5.2

Réglementation et lignes directrices

5.2 RÉGLEMENTATION ET LIGNES DIRECTRICES

5.2.1 Consultation

Aucune information.

5.2.2 Publication

Ligne directrice sur la conformité
(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 conformité* modifiée (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, laquelle prend effet le15 avril 2017.

La Ligne directrice est publiée ci-après et elle est disponible sur le site Web de l'Autorité au www.lautorite.qc.ca sous les onglets « Assureurs » ou « Institutions de dépôt » sous 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 : (514) 395-0337, poste 4688
Numéro sans frais : 1 877 525-0337
wassim.ferjani@lautorite.qc.ca

Le 13 avril 2017

DÉCISION N° 2017-PDG-0046

Ligne directrice sur la conformité

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 prévu 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 15 décembre 2016 [(2016) vol. 13, n° 50, B.A.M.F., section 5.2.1] du projet de modification de la *Ligne directrice sur la conformité* (la « ligne directrice »);

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

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 modifiée 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 conformité* modifiée, 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 conformité* modifiée prend effet le 15 avril 2017.

Fait le 10 avril 2017

Louis Morisset
Président-directeur général

AUTORITÉ DES MARCHÉS FINANCIERS

LIGNE DIRECTRICE SUR LA CONFORMITÉ

Avril 2017

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, de la complexité de leurs activités et de leur profil de risque. 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 conformité.

Champ d'application

La *Ligne directrice sur la conformité* s'applique 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. 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[2] d'assurance 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 tel qu'il est précisé dans la présente ligne directrice.

Les expressions génériques « institution financière » ou « institution » sont utilisées pour faire référence à toutes les entités financières 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 conformité* est effective depuis le 1er avril 2009.

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 appropriée 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 et qu'elle les ait mises en œuvre depuis le 1er avril 2011.

Afin de tenir compte de l'évolution des principes de gestion saine et prudente issus des instances internationales en lien avec la conformité et pour être en harmonie avec les lignes directrices sur la gouvernance et sur la gestion intégrée des risques, la *Ligne directrice sur la conformité* est révisée en date du 15 avril 2017. Afin de permettre aux institutions financières de s'approprier les nouvelles attentes, celles-ci disposent d'une période transitoire d'un an. Par conséquent, l'Autorité s'attend à ce que l'institution financière ait effectué les changements nécessaires d'ici le 15 avril 2018. 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.

Comme il est précisé dans la version initiale de la présente ligne directrice, les développements en matière de gestion de la conformité et les constats effectués dans le cadre des travaux de surveillance de l'Autorité pourraient mener ultérieurement à d'autres modifications de cette ligne directrice.

Introduction

L'Autorité s'est donné comme cible de favoriser la convergence entre les objectifs de protection du consommateur de produits et services financiers et l'essor des institutions financières, et ce, dans un souci d'équité, d'intégrité et de pérennité du secteur financier. À ce titre, elle accorde une grande importance aux mesures qui doivent être mises en place par les institutions financières afin d'assurer la conformité de ces dernières à l'ensemble des lois, règlements et lignes directrices auxquels elles sont assujetties.

Les institutions financières se préoccupent de plus en plus du risque de non-conformité compte tenu notamment des conséquences sur leur réputation et leur solvabilité. Dans cette optique, la gestion de la conformité devrait occuper une place importante au sein des institutions financières. Instaurer et véhiculer une culture de conformité devient la clé d'une gestion saine et prudente et de saines pratiques commerciales et une mesure d'atténuation des risques pouvant découler de la non-conformité.

Les principes fondamentaux et orientations publiés par le Comité de Bâle sur le contrôle bancaire[3] et l'Association internationale des contrôleurs d'assurance[4] exposent clairement la nécessité et l'importance pour les institutions financières de s'assurer de leur conformité aux lois, règlements et lignes directrices et, pour les autorités de réglementation, de leur fournir les encadrements nécessaires pour ce faire.

L'Autorité adhère aux principes et orientations énoncés par ces instances internationales favorisant des pratiques de gestion saine et prudente. Par son habilitation prévue aux diverses lois sectorielles[5], elle donne la présente ligne directrice aux institutions financières, signifiant ainsi explicitement ses attentes en matière de gestion de la conformité.

Il est à noter que le terme générique « risque de non-conformité » est utilisé dans la présente pour faire référence au risque de non-conformité réglementaire inhérent aux lois, règlements et lignes directrices auxquels l'institution financière est assujettie. Toutefois, ce risque n'inclut pas les risques liés aux normes déontologiques.

