orientations à l'égard de la gestion du risque opérationnel.

Étant donné que les risques opérationnels sont inhérents au fait d'exercer des activités, l'institution entière y est exposée, notamment par l'insuffisance ou l'inefficacité des contrôles sur les personnes, les processus, les systèmes ou les évènements externes[5]. Le déploiement des nouvelles technologies ainsi que le rythme soutenu des changements structurels viennent exacerber l'exposition des institutions financières à ces risques opérationnels.

Dans cette optique, l'Autorité considère donc le risque opérationnel comme l'un des risques majeurs auxquels les institutions financières sont exposées. Ainsi, dans l'esprit d'adhérer aux principes directeurs en la matière et compte tenu de l'importance croissante de ce risque, l'Autorité considère essentiel d'établir ses attentes quant à la gestion requise des risques opérationnels. Au chapitre de la gouvernance, la mise en oeuvre de cette ligne directrice vise à promouvoir le renforcement de la culture de risques puisque l'identification, l'évaluation, le contrôle, l'atténuation et la surveillance de risques opérationnels demandent l'engagement des différentes parties de l'institution, et au premier chef, du conseil d'administration, de la haute direction et des différentes lignes de défense[6].

En outre, la gestion des risques inhérents aux personnes, processus et systèmes facilite la définition de niveaux de tolérance au risque opérationnel et la surveillance des risques par segment d'affaires ainsi que l'optimisation des processus et systèmes d'information, comme le préconise la *Ligne directrice sur la gestion intégrée des risques*[7].

Compte tenu de sa nature générale, cette ligne directrice se situe dorénavant en amont de l'encadrement plus spécifique portant sur des sujets liés au risque opérationnel, notamment sur la gestion de la continuité des activités[8] ainsi que la gestion des risques

---

3 BANK FOR INTERNATIONAL SETTLEMENTS. *Operational Risk Management*, September 1998.

4 INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS. *Insurance Core Principles*, updated November 2015.

5 Le Comité de Bâle définit le risque opérationnel comme le risque de pertes dues à des personnes, processus ou systèmes inadéquats ou défaillants, ou résultants d'évènements extérieurs. Cette définition comprend le risque juridique, mais exclut le risque stratégique et le risque de réputation. BANK FOR INTERNATIONAL SETTLEMENTS. *Principles for the Sound Management of Operational Risk*, June 2011.

6 AUTORITÉ DES MARCHÉS FINANCIERS. *Ligne directrice sur la gouvernance,* avril 2009. Un projet de modification à la *Ligne directrice sur la gouvernance* a été publié pour consultation le 31 mars 2016.

7 AUTORITÉ DES MARCHÉS FINANCIERS. *Ligne directrice sur la gestion intégrée des risques*, avril 2009, mise à jour en mai 2015.

8 AUTORITÉ DES MARCHÉS FINANCIERS. *Ligne directrice sur la gestion de la continuité des activités*, avril 2010.

liés à l'impartition[9] et à la criminalité financière[10]. Conséquemment, tout nouvel encadrement prudentiel en matière de risques inhérents aux personnes, processus, systèmes ou évènements externes nécessitera que des précisions soient apportées aux grands principes énoncés dans la présente.

Il importe de noter que la présente ligne directrice ne considère ni la modélisation ni la quantification du risque opérationnel puisque ce sujet est spécifiquement abordé dans l'encadrement relatif aux exigences de capital des différentes entités mentionnées au champ d'application. Par ailleurs, les orientations prudentielles à l'égard de la gestion du risque opérationnel doivent être comprises comme étant complémentaires aux exigences du capital en vigueur plutôt que comme une conséquence de cette activité, comme le suggère le Comité de Bâle[11].

9 AUTORITÉ DES MARCHÉS FINANCIERS. *Ligne directrice sur la gestion de risques liés à l'impartition*, avril 2009 (mise à jour décembre 2010).

10 AUTORITÉ DES MARCHÉS FINANCIERS. *Ligne directrice sur la gestion de risques liés à la criminalité financière*, juin 2012.

