5.2

Réglementation et lignes directrices

5.2 RÉGLEMENTATION ET LIGNES DIRECTRICES

5.2.1 Consultation

Aucune information.

5.2.2 Lignes directrices

Ligne directrice sur la gestion du risque opérationnel
(Loi sur les assurances, RLRQ, c. A-32, art. 325.0.1 et 325.0.2)
(Loi sur les coopératives de services financiers, RLRQ, c. C-67.3, art. 565)
(Loi sur sociétés de fiducie et les sociétés d'épargne, RLRQ, c. S-29.01, art. 314.1)

L'Autorité des marchés financiers (l'« Autorité ») publie la *Ligne directrice sur la gestion du risque opérationnel* (la « Ligne directrice »), s'appliquant aux assureurs de personnes, aux assureurs de dommages, aux sociétés de gestion de portefeuille contrôlées par un assureur, aux coopératives de services financiers ainsi qu'aux sociétés de fiducie et sociétés d'épargne. La date de prise d'effet de la Ligne directrice est le 1er décembre 2016.

La Ligne directrice est publiée ci-après et disponible sur le site Web de l'Autorité au www.lautorite.qc.ca, sous les onglets « Assurance et planification financière » ou « Institutions de dépôt », à la rubrique « Lignes directrices ».

Renseignements additionnels

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

Wassim Ferjani
Direction de l'encadrement prudentiel des institutions financières
Autorité des marchés financiers
Téléphone : (418) 525-0337, poste 4688
Numéro sans frais : 1 877 525-0337
Courrier électronique : wassim.ferjani@lautorite.qc.ca

Le 24 novembre 2016

DÉCISION N° 2016-PDG-0158

Ligne directrice sur la gestion du risque opérationnel

Vu le pouvoir de l'Autorité des marchés financiers (l'« Autorité ») de donner des lignes directrices applicables aux assureurs de personnes, aux assureurs de dommages et aux sociétés de gestion de portefeuille contrôlées par un assureur après consultation du ministre des Finances (le « Ministre ») et de la fédération de sociétés mutuelles d'assurance, le tout, conformément à l'article 325.0.1 et au paragraphe 3° du premier alinéa et au deuxième alinéa de l'article 325.0.2 de la *Loi sur les assurances*, RLRQ, c. A-32 (la « LA »);

Vu le pouvoir de l'Autorité de donner des lignes directrices applicables aux coopératives de services financiers après consultation du Ministre et des fédérations, le tout, conformément au paragraphe 3° du premier alinéa et au deuxième alinéa de l'article 565 de la *Loi sur les coopératives de services financiers*, RLRQ, c. C-67.3 (la « LCSF »);

Vu le pouvoir de l'Autorité de donner des lignes directrices applicables aux sociétés de fiducie et aux sociétés d'épargne après consultation du Ministre, conformément au paragraphe 3° du premier alinéa et au deuxième alinéa de l'article 314.1 de la *Loi sur les sociétés de fiducie et les sociétés d'épargne*, RLRQ, c. S-29.01 (la « LSFSÉ »);

Vu le pouvoir de l'Autorité de donner une ligne directrice prévue à l'article 325.0.1 de la LA, à l'article 565 de la LCSF et à l'article 314.1 de la LSFSÉ, qui appartient exclusivement à son président-directeur général, conformément à l'article 24 de la *Loi sur l'Autorité des marchés financiers*, RLRQ, c. A-33.2;

Vu la publication pour consultation au Bulletin de l'Autorité (le « Bulletin ») le 26 mai 2016 [(2016) vol. 13, n° 21, B.A.M.F., section 5.2.1] du projet de la *Ligne directrice sur la gestion du risque opérationnel* (la « ligne directrice »);

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

Vu la consultation auprès de Groupe Promutuel Fédération de sociétés mutuelles d'assurance générale, conformément à l'article 325.0.1 de la LA et auprès de la Fédération des caisses Desjardins du Québec, conformément à l'article 565 de la LCSF;