---

3 BANQUE DES RÈGLEMENTS INTERNATIONAUX. COMITÉ DE BÂLE SUR LE CONTRÔLE BANCAIRE. *Orientations. Principes de gouvernance d'entreprise à l'intention des banques*, juillet 2015. *Principes fondamentaux pour un contrôle bancaire efficace*, septembre 2012. BANK FOR INTERNATIONAL SETTLEMENTS. BASEL COMMITTEE ON BANKING SUPERVISION. *Joint Forum - Principles for the supervision of financial conglomerates*, September 2012.

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

5 *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 les sociétés de fiducie et les sociétés d'épargne, RLRQ, c. S-29.01, art. 314.1.

1. Cadre de gestion de la conformité

L'Autorité s'attend à ce que l'institution financière établisse un cadre de gestion de la conformité, prévoyant la mise en place d'une fonction de conformité indépendante. Ce cadre devrait être mis à jour sur une base régulière et devrait permettre à l'institution financière de respecter les lois, règlements et lignes directrices couvrant l'ensemble de ses activités et à promouvoir et soutenir une culture de conformité.

Un cadre de gestion de la conformité contient les principes de base permettant à l'institution financière d'identifier, d'évaluer, de contrôler, d'atténuer et de faire le suivi du risque de non-conformité lié à ses activités. Ce cadre devrait être constitué des politiques et procédures ou tout autre mécanisme de contrôle[6] et devrait définir les risques de non-conformité à couvrir par l'institution. Il devrait être élaboré selon la nature, la taille, la complexité des activités et le profil de risque de l'institution financière.

Le cadre de gestion de la conformité, au même titre que le cadre de gouvernance et le cadre de gestion intégrée des risques, est une composante essentielle pour assurer une gestion saine et prudente et de saines pratiques commerciales d'une institution financière. Dans cet ordre d'idée, l'Autorité considère qu'il devrait s'arrimer au cadre global de la gestion des risques.

Les politiques et les procédures constituant le cadre de gestion de la conformité devraient notamment permettre de :

- définir les rôles et responsabilités des différents intervenants impliqués dans la gestion de la conformité;
- documenter la méthodologie utilisée pour identifier, évaluer, contrôler, atténuer et faire le suivi du risque de non-conformité lié à ses activités;
- veiller à ce que l'institution financière opère dans le respect des lois, règlements et lignes directrices;
- surveiller les expositions importantes au risque de non-conformité;
- s'assurer de l'adéquation, du respect et de l'efficacité des mécanismes de contrôle permettant d'atténuer les expositions importantes au risque de non-conformité;
- s'assurer qu'une vigie à l'égard des lois, règlements et lignes directrices en vigueur soit effectuée;
- s'assurer qu'une information suffisante et pertinente sur l'efficacité de la gestion du risque de non-conformité soit communiquée à la haute direction et au conseil d'administration en temps opportun;
- rendre compte des résultats significatifs découlant de la supervision et de l'évaluation de la conformité effectuée respectivement par la fonction de conformité[7] et par la fonction d'audit interne[8], le cas échéant;

6 Il peut s'agir aussi de programmes, de processus ou de structures.

7 Lorsqu'il est fait mention de la fonction de conformité, il peut s'agir de toute autre fonction de supervision indépendante de la deuxième ligne de défense.

- faire l'évaluation du cadre de gestion de la conformité et la fonction de conformité par l'audit interne ou par l'audit externe dans certains cas;
- proposer des plans d'action lorsque des lacunes importantes sont décelées.

Étant donné les impacts potentiels importants que peuvent avoir les risques de non-conformité sur la réputation de l'institution financière, cette dernière devrait disposer d'une solide culture de conformité relevant de la responsabilité de chacun des employés, initiée et appuyée par la haute direction et le conseil d'administration et ne reposant pas uniquement sur la conformité avec les lois, règlements et lignes directrices mais aussi sur l'honnêteté et la bonne foi, en tout temps.

Fonction de conformité

Une fonction de conformité indépendante des activités qu'elle supervise est une des composantes clés de la deuxième ligne de défense[9] de l'institution financière et une base essentielle des pratiques de gestion saine et prudente.

D'emblée, il importe de préciser qu'une fonction de conformité n'est pas forcément une unité particulière au sein de l'institution financière dans la mesure où il est possible d'utiliser des fonctions qui existent déjà de façon à ne pas créer de structures supplémentaires qui pourraient alourdir le fonctionnement de l'institution.

La fonction de conformité devrait être idéalement confiée à un chef de la conformité[10]. Le personnel chargé de la conformité pourrait être impliqué dans des unités d'affaires[11]. Il importera toutefois que ces unités puissent, le cas échéant, rendre compte au chef de la conformité ou à la personne responsable de cette fonction au sein de l'institution financière, laquelle devrait être indépendante de la gestion des opérations.

Pour être efficace et assumer correctement son rôle au sein de la deuxième ligne de défense[12], la fonction de conformité devrait disposer selon la nature, la taille, la complexité des activités et le profil de risque de l'institution financière, de l'autorité suffisante, du positionnement hiérarchique adéquat, de l'indépendance par rapport à la gestion des opérations, des ressources nécessaires et du libre accès au conseil d'administration.