11 BANK FOR INTERNATIONAL SETTLEMENTS. *Review of the Principles for the Sound Management of Operational Risk*, October 2014.

1. Gestion du risque opérationnel

L'Autorité s'attend à ce que l'institution financière gère adéquatement son risque opérationnel en lien avec sa stratégie et son appétit pour le risque. Cette gestion devrait considérer l'exposition aux risques opérationnels de toutes les personnes, activités, processus et systèmes de l'institution de même que l'exposition à ces risques des tierces parties.

Gestion du risque opérationnel

Comme préconisé par la *Ligne directrice sur la gestion intégrée de risques*, la gestion adéquate des risques débute par la promotion d'une solide culture de risques. En ce qui a trait aux risques opérationnels, l'établissement d'une telle culture doit nécessairement émaner du conseil d'administration et de la haute direction et être modulé en fonction de l'ampleur de l'exposition aux risques opérationnels et, conséquemment, de l'engagement requis de tous les paliers de l'institution, afin de bien gérer ces types de risques.

Cette initiative de sensibilisation devrait viser notamment les intervenants engagés dans la mise en œuvre des différents produits, activités, processus et systèmes au sein de l'institution.

La sensibilisation devrait viser également les parties prenantes hors de l'institution, notamment les fournisseurs de services clés, du fait que l'impartition expose l'institution aux risques opérationnels (p. ex., l'exposition aux cyberrisques). De plus, le renforcement de la culture passe par l'offre de formation continue sur le traitement de risques opérationnels, laquelle devrait relever des responsables de toutes les unités[12].

Bien que les orientations de la *Ligne directrice sur la gestion intégrée de risques* soient applicables à tous les types de risques, le risque opérationnel demande une gestion particulière, voire plus englobante, du fait qu'il sollicite l'engagement des responsables de l'ensemble des activités, processus et systèmes d'une institution financière.

La gestion du risque opérationnel devrait aussi déceler les situations où la conduite des intervenants associés à un produit, une activité, un processus ou un système en particulier, n'assurent pas le traitement équitable du consommateur[13]. À titre d'exemple, une brèche dans la sécurité de l'information causée par une divulgation accidentelle de renseignements personnels d'un client ou une fuite d'informations confidentielles résultant d'un acte délibéré constituent la matérialisation d'un risque opérationnel susceptible de nuire au traitement équitable du consommateur, lequel pourrait ultimement atteindre la réputation d'une institution.

L'efficacité de cette gestion devrait être régulièrement validée et vérifiée, notamment en fonction de la variation de l'exposition aux risques opérationnels. Cette variation serait attribuable, par exemple, à la mise en marché de nouveaux produits ou aux

12 Dans le contexte de la présente ligne directrice, une unité correspond à la plus petite composante de l'institution à laquelle lui est attribuée une responsabilité opérationnelle ou administrative.

13 AUTORITÉ DES MARCHÉS FINANCIERS. *Ligne directrice sur les saines pratiques commerciales,* juin 2013.

modifications résultant des transformations organisationnelles touchant les processus et systèmes (p. ex., cession, acquisition, fusion).

Conséquemment à ces changements, il peut s'avérer nécessaire de réviser les niveaux de tolérance au risque opérationnel. Toutefois, il est attendu qu'une décision de cette nature soit le fruit de discussions entre toutes les parties prenantes. À ce titre, l'approbation du conseil d'administration serait requise.

La gestion du risque opérationnel devrait servir à valider l'efficacité des mécanismes de contrôle interne en place. Il est attendu que ces contrôles soient établis en fonction du niveau de tolérance au risque opérationnel afin de respecter les niveaux de tolérance au risque déterminés par chaque secteur d'activité ainsi que de proposer d'autres contrôles mieux adaptés à la situation, le cas échéant.

Identification et évaluation des risques opérationnels

L'Autorité s'attend à ce que toutes les parties intéressées au sein de l'institution contribuent à l'identification et à l'évaluation du risque opérationnel inhérent à leurs secteurs d'activité respectifs. Afin d'uniformiser l'identification de ce type de risque, l'institution devrait se doter d'une taxonomie et d'outils d'identification communs permettant aux instances décisionnelles de bénéficier d'une vision complète de l'exposition aux risques opérationnels.