Vu la consultation effectuée auprès du Ministre, conformément à l'article 325.0.1 de la LA, à l'article 565 de la LCSF et à l'article 314.1 de la LSFSÉ;

Vu le projet de la ligne directrice proposé par la Direction principale de l'encadrement des institutions financières, de la résolution et de l'assurance-dépôts et la recommandation du surintendant de l'encadrement de la solvabilité de donner celle-ci;

En conséquence :

L'Autorité donne la *Ligne directrice sur la gestion du risque opérationnel*, dans ses versions française et anglaise, dont les textes sont annexés à la présente décision, et en autorise la publication au Bulletin.

La *Ligne directrice sur la gestion du risque opérationnel* prend effet le 1er décembre 2016.

Fait le 22 novembre 2016.

Louis Morisset
Président-directeur général

AUTORITÉ
DES MARCHÉS
FINANCIERS

LIGNE DIRECTRICE SUR LA GESTION DU RISQUE OPÉRATIONNEL

Décembre 2016

TABLE DES MATIÈRES

Préambule **2**

Champ d'application **3**

Prise d'effet et processus de mise à jour **4**

Introduction **5**

1. Gouvernance de l'institution financière **7**

1.1 Rôles et responsabilités du conseil d'administration 7
1.2 Rôles et responsabilités de la haute direction 7
1.3 Rôles et responsabilités des lignes de défense 8

2. Gestion du risque opérationnel **9**

2.1 Identification et évaluation des risques opérationnels 10
2.2 Surveillance et divulgation 11
2.3 Contrôle et atténuation 11

3. Surveillance des pratiques de gestion saine et prudente **13**

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 décembre 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.

L'Autorité s'attend à ce que l'institution financière s'approprie les attentes de la présente ligne directrice et qu'elle les mette en œuvre d'ici le 1er décembre 2017. Dans la mesure où une institution a déjà mis en place un tel encadrement, l'Autorité pourra en vérifier la conformité avec les 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.

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[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 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[6], et au premier chef, du conseil d'administration, de la haute direction et des différentes lignes de défense[7].

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[8] d'affaires ainsi que l'optimisation des

---

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

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

5 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.

6 Selon la norme ISO 9001: 2015, l'expression « parties intéressées » inclut toute personne ou organisme pouvant être affectées 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].

7 AUTORITÉ DES MARCHÉS FINANCIERS. *Ligne directrice sur la gouvernance*, septembre 2016.

8 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.

processus et systèmes d'information, comme le préconise la *Ligne directrice sur la gestion intégrée des risques*[9].

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[10] ainsi que la gestion des risques liés à l'impartition[11] et à la criminalité financière[12]. 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[13].

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

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

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

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

13 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 comme l'énoncent la *Ligne directrice sur la gouvernance*, la *Ligne directrice sur la gestion intégrée des risque*s, et la *Ligne directrice sur les critères de probité et de compétence* 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 :

- établir, approuver et réexaminer périodiquement le cadre de gestion des risques opérationnels;
- veiller à la promotion d'une culture de gestion du risque opérationnel au sein de l'institution financière;
- s'assurer de l'efficacité du cadre de gestion du risque opérationnel et de sa cohésion avec le cadre de gestion intégrée des risques;
- superviser la haute direction afin de s'assurer que le cadre de gestion des risques opérationnels est effectivement appliqué;
- approuver et réexaminer le niveau de tolérance au risque opérationnel, en s'appuyant notamment sur les travaux de l'audit interne.

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, reflétant le cadre gestion du risque opérationnel conformément avec les niveaux de tolérance au risque opérationnel;
- s'assurer de la mise en place de mécanismes adéquats de divulgation des dépassements des niveaux de tolérance au risque opérationnel;
- définir les responsabilités et les rapports hiérarchiques afin de délimiter les attributions et encourager et maintenir l'imputabilité;

- s'assurer de la coordination appropriée et de la communication efficace[14] 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[15];
- veiller à la disponibilité, la suffisance et l'adéquation des ressources pour la gestion des risques opérationnels;
- s'assurer que les formations spécifiques en la matière sur les processus de gestion des risques soient dispensées aux responsables et leurs équipes impliquées.