La fonction de conformité devrait établir et maintenir des politiques et des procédures lui permettant d'évaluer, selon une approche fondée sur les risques, l'adéquation, le respect et l'efficacité des mécanismes de contrôle de la conformité à tous les niveaux de l'institution. Elle devrait en outre s'assurer d'un traitement approprié des risques

8 Lorsqu'il est fait mention de la fonction d'audit interne, il peut s'agir de toute autre fonction d'évaluation indépendante désignant la troisième ligne de défense.

9 Les fonctions de la deuxième ligne de défense devraient être indépendantes de la gestion des opérations. L'Autorité est consciente que la diversité au niveau de la nature, la taille, la complexité et le profil de risque des institutions financières ont un impact sur la composition et la structure de la deuxième ligne de défense (voir la *Ligne directrice sur la gouvernance*).

10 Voir Section 2.3.2 « Rôles et responsabilités du chef de la conformité ».

11 Lorsqu'il est fait mention d'une unité d'affaires, il s'agit de la plus petite composante de l'institution à laquelle est attribuée une responsabilité opérationnelle ou administrative.

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

importants de non-conformité lors de la mise en œuvre du cadre de gestion de la conformité.

Selon une approche fondée sur les risques, la fonction de conformité devrait aussi voir à ce que le cadre de gestion de la conformité soit suffisamment robuste pour être en mesure de déceler les lacunes importantes en matière de conformité touchant l'institution financière et de les acheminer à la haute direction et au conseil d'administration.

Elle devrait en outre évaluer la fiabilité des informations fournies par les gestionnaires/directeurs opérationnels et s'assurer que les directions concernées prennent les mesures appropriées pour pallier aux lacunes importantes décelées en matière de conformité.

La fonction de conformité devrait notamment :

- élaborer le cadre de gestion de la conformité et coordonner sa mise en œuvre au sein de l'institution financière;
- détenir une très bonne connaissance des lois, règlements et lignes directrices s'appliquant aux activités de l'institution, et ce, pour toutes les juridictions où elle fait affaire;
- aider la haute direction à gérer efficacement le risque de non-conformité auquel fait face l'institution financière;
- fournir au conseil d'administration et à la haute direction les renseignements nécessaires lui permettant d'obtenir une vue d'ensemble sur la conformité de l'institution;
- veiller à l'uniformité des méthodes de supervision de la conformité à tous les niveaux de l'institution financière afin d'en assurer une gestion harmonisée;
- être impliquée en amont des projets pouvant exercer un impact sur la conformité des activités afin d'identifier et d'évaluer de façon proactive les enjeux et risques potentiels de non-conformité;
- aider à sensibiliser et à former le personnel et, plus particulièrement, les employés engagés dans des activités à haut risque de non-conformité;
- agir comme un point de contact central pour répondre aux interrogations des membres du personnel au sujet de la conformité;
- fournir des orientations aux membres du personnel quant à l'application appropriée des lois, règlements et lignes directrices sous la forme de politiques, directives, procédures et autres documents.

Il importe de rappeler que l'institution financière conserve la pleine responsabilité de toute fonction de conformité impartie[13] de même que celle de la reddition de comptes liée à cette fonction.

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

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*[14].

[14] AUTORITÉ DES MARCHÉS FINANCIERS. *Ligne directrice sur la gouvernance*, septembre 2016.

2. Rôles et responsabilités

L'Autorité s'attend à ce que les rôles et responsabilités des intervenants impliqués dans la gestion de la conformité soient clairement définis.

Un élément essentiel au bon fonctionnement d'un cadre de gestion de la conformité repose sur l'engagement de l'institution financière à promouvoir les valeurs d'un comportement soucieux du respect de la conformité. Les objectifs du cadre de gestion de la conformité seront plus faciles à atteindre si les rôles et les responsabilités sont bien identifiés et que leur attribution est connue et bien comprise au sein de l'institution financière.

Le conseil d'administration et la haute direction sont ultimement responsables de voir à ce que l'institution financière soit en conformité continue avec les lois, règlements et lignes directrices. Les rôles et responsabilités généralement attribués au conseil d'administration, à la haute direction et aux trois lignes de défense[15] sont les suivants.

2.1 Rôles et responsabilités du conseil d'administration[16]

Compte tenu de la responsabilisation accrue et de l'imputabilité des membres du conseil d'administration, ces derniers devraient bien comprendre l'exposition de l'institution financière à un risque important de non-conformité et voir à ce que l'institution dispose d'un cadre de gestion de la conformité efficace. Les membres du conseil d'administration ont avantage à s'assurer que ce cadre fasse l'objet d'une mise à jour et d'une évaluation périodiques.