Plusieurs outils sont à la disposition des institutions financières pour faciliter leur effort d'identification et d'évaluation du risque opérationnel. Parmi ces outils, mentionnons par exemple :

- les exercices d'autoévaluation des risques;
- les analyses de l'efficacité de contrôles;
- les analyses des évènements de perte, tant à l'intérieur qu'à l'extérieur de l'institution;
- les analyses de risques spécifiques à chaque produit, processus et système en place;
- les analyses de scénarios établis à partir de l'opinion d'experts;
- les modèles de quantification de l'exposition.

L'Autorité ne privilégie aucun outil d'identification ou d'évaluation de risques opérationnels en particulier puisqu'il appartient à l'institution de les mettre en œuvre en fonction de sa taille, sa nature, sa complexité et son profil de risque. L'outil ou l'ensemble des outils sélectionné devrait être utilisé de façon uniforme dans toutes les unités afin de parvenir à une évaluation complète de l'exposition aux risques opérationnels.

Considérant les attentes émises par l'Autorité dans sa *Ligne directrice sur la gestion des risques liés à l'impartition*, les risques opérationnels inhérents à toutes les ententes d'impartition importantes devraient être identifiés et évalués. De plus, l'institution

financière devrait s'assurer que ses fournisseurs de services clés respectent les meilleures pratiques en matière de gestion du risque opérationnel.

En outre, les processus internes d'approbation de nouveaux produits, activités, processus ou systèmes devraient considérer l'identification et l'évaluation de ses risques opérationnels inhérents en s'assurant que le niveau de tolérance pour ce type de risque ne soit pas dépassé.

Surveillance et divulgation

L'Autorité s'attend à ce que les rapports sur les risques opérationnels reflètent les actions prises par l'institution afin d'établir les sources significatives de risques qui seraient non atténués et ultimement respecter son niveau de tolérance à ces risques. En particulier, il est attendu que l'efficacité et l'efficience de mesures de contrôle en place soient surveillées et que les principales actions envisagées permettant de mitiger la fréquence et l'impact d'incidents opérationnels soient divulguées[14].

Les meilleures pratiques militent en faveur de la constitution d'un registre d'incidents, lequel devrait être utilisé pour y inscrire les dépassements de limites ou de niveaux de tolérance préétablis de risques opérationnels. De plus, l'institution devrait s'assurer que la procédure de mise à jour de ce registre s'effectue de façon cohérente dans toutes les unités à partir de politiques déterminées au préalable.

À partir de l'analyse des incidents les plus significatifs inscrits, par exemple, au registre, les rapports sur les risques opérationnels devraient permettre au conseil d'administration et à la haute direction d'établir les principales sources du risque opérationnel non atténuées. Ces rapports devraient inclure notamment la provenance, soit interne ou externe, ainsi que l'ensemble des impacts attendus[15]. En outre, les rapports devraient incorporer les recommandations effectuées tant par l'Autorité que par les fonctions d'audit, le cas échéant, au sujet de la gestion du risque opérationnel ainsi que les plans d'action correspondants approuvés par les instances décisionnelles.

Par ailleurs, le conseil d'administration et la haute direction devraient déterminer la façon la plus adéquate de présenter l'efficacité de leur gestion du risque opérationnel aux parties intéressées.

Contrôle et atténuation

L'Autorité s'attend à ce que les mécanismes de contrôle interne permettent d'atténuer efficacement l'exposition au risque opérationnel inhérent aux personnes, activités, processus et systèmes reliés à l'opération de l'institution financière.

[14] AUTORITÉ DES MARCHÉS FINANCIERS. *Ligne directrice sur l'agrégation des données sur les risques et la divulgation des risques,* Février 2016.

[15] La *Ligne directrice sur la continuité des activités* recommande l'établissement des processus pour l'identification des incidents opérationnels majeurs.

