AUTORITÉ
DES MARCHÉS
FINANCIERS

LIGNE DIRECTRICE SUR LA GESTION DU RISQUE OPÉRATIONNEL

Décembre 2016

TABLE DES MATIÈRES

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 »)[1] 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[2]. 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.

Le risque opérationnel se définit comme étant le risque de pertes dues à des défaillances ou inadéquations attribuables à des personnes, des processus des systèmes ou résultant d'évènements externes[3]. 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 œuvre 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 intéressées internes[4], et au premier chef, du conseil d'administration, de la haute direction et des différentes lignes de défense[5].

En outre, la gestion des risques inhérents aux personnes, processus, systèmes et évènements externes facilite la définition de niveaux de tolérance au risque opérationnel et la surveillance des risques par unité/secteur[6] 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 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

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

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

3 Cette définition inclut 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.

4 Selon la norme ISO 9001: 2015, l'expression « parties intéressées » inclut tout organisme ou toute personne ou pouvant être affecté(e) par une décision ou une activité. En plus, le Principe 5 adopté par les pays du G7 pour défendre le système financier contre les cyberattaques cite des exemples de parties intéressées à la fois internes et externes, telles que les autorités judiciaires, les autorités de réglementation et d'autres autorités publiques, de même que les actionnaires, les fournisseurs de services découlant d'ententes d'impartition et les consommateurs, le cas échéant.G7.* Fundamental Elements of Cybersecurity for the Financial Sector, Principe *5, October 2016.

5 AUTORITÉ DES MARCHÉS FINANCIERS. *Ligne directrice sur la gouvernance*.

6 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. À noter qu'un secteur d'affaires peut être formé d'une ou de plusieurs unités.

7 AUTORITÉ DES MARCHÉS FINANCIERS. *Ligne directrice sur la gestion intégrée des risques*.

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

9 AUTORITÉ DES MARCHÉS FINANCIERS. *Ligne directrice sur la gestion de risques liés à l'impartition*.

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

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].

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

1. Gouvernance de l'institution financière

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 est essentielle à la saine gestion du risque opérationnel.

1.1 Rôles et responsabilités du conseil d'administration

Dans le cadre précis de la gestion des risques opérationnels et en lien avec les attentes énoncées à la *Ligne directrice sur la gouvernance* et à la *Ligne directrice sur la gestion intégrée des risques*, le conseil d'administration devrait notamment :

- examiner périodiquement et approuver le cadre de gestion des risques opérationnels;
- examiner périodiquement et approuver le niveau de tolérance au risque opérationnel, en s'appuyant notamment sur les travaux de l'audit interne.
- s'assurer de l'application effective du cadre de gestion des risques opérationnels;
- s'assurer de l'efficacité du cadre de gestion du risque opérationnel et de sa cohésion avec le cadre de gestion intégrée des risques;
- veiller à ce que la haute direction fasse la promotion d'une culture de bonne gestion du risque opérationnel;

1.2 Rôles et responsabilités de la haute direction

Dans le cadre précis de la gestion des risques opérationnels et en lien avec les attentes énoncées à la *Ligne directrice sur la gouvernance* et à la *Ligne directrice sur la gestion intégrée des risques*, la haute direction devrait notamment :

- mettre en œuvre et maintenir des politiques, des processus et des systèmes appropriés au cadre de gestion et aux niveaux de tolérance des risques opérationnels;
- s'assurer de la présence de mécanismes adéquats de divulgation des dépassements de niveaux de tolérance au risque opérationnel;
- s'assurer de bien définir les rôles et rapports hiérarchiques afin de délimiter les responsabilités et d'assurer le maintien quant à l'imputabilité des risques opérationnels;
- s'assurer de la disponibilité, la suffisance et l'adéquation des ressources pour une bonne gestion du risque opérationnel;
- s'assurer de la coordination appropriée et de la communication efficace[12] entre, d'une part, le chef de la gestion des risques et le responsable de la gestion des risques opérationnels et, d'autre part, entre ces derniers et les gestionnaires des secteurs d'affaires ainsi que les responsables des services impartis[13];

[12] AUTORITÉ DES MARCHÉS FINANCIERS. *Ligne directrice sur la gestion intégrée des risques*.
[13] AUTORITÉ DES MARCHÉS FINANCIERS. *Ligne directrice sur la gestion des risques liés à l'impartition*.

- veiller au maintien des compétences par la dispense de formations spécifiques aux responsables et équipes impliquées dans les risques opérationnels .

Certes, le conseil d'administration et la haute direction sont responsables au premier chef de l'élaboration du cadre de gestion des risques opérationnels de même que la promotion d'une culture de gestion des risques. Toutefois, ils peuvent bénéficier de l'appui des 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.

1.3 Rôles et responsabilités des lignes de défense

> Afin d'optimiser la gestion du risque opérationnel, l'institution financière devrait disposer d'une structure de gouvernance fiable en s'inspirant du modèle des trois lignes de défense[14].