Dans ce contexte, le conseil d'administration devrait notamment :

- approuver les politiques importantes, incluant l'approbation des critères d'escalade en réponse à la matérialisation des risques importants de non-conformité, du cadre de gestion de la conformité et leurs modifications, le cas échéant;
- approuver les décisions de nomination, de révocation et de rémunération du chef de la conformité;
- s'assurer d'obtenir suffisamment de renseignements pertinents pour faire face aux lacunes importantes relatives à la conformité afin d'avoir l'assurance objective que l'institution se conforme aux lois, règlements et lignes directrices;
- examiner les rapports produits par la fonction de conformité et par l'audit interne et/ou externe, le cas échéant;
- veiller à l'application des recommandations et à l'exécution des plans d'action à l'égard des lacunes importantes, le cas échéant;
- veiller à ce que la fonction de conformité ait l'autorité suffisante, le positionnement hiérarchique adéquat, l'indépendance par rapport à la gestion des opérations, les

[15] AUTORITÉ DES MARCHÉS FINANCIERS. *Ligne directrice sur la gouvernance*, septembre 2016.

[16] Lorsqu'il est fait mention du conseil d'administration, il peut s'agir d'un comité de ce dernier formé, par exemple, à des fins d'examen de points particuliers.

ressources nécessaires et le libre accès au conseil d'administration et qu'elle fasse l'objet d'évaluations périodiques.

2.2 Rôles et responsabilités de la haute direction

Il incombe à la haute direction de mettre en place une fonction de conformité au sein de l'institution financière. Elle devrait aussi veiller à ce que les politiques et procédures soient développées et appliquées efficacement par les personnes qui disposent de la compétence pour ce faire et que toutes ces personnes comprennent et assument leurs responsabilités à cet égard. Si certaines des responsabilités de conformité sont acquittées par le personnel de différentes unités d'affaires, la répartition des responsabilités entre chacune de ces unités devrait être clairement établie.

La haute direction devrait notamment :

- mettre en œuvre un cadre de gestion de la conformité, s'assurer de son application et de sa mise à jour sur une base régulière;
- définir les critères d'escalade en réponse à la matérialisation des risques importants de non-conformité;
- veiller à ce que les recommandations relatives aux lacunes importantes soient adéquatement prises en considération.

2.3 Rôles et responsabilités des lignes de défense

2.3.1 Rôles et responsabilités des gestionnaires/directeurs opérationnels[17]

Les gestionnaires/directeurs opérationnels devraient élaborer des procédures de contrôle relatives à la conformité et les intégrer aux activités quotidiennes de l'institution financière. Le but étant de prévenir et d'identifier rapidement le risque de non-conformité et d'en faire le suivi au chef de la conformité selon une fréquence déterminée par ce dernier.

2.3.2 Rôles et responsabilités du chef de la conformité

La fonction de conformité devrait être idéalement sous la responsabilité d'un chef de la conformité ou, à défaut de l'existence d'un tel poste, d'une personne détenant un niveau d'autorité suffisant pour assurer son indépendance et disposant des pouvoirs et des ressources nécessaires en fonction de la nature, de la taille et de la complexité des activités et du profil de risque de l'institution, afin d'accomplir son mandat adéquatement.

Le chef de la conformité devrait posséder une expérience pertinente, une formation adéquate et disposer des compétences nécessaires et d'une bonne connaissance de l'institution financière et des lois, règlements et lignes directrices applicables.

[17] Les directions opérationnelles constituent la première ligne de défense responsable de la gestion quotidienne des risques (voir la *Ligne directrice sur la gouvernance*).

Le chef de la conformité devrait plus précisément :

- conseiller et informer régulièrement le conseil d'administration et la haute direction sur la conformité de l'institution financière aux lois, règlements et lignes directrices ainsi que sur les expositions et lacunes importantes décelées, le cas échéant;
- donner son avis sur l'adéquation, le respect et l'efficacité des mécanismes de contrôle de la conformité à tous les niveaux de l'institution;
- s'assurer que les risques importants de non-conformité identifiés soient validés avec la haute direction et le conseil d'administration, afin qu'ils correspondent au niveau de sensibilité et de priorisation de ces derniers, et recommander leur ajustement, le cas échéant;
- affiner ses mandats et développer des relations de collaboration efficaces avec les gestionnaires/directeurs opérationnels et les chefs des fonctions de supervision de la deuxième ligne de défense, notamment en ce qui a trait à l'élaboration des politiques relatives aux risques importants de non-conformité;
- mettre en place une procédure d'escalade en réponse à la matérialisation des risques importants de non-conformité rencontrant les critères préalablement définis par la haute direction et approuvés par le conseil d'administration.