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[16].

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.

14 AUTORITÉ DES MARCHÉS FINANCIERS. *Ligne directrice sur la gestion intégrée des risques*, mai 2015.

15 AUTORITÉ DES MARCHÉS FINANCIERS. *Ligne directrice sur la gestion des risques liés à l'impartition*, décembre 2010.

16 AUTORITÉ DES MARCHÉS FINANCIERS. *Ligne directrice sur la gouvernance*, septembre 2016.

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 des 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'assurent 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[17]. 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.)[18]. 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 :

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

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

- 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.

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.

AUTORITÉ
DES MARCHÉS
FINANCIERS

OPERATIONAL RISK MANAGEMENT GUIDELINE

December 2016

TABLE OF CONTENTS

Preamble **3**

Coming into effect and updating **5**

Introduction **6**

1. Governance of financial institutions **8**

1.1 Roles and responsibilities of the board of directors 8

2. Operational risk management **10**

2.1 Identification and assessment of operational risk 11
2.2 Monitoring and reporting 11
2.3 Control and mitigation 12

3. Supervision of sound and prudent management practices **13**

Preamble

The *Autorité des marchés financiers* (the "AMF") establishes guidelines setting out its expectations with respect to financial institutions' legal requirement to follow sound and prudent management practices. This guideline therefore covers the interpretation, execution and application of that requirement.

The AMF favours a principles-based approach rather than a specific rules-based approach. As such, the guidelines provide financial institutions with the necessary latitude to determine the requisite strategies, policies and procedures for implementation of such management principles and to apply sound practices based on the nature, size and complexity of their activities. In this regard, the guidelines illustrate how to comply with the principles described.

AMF Note

The AMF considers governance, integrated risk management and compliance (GRC) as the foundation stones for the sound and prudent management and sound commercial practices of financial institutions and, consequently, as the basis for the prudential framework provided by the AMF.

This guideline is part of this approach and sets out the AMF's expectations regarding operational risk management practices.

Scope

This *Operational Risk Management Guideline* is intended for insurers of persons (life and health), damage (P&C) insurers, portfolio management companies controlled by an insurer, financial services cooperatives as well as trust and savings companies, which are governed by the following Acts:

- *An Act respecting insurance*, CQLR, c. A-32;
- *An Act respecting financial services cooperatives,* CQLR, c. C-67.3;
- *An Act respecting trust companies and savings companies,* CQLR, c. S-29.01.

Lastly, this guideline applies to financial institutions operating independently as well as to financial institutions operating as members of a financial group.[1] As regards financial services cooperatives and mutual insurance associations[2] that are members of a federation, the standards or policies adopted by the federation should be consistent with—and even converge on—the principles of sound and prudent management as detailed in this guideline.

The generic terms “financial institution” and “institution” refer to all financial entities covered by the scope of this guideline.

[1] For purposes of this guideline, “financial group” refers to any group of legal persons composed of a parent company (financial institution or holding company) and legal persons affiliated with them.

[2] Mutual insurance associations are damage insurers that are within scope of this guideline.

Coming into effect and updating

This *Operational Risk Management Guideline* comes into effect on December 1, 2016.

With respect to the legal requirement of institutions to follow sound and prudent management practices, the AMF expects each institution to adopt the principles of this guideline in developing strategies, policies and procedures based on its nature, size, complexity and risk profile.

The AMF expects financial institutions to adopt the expectations in this guideline and implement them by December 1, 2017. Where an institution has already implemented such a framework, the AMF may verify its compliance with the prescribed legal requirements.

This guideline will be updated based on operational risk management developments and in light of the AMF's findings in the course of its supervision of financial institutions.