Le modèle des trois lignes de défense permet d'établir une distinction entre les rôles et responsabilités des intervenants en matière de gestion du risque opérationnel. Il devrait également être établi en fonction de la nature, de la taille, de la complexité des activités et du profil de risque de l'institution financière.

Ce modèle devrait en outre permettre de coordonner les initiatives visant à améliorer les pratiques de gestion du risque opérationnel au sein de l'institution financière en lien avec des facteurs plus subjectifs comme sa culture et ses valeurs.

L'Autorité a déjà exprimé ses attentes quant aux rôles et responsabilités des lignes de défense dans sa *Ligne directrice sur la gouvernance*. Les institutions financières devraient s'en inspirer et adapter ces notions au contexte de gestion des risques opérationnels.

2. 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 inhérents aux personnes, processus, systèmes ou évènements externes de l'institution de même que l'exposition de tierces parties à ces risques.

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.

La sensibilisation devrait aussi viser les parties intéressées externes, notamment les fournisseurs de services découlant d'ententes d'impartition importantes, 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 tous les secteurs d'affaires.

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 est inhérent aux personnes, processus, systèmes ou évènements externes de l'institution financière et 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'assure pas le traitement équitable du consommateur. 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 d'une variation importante de l'exposition aux risques opérationnels. Cette variation serait attribuable, par exemple, à la mise en marché de nouveaux produits ou aux modifications résultant des transformations organisationnelles touchant les personnes, les processus, les systèmes ou attribuables à des évènements externes (p. ex., cession, acquisition, fusion). Conséquemment à ces changements, il peut s'avérer nécessaire de réviser les niveaux de tolérance au risque opérationnel.

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'affaires ainsi que de proposer d'autres contrôles mieux adaptés à la situation, le cas échéant.

2.1 Identification et évaluation des risques opérationnels

> L'Autorité s'attend à ce que l'institution financière se dote d'une taxonomie des différents types de risques opérationnels afin d'uniformiser l'identification, la catégorisation et l'évaluation de ces risques et en assurer une attribution adéquate des responsabilités quant à leur atténuation et leur suivi.

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 d'affaires 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, découlant d'ententes d'impartition importantes, ont la capacité d'assurer un service de qualité.

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.

2.2 Surveillance et divulgation

> L'Autorité s'attend à ce que les rapports sur les risques opérationnels reflètent les niveaux de tolérance aux risques de l'institution financière. Ils doivent aussi permettre le suivi de l'évolution de l'exposition aux risques ainsi que l'efficacité et l'efficience des mesures mises en place pour leur traitement.

Les meilleures pratiques militent en faveur de la constitution d'un registre d'incidents, lequel devrait être utilisé pour y inscrire les dépassements des niveaux de tolérance préétablis de risques opérationnels. De plus, l'institution devrait s'assurer que la procédure de mise à jour de ce registre ou de tout autre mécanisme de divulgation s'effectue de façon cohérente dans tous les unités/secteurs d'affaires 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 potentiels[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, en matière de divulgation et de transparence, l'Autorité s'attend notamment à ce que les institutions financières répondent aux attentes contenues dans la Ligne directrice sur la gouvernance en mettant en place les mécanismes nécessaires pour aviser promptement les parties intéressées internes et externes susceptibles de subir un préjudice d'importance significative suite à un incident opérationnel majeur (cyberincident, dysfonctionnement des systèmes, etc.)[16]. Une telle démarche permettra à l'Autorité, en tant qu'une des parties intéressées, d'être proactive dans l'identification des pratiques pouvant nuire à la gestion des risques opérationnels.

2.3 Contrôle et atténuation

> L'Autorité s'attend à ce que les mécanismes de contrôle interne permettent d'atténuer efficacement l'exposition aux risques opérationnels inhérents aux personnes, processus, systèmes ou évènements externes de l'institution financière selon leur degré d'importance.

L'Autorité a déjà mentionné dans sa *Ligne directrice sur la gouvernance* que les mécanismes de contrôle devraient donner aux instances décisionnelles l'assurance raisonnable quant à l'atteinte des objectifs en matière :

- d'efficacité et d'efficience des opérations;
- de protection des actifs;
- de fiabilité et de transparence de l'information financière et non financière interne et externe;
- de conformité aux lois, règlements et normes applicables.

Il est attendu que ces mécanismes soient adaptables à l'évolution des affaires et des changements technologiques au sein de l'institution financière. En outre, les institutions financières ayant recours à une couverture d'assurance pour le transfert du risque de nature opérationnelle devraient toujours l'utiliser de façon complémentaire à leurs propres mécanismes de contrôle pour ce type de risque.

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

[16] Voir le *Principe 5 dans G7 Fundamental Elements of Cybersecurity for the Financial Sector*, October 2016.