Le chef de la conformité devrait rendre compte périodiquement au conseil d'administration ou au comité d'audit, au comité de conformité ou à tout autre comité pertinent. De plus, il devrait être en mesure de se réunir en privé avec le conseil d'administration ou son président au moins une fois par année sans la présence de la haute direction afin de confirmer, entre autres, son indépendance au sein de l'institution financière, certains enjeux, voire même des points divergents avec la haute direction.

Les rapports portant sur la conformité devraient renfermer suffisamment de renseignements fiables, pertinents et utiles pour permettre au conseil d'administration et à la haute direction de porter un jugement éclairé sur la gestion de la conformité à tous les niveaux de l'institution financière. Les rapports pourraient par exemple couvrir :

- la portée et les résultats de la supervision de la gestion de la conformité, y compris les lacunes importantes au niveau de l'application du cadre de gestion de la conformité, les cas importants de dérogation ainsi que les expositions importantes au risque de non-conformité et leurs conséquences potentielles sur l'institution financière;
- les recommandations et les plans d'action à l'égard des lacunes importantes et des dérogations, le cas échéant;
- les interventions effectuées par les différents régulateurs au sein de l'institution financière;
- l'information sur les changements importants apportés aux lois, règlements et lignes directrices;
- les enjeux et les nouvelles tendances en matière de conformité au sein du secteur financier.

La documentation afférente à la gestion de la conformité, incluant les rapports présentés à la haute direction et au conseil d'administration, devrait être conservée selon des procédures de conservation cohérentes avec les orientations définies par l'institution financière ou avec toute exigence réglementaire ou autre appropriée.

2.3.3 Rôles et responsabilités de l'audit interne[18]

L'audit interne devrait fournir une assurance objective quant à l'adéquation, au respect et à l'efficacité de la supervision de la conformité, en l'évaluant au niveau de la gestion quotidienne des opérations et de la fonction de conformité. Cette évaluation devrait aussi porter sur le cadre de gestion de la conformité et s'effectuer sur une base périodique selon une approche fondée sur les risques.

L'évaluation devrait déterminer si les politiques et procédures en place sont appropriées, bien respectées et conformes aux lois, règlements et lignes directrices. La portée de l'évaluation devrait être documentée et devrait dépendre de la nature, de la taille, de la complexité des activités et du profil de risque de l'institution financière.

Les rapports d'audit interne devraient être communiqués aux gestionnaires/directeurs opérationnels concernés, au chef de la conformité, à la haute direction et au conseil d'administration. Ils devraient renfermer suffisamment de renseignements fiables, pertinents et utiles sur les objectifs, la portée ainsi que les conclusions, recommandations et plans d'action appropriés. Les mesures correctives prises en réponse à ces recommandations devraient faire l'objet d'un suivi adéquat de la part des auditeurs internes.

Les rapports d'audit devraient entre autres faciliter la compréhension par le conseil d'administration de l'exposition de l'institution financière aux risques de non-conformité. Ils devraient ainsi l'aider à juger de la fiabilité de l'assurance que lui fournissent le chef de conformité et la haute direction quant à la supervision de la conformité à tous les niveaux de l'institution.

[18] L'Autorité invite les institutions financières à consulter la *Ligne directrice sur la gouvernance*, où elle exprime ses attentes quant aux rôles et responsabilités des fonctions d'audit et dans laquelle sont couverts plusieurs volets en la matière, notamment : l'indépendance, l'objectivité, les compétences, connaissances et disponibilité des ressources, l'accès à l'information, etc.

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 et de saines pratiques commerciales 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 énoncés à la présente ligne directrice en considérant les attributs propres à chaque institution.

De même, l'efficacité et la pertinence des stratégies, politiques et procédures mises en place ainsi que la qualité de la supervision et le contrôle exercés par le conseil d'administration et la haute direction seront évaluée.

Les pratiques en matière de conformité 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

COMPLIANCE GUIDELINE

April 2017

TABLE OF CONTENTS

Preamble

The *Autorité des marchés financiers* ("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 this 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 their nature, size, operational complexity and risk profile. In this regard, the guideline illustrates 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 forms part of that approach and sets out the AMF's expectations regarding compliance practices.

Scope

This *Compliance 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. 67.3;
- *An Act respecting trust companies and savings companies,* CQLR, c. S-29.01.

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 therewith.

2 Mutual insurance associations are damage insurers covered by this guideline.

Coming into effect and updating

This *Compliance Guideline* has been in effect since April 1, 2009.

With respect to the legal requirement of institutions to follow sound and prudent management practices, the AMF expects each institution to have developed strategies, policies and procedures based on its nature, size, operational complexity and risk profile, and to have adopted the principles underlying this guideline since April 1, 2011.