Introduction

Operational risk management has been of growing interest to the financial sector for close to two decades. The Basel Committee on Banking Supervision (the "Basel Committee")[3] was the first in the industry to set out its expectations. The International Association of Insurance Supervisors (IAIS) also recommends the sound management of operational risks.[4] In response to these increasing concerns of international bodies, several members of the Organisation for Economic Co-operation and Development (OECD) have published guidance regarding operational risk management.

Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.[5] The use of new technology and the sustained pace of structural change increase financial institutions' exposure to such risks.

The AMF therefore considers operational risk to be one of the major risks to which financial institutions are exposed. With the aim of adhering to guiding principles in such matters and in view of the growing importance of this risk, the AMF considers it essential to set out its expectations regarding the necessary management of operational risk. With respect to governance, this guideline aims to promote the strengthening of the risk culture since the identification, assessment, control, mitigation and oversight of operational risk require the commitment of all internal stakeholders[6] and primarily the board of directors, senior management and the different lines of defence.[7]

In addition, the management of risks inherent to people, processes, systems and external events helps determine the level of tolerance to operational risk and the oversight of risks according to business sector[8], along with the optimization of processes and information systems, as recommended in the *Integrated Risk Management Guideline*.[9]

Given the general nature of this guideline, it will henceforth be the umbrella guideline for more specific guidelines on areas related to operational risk, including business continuity management,[10] outsourcing risk management[11] and financial crime risk

---

3 Bank for International Settlements. *Operational Risk Management*, September 1998.

4 International Association of Insurance Supervisors. *Insurance Core Principles*, updated November 2015.

5 This definition includes legal risk, but excludes strategic and reputational risk. Bank for International Settlements. *Principles for the Sound Management of Operational Risk*, June 2011.

6 According to ISO 9001: 2015, the expression "stakeholders" includes any person or organization that may be affected by a decision or activity. In addition, Principle 5, adopted by the G7 countries to protect the financial system against cyberattacks, cites examples of both internal and external stakeholders, such as law enforcement, regulators and other public authorities, as well as shareholders, third-party service providers and consumers, as appropriate. [G7, *Fundamental Elements of Cybersecurity for the Financial Sector*, Principle 5, October 2016].

7 Autorité des marchés financiers. *Governance Guideline,* September 2016.

8 For the purposes of this guideline, a unit corresponds to the institution's smallest component to which operational or administrative responsibility is given. A business sector can consist of one or more units.

9 Autorité des marchés financiers. *Integrated Risk Management Guideline,* April 2009, updated May 2015.

10 Autorité des marchés financiers. *Business Continuity Management Guideline,* April 2010.

management.[12] As a result, any new prudential framework regarding the risks inherent to people, processes, systems or external events will clarify the broad principles set forth herein.

It is important to note that this guideline does not consider either the modeling or quantification of operational risk since these issues are specifically discussed in the framework relating to the capital requirements of the various entities referred to above. Furthermore, the prudential orientations regarding operational risk management should be seen as complementary to the calculation of operational risk capital requirements rather than a consequence of that activity, as suggested by the Basel Committee.[13]

[11] Autorité des marchés financiers. *Outsourcing Risk Management Guideline*, April 2009, updated December 2010.

[12] Autorité des marchés financiers. *Financial Crime Risk Management Guideline*, June 2012.

[13] Bank for International Settlements. *Review of the Principles for the Sound Management of Operational Risk*, October 2014.

1. Governance of financial institutions

The AMF expects the board of directors and senior management to set up a sound governance structure to foster compliance with operational risk management orientations.

The implementation of a reliable governance structure as set forth in the *Governance Guideline,* the *Integrated Risk Management Guideline* and the *Guideline Governing Integrity and Competency Criteria* is essential to the sound management of operational risk.

1.1 Roles and responsibilities of the board of directors

In keeping with the operational risk management framework and the expectations in the *Governance Guideline* and the *Integrated Risk Management Guideline*, the board of directors should:

- establish, approve and periodically re-examine the operational risk management framework;
- ensure the promotion of an operational risk management culture within the financial institution;
- ensure the effectiveness of the operational risk management framework and its consistency with the integrated risk management framework;
- supervise senior management to ensure that the operational risk management framework is being applied;
- approve and re-examine the operational risk tolerance level, supported principally by the work of the internal audit function.