L'Autorité a déjà exprimé ses attentes quant aux mécanismes de contrôle interne dans sa *Ligne directrice sur la gouvernance*. En lien avec la gestion du risque opérationnel, il est attendu que ces mécanismes permettent de mitiger efficacement l'exposition de toutes les personnes, activités, processus et systèmes de l'institution aux risques opérationnels. Ces mécanismes doivent être modifiables, notamment en fonction de l'évolution de ses affaires et des changements technologiques.

Indépendamment de mécanismes privilégiés par chaque institution, il est attendu que leur mise en place soit uniforme et adaptable aux changements majeurs dans les activités, processus et systèmes liés aux opérations.

En outre, les institutions financières ayant recours à une couverture d'assurance pour le transfert du risque de nature opérationnel devraient toujours l'utiliser de façon complémentaire à leurs propres mécanismes de contrôle pour ce type de risque.

2. Gouvernance

Rôle du conseil d'administration et de la haute direction

L'Autorité s'attend à ce que le conseil d'administration et la haute direction mettent en place une solide structure de gouvernance afin de favoriser la conformité des orientations en matière de gestion du risque opérationnel.

La mise en place d'une solide structure de gouvernance comme l'énonce la *Ligne directrice sur la gouvernance* et la *Ligne directrice sur les critères de probité et de compétence*[16] est essentielle à la saine gestion du risque opérationnel.

L'un des rôles du conseil d'administration est de s'assurer que la haute direction déploie tous les efforts pour sensibiliser les unités sur l'importance de gérer leur exposition au risque opérationnel. De même, la haute direction devrait s'assurer d'offrir une formation spécifique en la matière aux parties prenantes, notamment aux gestionnaires de ces unités. Ainsi, le conseil d'administration devrait s'assurer que les membres de la haute direction s'appuient sur une expertise collective dans la gestion du risque opérationnel.

Le conseil d'administration demeure responsable de l'approbation de l'encadrement de la gestion du risque opérationnel, conformément aux rôles et responsabilités qui lui sont dévolus dans la *Ligne directrice sur la gouvernance*. De plus, le conseil d'administration devrait s'assurer de l'efficacité de cet encadrement, de sa cohésion avec la gestion intégrée de risques et de l'adaptation continue du niveau de tolérance au risque opérationnel, en s'appuyant notamment sur les travaux de l'audit interne.

Quant à la cohésion de la gestion du risque opérationnel avec le cadre de gestion intégrée des risques, la haute direction devrait veiller à la coordination appropriée entre les responsables de différents types de risques. Cette coordination est aussi requise dans toutes les unités afin d'éviter la duplication d'efforts liés à la gestion de risques. De ce fait, les lignes de défense devraient être appelées à valider et vérifier l'intégration des efforts de coordination de la gestion de différents types de risques.

Par la suite, il est attendu que la haute direction s'assure de la mise en place d'une procédure pour la divulgation des dépassements des limites du risque opérationnel dans un registre d'incidents. Le registre, ainsi que tout autre mécanisme déployé pour la divulgation de risques opérationnels, devrait être utilisé par toutes les unités et consulté par les instances décisionnelles comme source d'information sur les améliorations requises au cadre de gestion pour ce type de risques.

De plus, advenant un changement organisationnel ou technologique majeur dans une institution, le conseil d'administration et la haute direction devraient s'assurer que ce changement respecte leur niveau de tolérance au risque opérationnel.

En outre, il est attendu que la haute direction s'assure que l'exposition au risque opérationnel résultant des ententes d'impartition d'importance soit considérée par les

[16] AUTORITÉ DES MARCHÉS FINANCIERS. *Ligne directrice sur les critères de probité et compétence*, juin 2012.

responsables de la gestion du risque opérationnel de différentes unités. De plus, l'évaluation de toute nouvelle entente d'impartition d'importance devrait valider la solidité de la gestion du risque opérationnel du fournisseur ou du consultant concerné.

Le conseil d'administration et la haute direction devraient s'appuyer sur les différentes lignes de défense pour valider et vérifier que la gestion du risque opérationnel est appliquée à toutes les activités, processus et systèmes de l'institution. Pour y arriver, ils devraient s'assurer que chaque ligne de défense dispose des ressources nécessaires pour bien accomplir ses responsabilités et que leurs travaux soient adéquatement coordonnés.