To reflect the evolution of principles of sound and prudent management emanating from international bodies in connection with compliance, and to be consistent with the *Governance Guideline* and the *Integrated Risk Management Guideline*, this *Compliance Guideline* has been updated to April 15, 2017. A one-year transition period has been set to enable financial institutions to adjust to the new expectations. The AMF therefore expects financial institutions to make the necessary adjustments by April 15, 2018. If an institution has already set up such a framework, the AMF may verify whether the framework enables it to comply with the legal requirements.

As mentioned in the original version of this guideline, developments in compliance management and the AMF's observations in the course of its supervision could lead to other changes to this guideline.

Introduction

The AMF seeks to converge two objectives—the protection of consumers of financial products and services and the development of financial institutions—based on equity, integrity and the financial sector's sustainability. In this regard, it places high priority on the measures to be implemented by financial institutions to ensure that they comply with all laws, regulations and guidelines to which they are subject.

Financial institutions are increasingly concerned about compliance risk, in particular because of the impact on their reputation and solvency. Therefore, compliance management should be an important focus for financial institutions. Adopting and fostering a compliance culture is critical to ensuring sound and prudent management and sound commercial practices. It may also serve to mitigate any risks arising from non-compliance.

The core principles and guidance published by the Basel Committee on Banking Supervision[3] and the International Association of Insurance Supervisors[4] clearly explain the need and importance for financial institutions to ensure their compliance with laws, regulations and guidelines and, for regulatory authorities, to provide them with the frameworks necessary to do so.

The AMF adheres to the principles and guidance published by international bodies that foster sound and prudent management practices. Pursuant to the authority conferred upon it under various sector-based statutes,[5] the AMF is issuing this guideline to explicitly inform financial institutions of its expectations regarding compliance management.

The term "compliance risk" is used in this guideline to mean the risk of non-compliance with the laws, regulations and guidelines applicable to financial institutions. This risk does not however include ethical risks.

[3] BANK FOR INTERNATIONAL SETTLEMENTS. BASEL COMMITTEE ON BANKING SUPERVISION. *Guidelines. Corporate Governance Principles for Banks*, July 2015. *Core principles for effective banking supervision*, September 2012. BANK FOR INTERNATIONAL SETTLEMENTS. BASEL COMMITTEE ON BANKING SUPERVISION. *Joint Forum, Principles for the supervision of financial conglomerates*, September 2012.

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

[5] *An Act respecting insurance*, CQLR, c. A-32, sections 325.0.1 and 325.0.2;

An Act respecting financial services cooperatives, CQLR, c. C-67.3, section 565;

An Act respecting trust companies and savings companies, CQLR, c. S-29.01, section 314.1.

1. Compliance management framework

The AMF expects each financial institution to establish a compliance management framework that includes an independent compliance function. It should be regularly updated and enable financial institutions to comply with the laws, regulations and guidelines applicable to their full spectrum of activities and to foster and support a compliance culture.

A compliance management framework contains the basic principles allowing financial institutions to identify, assess, control, mitigate and monitor compliance risk related to their activities. The framework should consist of policies and procedures or any other control mechanisms[6] and should define the compliance risks to be covered. It should be developed taking into account the nature, size, operational complexity and risk profile of the financial institution.

The compliance management framework, like the governance framework and the integrated risk management framework, is a critical component for ensuring sound and prudent management and sound commercial practices. As such, the AMF considers that it should be aligned to the overall risk management framework.

The main purpose of the policies and procedures making up the compliance management framework is to:

- define the roles and responsibilities of the various stakeholders assigned to compliance management;
- document the methodology used to identify, assess, control, mitigate and monitor compliance risk related to the institution's activities;
- ensure that the financial institution operates in accordance with laws, regulations and guidelines;
- monitor material exposure to compliance risk;
- ensure the adequacy, observance and effectiveness of controls used to mitigate material exposure to compliance risk;
- monitor existing laws, regulations and guidelines;
- ensure that senior management and the board of directors are given sufficient relevant information on the effectiveness of compliance risk management on a timely basis;
- report on significant results from compliance oversight and assessments conducted, respectively, by the compliance function[7] and the internal audit function,[8] as applicable;

6 These may be programs, processes or structures.

7 A reference to the compliance function can also include any other independent oversight function in the second line of defense.

8 A reference to the internal audit function can also include any other independent assessment function in the third line of defense.

- allow internal audit or, in certain cases, external audit, to assess the compliance management framework and the compliance function;
- recommend action plans where material deficiencies are identified.

Given the potentially significant impact of compliance risk on their reputation, financial institutions should at all times have a strong compliance culture that is initiated and supported by senior management and the board of directors and based on honesty and good faith, rather than solely on compliance with laws, regulations and guidelines.

Compliance function

A compliance function independent of the activities it oversees is a key component of a financial institution's second line of defense[9] and an essential basis of sound and prudent management practices.