1.1 Roles and responsibilities of senior management

In keeping with the operational risk management framework and the expectations in the *Governance Guideline* and the *Integrated Risk Management Guideline,* senior management should:

- implement and maintain policies, processes and systems reflecting the operational risk management framework in accordance with operational risk tolerance levels;
- ensure that adequate mechanisms are set up for reporting situations where operational risk tolerance levels are exceeded;
- establish hierarchical responsibilities and reporting in order to delineate the allocation of duties and promote and maintain accountability;
- ensure appropriate co-ordination and effective communication[14] between, on one hand, the chief risk officer and the operational risk officer and, on the other hand, between these two individuals, business line managers and outsourcing officers;[15]

[14] Autorité des marchés financiers. *Integrated Risk Management Guideline,* May 2015.

- ensure the availability, sufficiency and adequacy of operational risk management resources;
- ensure that targeted risk management training is given to managers and their teams.

The board of directors and senior management have primary responsibility for defining the operational risk management framework and promoting a risk management culture. However, they can rely on the support of the various lines of defence to validate and verify that operational risk management is being applied to all of the institution's activities, processes and systems.

To do this, they must ensure that each line of defence has the necessary resources and that their work is co-ordinated appropriately.

1.2 Roles and responsibilities of the lines of defence

In order to optimize operational risk management, a financial institution should have a sound governance structure that is based on the three lines of defence model.[16]

The three lines of defence model delineates between the roles and responsibilities of the various operational risk management stakeholders. It should be established in light of the financial institution's nature, size, risk profile and operational complexity.

This model should also enable the institution to co-ordinate initiatives to improve its operational risk management practices in regard to more subjective factors, such as its culture and values.

The AMF has already articulated its expectations concerning the roles and responsibilities of the lines of defence in its *Governance Guideline*. Financial institutions should draw on these concepts and adapt them to their operational risk management context.

[15] Autorité des marchés financiers. *Outsourcing Risk Management Guideline*, December 2010.

[16] Autorité des marchés financiers. *Governance Guideline,* September 2016.

2. Operational risk management

The AMF expects financial institution to adequately manage operational risk in relation to strategy and risk appetite. Such management should take into account the institution's operational risk exposure inherent to people, processes, systems or external events as well as the exposure of third parties to these risks.

As recommended by the *Integrated Risk Management Guideline*, adequate risk management begins with promoting a sound risk culture. In terms of operational risks, the establishment of such a culture must come from the board of directors and senior management and be modeled on the extent of operational risk exposure and, accordingly, the commitment required by all levels of the institution to properly manage these risks.

This awareness should also extend to external stakeholders, including material third-party service providers, since outsourcing exposes an institution to operational risks (e.g., cyber-risk exposure). In addition, the culture can be strengthened by providing ongoing training on operational risks to individuals in charge of all business sectors.

Although the orientations of the *Integrated Risk Management Guideline* apply to all types of risk, operational risk calls for special and more comprehensive management since it is inherent in the people, processes, systems and external events of a financial institution and solicits the commitment of those in charge of the financial institution's activities, processes and systems.

Operational risk management should also bring to light situations where the conduct of stakeholders associated with particular products, activities, processes or systems does not ensure the fair treatment of consumers. For example, a security breach caused by the accidental disclosure of a customer's personal information or the deliberate leaking of confidential information is a form of operational risk that might affect the fair treatment of consumers, which could ultimately harm an institution's reputation.

The effectiveness of such management should be validated and verified regularly, based in particular on a significant variation in exposure to operational risk, which could be attributable to factors such as the marketing of new products or changes resulting from organizational transformations affecting people, processes and systems or from external events (e.g., a transfer, acquisition or merger). Such changes can require a review of operational risk tolerance levels.

