DRAFT

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 a financial institution's legal requirement to follow sound and prudent management practices. These guidelines therefore cover 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 implementing these management principles and to apply sound practices based on their nature, size, operational complexity and risk profile. 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 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*, the *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 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, namely, 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 implemented by financial institutions to ensure they comply with all laws, regulations, guidelines and various standards to which they are subject.

Increased regulation has led to growing concern among many financial institutions about compliance risk, which can seriously impact their reputation and solvency. Therefore, compliance management should increasingly be a major issue for financial institutions. Adopting and fostering a compliance culture is critical to ensuring sound and prudent management. 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, guidelines and various standards 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.

It should be noted that the term "compliance risk" is used in this guideline in a generic sense and refers to the risk of non-compliance with the laws, regulations and guidelines to which financial institutions are subject.

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, including an independent compliance function. It should be regularly updated and enable financial institutions to comply with the legal, regulatory, normative and prudential requirements applicable to their activities and to foster and support a compliance culture.

A compliance management framework contains the basic principles allowing financial institutions to identify, assess, quantify, 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 type of 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 good governance and reliable internal control systems, is a critical component of a financial institution's sound and prudent management. As such, the AMF considers that it should be an integral part of an overall risk management framework.

The main purpose of the policies and procedures comprising 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, quantify, control, mitigate and monitor compliance risk related to the institution's activities;
- ensure that the financial institution operates with integrity and in accordance with its legal, regulatory, normative and prudential requirements;
- monitor material exposure to compliance risk;
- ensure the adequacy, observance and effectiveness of controls used to mitigate material exposure to compliance risk;
- monitor existing legal, regulatory, normative and prudential requirements;
- 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;
- generate reports 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 to assess the compliance management framework and the compliance function;
- recommend corrective measures where major problems are identified.

Given the potentially significant impact of compliance risk on their reputation, financial institutions should at all times have a strong compliance culture, supported by senior management and the board of directors, based on individual employee responsibility and on personal integrity, honesty, loyalty and good faith, rather than solely on compliance with laws, regulations and standards.

Compliance function

A compliance function independent of the activities it oversees is a key component of a financial institution's second line of defense 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.[9] Compliance staff may work in business units[10] and report to the management of the operations concerned. However, where applicable, these units must 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,[11] 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 financial institution of course remains fully responsible for any outsourced[12] 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* by implementing the necessary mechanisms for promptly advising internal and external stakeholders[13] likely to sustain serious harm due to a major compliance risk. Such an approach will enable the AMF, as a stakeholder, to be proactive in identifying practices that can undermine compliance management.

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

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

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

12 Autorité des marchés financiers. *Outsourcing Risk Management Guideline*, December 2010.

13 Autorité des marchés financiers. *Operational Risk Management Guideline*, December 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 staff at all levels of the financial institution are fully aware of their respective roles and responsibilities and understand them.

The board of directors and senior management are ultimately responsible for ensuring the financial institution's ongoing compliance with legal, regulatory, normative and prudential requirements. The board of directors, senior management and the three lines of defense[14] are generally assigned the following principal roles and responsibilities.

2.1 Roles and responsibilities of the board of directors[15]

Given their increased responsibility and accountability, board members should fully understand the financial institution's exposure to material compliance risk and ensure that a 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:

- approve the policies of the compliance management framework and any changes;
- approve decisions relating to the appointment, dismissal, performance evaluation and remuneration of the chief compliance officer;
- ensure that it has sufficient relevant information to address important compliance issues in order to have reasonable assurance that the institution conforms to laws, regulations and standards;
- analyze reports prepared by the compliance function;
- analyze reports prepared by internal audit;
- monitor key recommendations and action plans adopted with respect to planned corrective measures;
- 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.

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

[15] A reference to the board of directors can also include a board committee, such as a board committee established to 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.

On approval of the board of directors, senior management should:

- implement the compliance management framework;
- establish procedures for communication with and recourse to higher levels within the institution in response to the occurrence of compliance risks meeting predetermined criteria;
- ensure that due consideration is given to key compliance recommendations.

2.3 Roles and responsibilities of the lines of defense

2.3.1 Roles and responsibilities of operational managers[16]

Les gestionnaires/directeurs opérationnels devraient être responsables des contrôles relatifs à la gestion des risques de non-conformité et adopter des procédures relatives à la conformité en les intégrant 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 via des rapports périodiques au chef de la conformité, selon une fréquence déterminée par ce dernier.

2.3.2 Roles and responsibilities of the chief compliance officer

This section sets out the roles and responsibilities assumed by the compliance officer and/or the compliance function.

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 its legislative, regulatory, normative and prudential requirements.

More specifically, the chief compliance officer should:

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

- advise and inform the board of directors and senior management regularly about the financial institution's compliance with laws, regulations, guidelines and various standards, any deficiencies identified and the latest developments in compliance;
- ensure that the most 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 established by senior management and the board;
- 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;
- certify compliance with legal, regulatory, normative and prudential requirements applicable to the financial institution's operations.

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 used in operational management. It should ensure that material compliance risks are taken into account when implementing the compliance management framework.

The compliance function should also ensure that the compliance management framework is sufficiently robust to be able to identify compliance weaknesses impacting the financial institution and escalate them to senior management and the board of directors. The escalation process should be formal and based on criteria that are predetermined and approved by the board of directors.

It must also implement adequate processes to oversee compliance of day-to-day operations management, assess the reliability of the related information supplied by operational managers, and ensure that the relevant departments take appropriate steps to remedy any identified 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 legal, regulatory, normative and prudential requirements 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 to obtain an overview of the financial institution's compliance;
- oversee consistency of 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 on compliance matters, particularly employees with key responsibilities or 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, guidelines and various standards in the form of policies, directives, procedures, etc.

The chief compliance officer should report 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.

Reporting by the chief compliance officer, including reports for the board of directors and senior management, should be on a regular periodic basis. 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. Reports could cover the following:

- scope and results of compliance management oversight, including significant problems or 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;
- key recommendations for correcting deficiencies and non-compliance events;
- action plans adopted by management with respect to planned corrective measures;
- regulatory intervention;
- details of significant amendments to laws, regulations, guidelines or various standards;
- 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[17]

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 objectives, scope, conclusions and recommendations and appropriate action plans. Internal auditors should ensure adequate monitoring of the corrective measures taken by operational managers in response to these recommendations.

[17] 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 the policies and procedures in place are appropriate, observed and compliant with legal, regulatory, normative and prudential requirements. 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 objectives, scope, conclusions and recommendations and appropriate action plans. Internal auditors should ensure adequate monitoring of the corrective measures taken by operational managers in response to these recommendations.

Reports should facilitate the board of directors' periodic review of the compliance management framework and compliance function activities. They should help it assess the reliability of the assurance provided by the chief compliance officer and senior management as regards compliance oversight of operational management and independent supervisory functions, in particular the compliance function.

3. Oversight of sound and prudent management practices

In seeking to promote sound and prudent management 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.