AUTORITÉ
DES MARCHÉS
FINANCIERS

COMPLIANCE GUIDELINE

April 2017

Contents

Introduction[1]

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 a 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 are 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[2] and the International Association of Insurance Supervisors[3] 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,[4] 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.

1 This guideline was first published in April 2009

2 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. *Joint Forum, Principles for the supervision of financial conglomerates*, September 2012.

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

4 *Insurers Act*, CQLR, c. A-32.1, section 463; *Deposit institution and deposit protection act*, CQLR, c. I-13.2.2, section 42.2; *Act respecting financial services cooperatives*, CQLR, c. C-67.3, s. 565.1; *Trust companies and savings companies Act*, CQLR, c. S-29.02, section 254.

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[5] 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 with 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[6] and the internal audit function,[7] as applicable;
- 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.

5 These may be programs, processes or structures.
6 A reference to the compliance function can also include any other independent oversight function in the second line of defense.
7 A reference to the internal audit function can also include any other independent assessment function in the third line of defense.

Compliance function

Compliance function independent of the activities it oversees is a key component of a financial institution's second line of defense[8] 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 could be involved in business units.[10] 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,[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 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.

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;

8 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*)

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*.

- 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[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.[13]

[12] Autorité des marchés financiers, *Outsourcing Risk Management Guideline*.
[13] Autorité des marchés financiers. *Governance Guideline*.

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[14] are generally assigned the following 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 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;
- 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 compliance 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.

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:

[14] Autorité des marchés financiers. *Governance Guideline*.

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

- 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[16]

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 for his opinion on the adequacy, observance and effectiveness of controls at all levels of the financial institution;
- 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;

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

- 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[17]

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.

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.

[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.