Rôles des lignes de défense

Puisque l'exposition au risque opérationnel est inhérente à tous les produits, activités, processus et systèmes, l'Autorité s'attend à ce que la structure de gouvernance de l'institution soit renforcée par la participation permanente des différentes lignes de défense visant l'optimisation de la gestion du risque opérationnel.

La saine gestion du risque opérationnel devrait être assurée par les responsables de la première ligne de défense, dans tous les produits, les activités, les processus et les systèmes liés à ses fonctions. À cet effet, ces personnes doivent posséder ou acquérir les compétences requises en matière de gestion du risque opérationnel, et leurs responsabilités doivent être documentées.

En outre, les responsables de la première ligne de défense doivent divulguer les dépassements des niveaux de tolérance au risque de leur unité en utilisant, par exemple, un registre d'incidents de risques opérationnels. Ces personnes sont aussi responsables de traiter les risques opérationnels inhérents à tout nouveau produit, processus ou système mis en œuvre par leur unité.

Pour ce qui est de la deuxième ligne de défense, elle devrait être responsable de mettre en œuvre une taxonomie commune permettant l'identification de risques opérationnels et la standardisation des mécanismes de gouvernance pour ce type de risques. À leur tour, les responsables de la première ligne de défense doivent s'approprier cette taxonomie et l'utiliser dans leur gestion du risque opérationnel.

Il est primordial que la deuxième ligne de défense soit indépendante des activités afin qu'elle juge adéquatement l'efficacité des contrôles et d'autres mesures d'atténuation de risques opérationnels mises en place par la première ligne de défense.

Afin de veiller à l'efficacité de la gestion du risque opérationnel, les intervenants des deux premières lignes de défense devraient être en communication constante, en particulier lorsqu'il existe des différences quant à la perception et au traitement de risques opérationnels d'une unité en particulier. Il appartiendra ultimement au responsable de la gestion des risques de décider, par exemple, de la stratégie à adopter advenant le cas où des divergences majeures persistaient.

En outre, la deuxième ligne de défense devrait assurer la coordination de ses activités avec tous les intervenants à l'intérieur de l'institution en ce qui a trait aux risques spécifiques aux personnes, processus et systèmes.

Le projet de modification à la *Ligne directrice sur la gouvernance* mentionne que la deuxième ligne de défense comprend, entre autres, la supervision de la gestion des risques. Conséquemment, la gestion du risque opérationnel requiert l'intervention d'une personne ou d'une équipe dédiée à ce risque, idéalement sous la responsabilité du chef de la gestion de risques. À défaut de l'existence d'un tel poste, compte tenu de la taille, la nature, la complexité et le profil de risque de l'institution, celui-ci devrait être confié, par exemple, à un membre de la haute direction.

Pour sa part, la troisième ligne de défense devrait être responsable de vérifier, de façon indépendante, la gestion du risque opérationnel exercée par les deux premières lignes de défense. Il est aussi attendu que cette ligne de défense évalue le rôle de la haute direction au chapitre de la sensibilisation de tous les paliers de l'institution quant à la gestion adéquate du risque opérationnel, la surveillance du niveau de tolérance de risques opérationnels, ainsi que la cohésion efficace de la gestion du risque opérationnel avec celle des autres risques majeurs de l'institution.

3. Surveillance des pratiques de gestion saine et prudente

En lien avec sa volonté de favoriser l'instauration de pratiques de gestion saine et prudente au sein des institutions financières, l'Autorité entend procéder, dans le cadre de ses travaux de surveillance, à l'évaluation du degré d'observance des principes et orientations énoncés dans la présente ligne directrice.

En conséquence, l'efficacité et la pertinence des stratégies politiques et procédures mises en place, la qualité de la supervision et le contrôle exercé par le conseil d'administration et la haute direction seront évalués.

Les pratiques en matière de gestion du risque opérationnel évoluent constamment. L'Autorité s'attend à ce que les instances décisionnelles de l'institution financière connaissent les meilleures pratiques en la matière et se les approprient dans la mesure où celles-ci répondent à leurs besoins.