Operational risk management should serve to validate the effectiveness of the internal control mechanisms in place. It is expected that such controls will be established based on the level of operational risk tolerance in order to comply with the risk tolerance levels determined by each business sector and propose other controls better adapted to the situation, as applicable.

2.1 Identification and assessment of operational risk

The AMF expects financial institutions to set up taxonomy of operational risks in order to standardize the identification, classification and assessment of these risks and ensure the adequate allocation of duties for mitigating and monitoring them.

Several tools are available to financial institutions to facilitate their efforts to identify and assess operational risk. They include:

- risk self-assessment;
- control effectiveness analysis;
- internal and external loss event analysis;
- risk analysis specific to each current product, process and system;
- expert-based scenario analysis;
- exposure quantification modeling.

The AMF does not promote particular tools for identifying or assessing operational risk; it is up to institutions to choose and implement them based on their size, nature, complexity and risk profile. The chosen tool or set of tools should be used consistently throughout all business sectors in order to arrive at a comprehensive assessment of operational risk exposure.

In view of the expectations set forth by the AMF in its *Outsourcing Risk Management Guideline*, the operational risks inherent in all material outsourcing arrangements should be identified and assessed. Moreover, financial institutions should ensure that material third-party service providers are able to provide quality service.

In addition, internal procedures for approving new products, activities, processes or systems should encompass the identification and assessment of inherent operational risk by ensuring that the tolerance level for this type of risk is not exceeded.

2.2 Monitoring and reporting

The AMF expects operational risk reports to reflect a financial institution's risk tolerance levels. They must also enable the institution to track changes in risk exposure and the effectiveness and efficiency of the measures put in place to manage such risks.

Best practices advocate in favour of setting up a register to record incidents where pre-established operational risk levels are exceeded. An institution should ensure that the procedure for updating the register or any other disclosure mechanism is consistent across all business sectors according to pre-established policies.

Based on an analysis of the most significant incidents in the register, operational risk reports should allow the board of directors and senior management to identify the main sources of unmitigated operational risk. Such reports should include the source, whether

internal or external, as well as all potential impacts.[17] They should also incorporate the recommendations made by both the AMF and the audit functions, where applicable, about managing operational risk as well as the corresponding action plans approved by decision-making bodies.

Furthermore, the AMF expects financial institutions to meet the disclosure and transparency expectations set out in the *Governance Guideline* by implementing the necessary mechanisms for promptly advising internal and external stakeholders likely to sustain serious harm due to a major operational incident (cyber incident, system failure, etc.).[18] Such an approach will enable the AMF, as a stakeholder, to be proactive in identifying practices that can undermine operational risk management.

2.3 Control and mitigation

The AMF expects internal control mechanisms to efficiently mitigate the financial institution's operational risk exposure inherent to people, processes, systems or external events, according to their importance.

The AMF has indicated in its *Governance Guideline* that control mechanisms should give decision-making bodies reasonable assurance that the objectives relating to the following will be met:

- operational effectiveness and efficiency;
- safeguarding of assets;
- reliability and transparency of internal and external financial and non-financial information;
- compliance with applicable laws, regulations and standards.

The AMF expects these mechanisms to be adaptable to changes in the financial institution's business and in technology.

In addition, financial institutions using insurance to transfer operational risk should ensure that it always complements their own control mechanisms for this type of risk.

[17] The *Business Continuity Management Guideline* recommends establishing processes for identifying major operational incidents.

[18] Refer to Principle 5 in *G7 Fundamental Elements of Cybersecurity for the Financial Sector,* October 2016.

3. Supervision of sound and prudent management practices

In fostering the establishment of sound and prudent management practices within financial institutions, the AMF, as part of its supervisory activities, intends to assess the degree of compliance with the principles and orientations set forth in this guideline.

Accordingly, it will examine the effectiveness and relevance of its strategies, policies and procedures, the quality of its supervision and the control exercised by the board of directors and senior management.

Operational risk management practices are constantly evolving. The AMF expects decision-makers at financial institutions to remain current with best practices and to adopt them, to the extent that they address their needs.