A compliance function is not necessarily a particular unit within the financial institution. Existing functions can be used so as to avoid creating additional structures that could hinder operations.

The compliance function should ideally be entrusted to a chief compliance officer.[10] Compliance staff could be involved in business units.[11] However, where applicable, it is important that these units be able to report to the compliance officer or the person in charge of this function within the financial institution who should be independent from operational management.

To be effective and properly assume its role in the second line of defense,[12] the compliance function should have—in line with the institution's nature, size, operational complexity and risk profile—sufficient authority, an adequate hierarchical position, independence from operational management, the necessary resources and free access to the board of directors.

The compliance function should establish and maintain policies and procedures to assess, through a risk-based approach, the adequacy, observance and effectiveness of compliance controls at all levels of the institution. It should ensure that material compliance risks are taken into account when implementing the compliance management framework.

Using a risk-based approach, the compliance function should also ensure that the compliance management framework is sufficiently robust to be able to identify material compliance deficiencies impacting the financial institution and escalate them to senior management and the board of directors.

9 The functions involved in the second line of defense should be independent from operational management. The AMF is aware that diversity in terms of the nature, size, complexity and risk profile of financial institutions has an impact on the composition and structure of the second line of defense. (See the *Governance Guideline)*

10 Refer to section 2.3.2 "Roles and responsibilities of the compliance officer".

11 For purposes of this guideline, a business unit corresponds to the institution's smallest component with operational or administrative responsibility.

12 AUTORITÉ DES MARCHÉS FINANCIERS. *Governance Guideline*, September 2016.

It should also assess the reliability of the information supplied by operational managers and ensure that the relevant departments take appropriate steps to remedy any identified material compliance deficiencies.

The compliance function should, in particular:

- develop the compliance management framework and co-ordinate its implementation within the financial institution;
- have a thorough understanding of the laws, regulations and guidelines applicable to the institution's activities in all jurisdictions where it does business;
- assist senior management in effectively managing the compliance risk to which the financial institution is exposed;
- provide the information needed by the board of directors and senior management to obtain an overview of the financial institution's compliance;
- oversee consistency of compliance oversight methods across the financial institution to ensure their harmonized management;
- be involved upstream on projects that could impact operational compliance in order to proactively identify and assess potential compliance issues and risks;
- help train staff and raise their awareness on compliance matters, particularly employees involved in high-risk compliance activities;
- act as a liaison for staff questions pertaining to compliance;
- provide staff with guidance about the appropriate application of laws, regulations and guidelines in the form of policies, directives, procedures, etc.

The financial institution of course remains fully responsible for any outsourced[13] compliance function and fully accountable for this function.

Furthermore, the AMF expects financial institutions to meet the disclosure and transparency expectations set out in the *Governance Guideline*.[14]

13 AUTORITÉ DES MARCHÉS FINANCIERS. *Outsourcing Risk Management Guideline*, December 2010.

14 AUTORITÉ DES MARCHÉS FINANCIERS. *Governance Guideline,* September 2016.

2. Roles and responsibilities

The AMF expects the roles and responsibilities of stakeholders assigned to compliance management to be clearly defined.

One of the elements key to the effective operation of a compliance management framework is the financial institution's commitment to promoting values related to proper conduct in compliance matters. Compliance management framework objectives will be more easily achieved if roles and responsibilities are clearly identified and financial institution staff are fully aware of and understand their respective roles and responsibilities.

The board of directors and senior management are ultimately responsible for ensuring the financial institution's ongoing compliance with laws, regulations and guidelines. The board of directors, senior management and the three lines of defense[15] are generally assigned the following roles and responsibilities.

2.1 Roles and responsibilities of the board of directors[16]

Given their increased responsibility and accountability, board members should fully understand the financial institution's exposure to material compliance risk and ensure that an effective compliance management framework is in place. Board members are also responsible for ensuring this framework is updated and assessed periodically.

In this context, the board of directors should, in particular:

- approve key policies of the compliance management framework, including escalation criteria for material compliance risks, and any changes;
- approve decisions relating to the appointment, dismissal and remuneration of the chief compliance officer;
- ensure that it has sufficient relevant information to address material compliance deficiencies in order to have objective assurance that the institution conforms to laws, regulations and guidelines;
- examine reports prepared by the compliance function and by internal and/or external audit, as applicable;
- ensure application of recommendations and execution of action plans with respect to material deficiencies;
- ensure that the compliance function has sufficient authority, an adequate hierarchical position, independence from operational management, the necessary resources and free access to the board, and that regular reviews of this function are carried out.

15 AUTORITÉ DES MARCHÉS FINANCIERS. *Governance Guideline*, September 2016.

16 A reference to the board of directors can also include a board committee, such as one to establish and examine specific issues.

2.2 Roles and responsibilities of senior management

Senior management is responsible for establishing a compliance function within the financial institution. It should also ensure that policies and procedures are developed and effectively applied by qualified persons who understand and assume their responsibilities. If compliance-related responsibilities are carried out by staff from various business units, the allocation of such responsibilities among the units should be clearly defined.

Senior management should, in particular:

- implement a compliance management framework and ensure its application and updating on a regular basis define escalation criteria in response to the occurrence of material compliance risks;
- ensure that due consideration is given to recommendations concerning material deficiencies.

2.3 Roles and responsibilities of the lines of defense

2.3.1 Roles and responsibilities of operational managers[17]

Operational managers should establish compliance control procedures and integrate them into the financial institution's day-to-day activities. The goal is to prevent compliance risk and promptly identify potential risks and follow up on them with the chief compliance officer at a frequency he determines.

2.3.2 Roles and responsibilities of the chief compliance officer

The compliance function should ideally report to the chief compliance officer or, where this function does not exist, a person with sufficient authority to ensure its independence and who has the necessary powers and resources, depending on the institution's nature, size, operational complexity and risk profile, to adequately accomplish his mandate.

The chief compliance officer should have the relevant experience, appropriate education, the necessary competencies, and good knowledge of the financial institution and applicable laws, regulations and guidelines.

More specifically, the chief compliance officer should:

- advise and inform the board of directors and senior management regularly about the financial institution's compliance with laws, regulations and guidelines, and any material deficiencies identified;
- provide his opinion on the adequacy, observance and effectiveness of controls at all levels of the financial institution;

[17] Operational management constitutes the first line of defense responsible for day-to-day operations management (refer to the *Governance Guideline*).

- ensure that identified material compliance risks are validated with senior management and the board of directors so that these risks correspond to the level of sensitivity and priority they have established, and recommend any adjustments;
- refine his mandates and cultivate effective collaborative relationships with operational managers and oversight officers in the second line of defense, in particular with regard to developing policies for material compliance risks;
- implement an escalation procedure for material compliance risks based on criteria predetermined by senior management and approved by the board of directors.

The chief compliance officer should report regularly to the board of directors or to the audit committee, the compliance committee or any other relevant committee. He should be able to meet privately at least once a year with the board of directors or with the chair, without senior management in attendance, in order to confirm, among other things, his independence within the financial institution and to discuss certain issues and any points of disagreement with senior management.

Compliance reports should include sufficient reliable, pertinent and useful information to enable the board and senior management to make informed judgments on compliance management at all levels of the financial institution. For example, reports could cover the following:

- scope and results of compliance management oversight, including material deficiencies in the application of the compliance management framework, major instances of non-compliance as well as material exposure to compliance risk and the potential consequences for the financial institution;
- recommendations and action plans regarding material deficiencies and non-compliance events;
- regulatory intervention;
- details of significant amendments to laws, regulations and guidelines;
- compliance issues and trends in the financial sector.

Compliance management documentation, including reports for senior management and the board of directors, should be retained in accordance with the institution's procedures or any regulatory or other relevant requirement.

2.3.3 Roles and responsibilities of internal audit[18]

Internal audit should provide objective assurance as to the adequacy, observance and effectiveness of compliance oversight by assessing day-to-day operations management and the compliance function. This assessment should also cover the compliance management framework and be carried out regularly using a risk-based approach.

[18] The AMF encourages financial institutions to refer to the *Governance Guideline*, which sets out its expectations concerning the roles and responsibilities of the audit functions. The Guideline also covers several related matters, including the independence, objectivity, skills, knowledge and availability of resources, and access to information.

The assessment should determine whether policies and procedures in place are appropriate, observed and compliant with laws, regulations and guidelines. The scope of the assessment should be documented and be proportionate to the financial institution's nature, size, operational complexity and risk profile.

Internal audit reports should be provided to the relevant operational managers, the chief compliance officer, senior management and the board of directors. They should include sufficient reliable, pertinent and useful information about the audit objectives and scope, as well as conclusions, recommendations and appropriate action plans. Internal auditors should ensure adequate monitoring of the corrective measures taken in response to these recommendations.

Among other things, reports should facilitate board understanding of the institution's exposure to compliance risks. They should help it assess the reliability of the assurance provided by the chief compliance officer and senior management as regards compliance oversight at all levels of the institution.

3. Supervision of sound and prudent management practices

In seeking to promote sound and prudent management practices and sound commercial practices within financial institutions, the AMF may, as part of its supervisory work, assess the degree of compliance with principles set out in this guideline commensurate with the specific characteristics of each institution.

The effectiveness and relevance of implemented strategies, policies and procedures as well as the quality of oversight and control by the board of directors and senior management will also be assessed.

Compliance practices are constantly evolving. The AMF expects a financial institution's decision-making bodies to be aware of compliance best practices and tailor them to their needs.