DRAFT

AUTORITÉ DES MARCHÉS FINANCIERS

GOVERNANCE GUIDELINE

Initial publication: April 2009
Updated: July 2016

TABLE OF CONTENTS

Preamble **2**

Scope **3**

Coming into effect and updating **4**

Introduction **5**

1. Governance of a financial institution **6**

2. Role and responsibilities of the board of directors and senior management **8**

2.1 Role and responsibilities of the board of directors 8
2.2 Senior management's roles and responsibilities 12

3. Governance framework **13**

4. Internal control **16**

5. Risk Management **18**

6. Compliance **19**

7. Audit functions **21**

7.1 Internal auditing 21
7.2 External Auditors 22

8. Remuneration policy **24**

9. Disclosure and transparency **26**

Oversight of sound and prudent management practices **27**

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 and the complexity of their activities. In this regard, the guidelines illustrate how to comply with the principles described.

AMF Note

The AMF considers governance, integrated risk management and compliance (GRC) as the foundation stones for 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 governance practices.

Scope

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

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

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 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 Governance 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, complexity and risk profile, and to have adopted the principles underlying this guideline since April 1, 2011.

The Governance Guideline has been updated to July 1, 2016 to reflect the evolution of principles of sound and prudent management emanating from international bodies involved with governance. If an institution has already set up such a framework, the AMF may verify whether such a framework enables it to comply with the legal requirements.

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

Introduction

In the financial products and services industry, which depends on the confidence of consumers, sound governance is crucial. It constitutes the cornerstone of sound and prudent management.

With this in mind, the AMF wishes to ensure that financial institutions adopt sound governance practices by adopting and promoting a corporate culture based on ethical behaviour and accountability for boards of directors and senior management.

Corporate culture refers to the common values and standards that define a business and influence its mindset, conduct and the actions of all its staff. A good corporate culture is therefore essential to the viability of a financial institution, which fundamentally depends on the confidence of consumers. Conversely, a culture that has deficiencies can cause serious harm and damage an institution's reputation to the point where its viability is jeopardized.

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 for financial institutions to implement sound governance practices 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 governance.

[3] Basel Committee on Banking Supervision, Bank for International Settlements. *Corporate Governance Principles for Banks (Guidelines),* July 2015.

[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. Governance of a financial institution

> The AMF expects financial institutions to have efficient and effective governance based on a corporate culture which takes into account the long-term interests of the financial institution and its customers.

Efficient and effective governance is the cornerstone of the sound and prudent management of a financial institution.

This section gives an overview of the aspects the AMF considers essential to ensure effective and efficient governance of a financial institution. These components are described in detail in the following sections. They are primarily: a description of the roles and responsibilities of the board and senior management, a formal governance framework, internal controls, supervisory[6]and audit responsibilities, a remuneration policy and the transparent disclosure of information to all stakeholders.

In general terms, governance describes the administrative organization of an institution for the purpose of achieving its objectives, guiding it and managing its risks. To ensure the exercise of effective and efficient governance, it is essential that the roles and responsibilities of members of the board of directors and senior management be clearly defined, and more specifically as they relate to a corporate culture which reflects its fundamental values.

Efficient and effective governance involves implementing a formal operating structure, monitoring and accountability through policies, procedures and information systems that help organize and oversee the management of the financial institution.

Efficient and effective governance requires risk management and control mechanisms throughout the organization's various sectors and levels, which entails a rigorous and coordinated approach. In this regard, the three lines of defense model[7] is suitable for all types of financial institutions and can be adapted according to their nature, size, complexity and risk profile. It provides a reliable structure which allows a distinction to be drawn between the roles and responsibilities of everyone involved. Using this model, financial institutions can delegate and coordinate the risk management and control functions according to a systematic approach based on the three lines of defense:

- The first line of defense corresponds to functions related to controls and corrective action by managers who have day-to-day ownership and management of risk and control.
- The second line of defense includes various risk management and compliance functions that include finance and actuarial practices, where applicable.

[6] In particular finance, risk management, compliance and, where applicable, actuarial practices.

[7] The institute of Internal auditors. *Leveraging COSO across the Three Lines of Defense*, July 2015.

- The third line of defense, internal auditing, provides independent, objective assurance regarding the overall effectiveness of risk management, control and governance processes.

Compensation is another important and intrinsic aspect of good governance for a financial institution and it is therefore expected that financial institutions will adopt a remuneration policy for board members, senior management, executives with supervisory functions and employees with key roles in risk-taking. The policy should be articulated in such a manner that does not encourage excessive risk-taking and consider the financial institution's long-term interests.

Lastly, sound governance involves a financial institution disclosing the main aspects of its governance framework and being sufficiently transparent toward all interested parties to allow them to assess the institution's effectiveness and performance

2. Role and responsibilities of the board of directors and senior management

The AMF expects the roles and responsibilities of the board of directors and senior management to be clearly defined and separate to ensure that their members act with integrity, competently and independently.

The very nature of a financial institution, its role in the economy and the type of risks related to its operations are areas where officers must have a high level of expertise, the necessary qualifications and a good sense of judgment. In addition to these aptitudes necessary for the sound management of a financial institution, directors and senior management must also perform their functions with integrity. The AMF's expectations regarding these aspects are clearly described in a separate guideline[8].

The AMF also expects a majority of board members to be independent. The notion of independence is characterized by the ability of board members to collectively or individually exercise objective and impartial judgment over the financial institution's affairs without undue influence from senior management or third parties. Where directors are not independent, the institution should document the procedures used to foster open discussion and unbiased judgment.

The stability and effectiveness of a financial institution depend first and foremost on the accountability of directors and senior management. Particular attention should therefore be paid to the quality of the monitoring and control carried out by senior management and the board of directors when policies are developed and strategic decisions made. Managing a financial institution requires an in-depth understanding of the entity, the environment in which it operates, its sectors of activity and its risk profile. This knowledge may also encompass areas such as the nature of risk, regulation, lines of business, products, and accounting and/or actuarial principles. From this perspective, it would seem essential for financial institutions to set out their intentions with respect to succession planning and remuneration for key management positions in a policy or other document.

2.1 Role and responsibilities of the board of directors[9]

The board of directors supervises the tasks carried out by senior management. As such, it must ensure that effective governance mechanisms are implemented, in particular by taking into consideration the relevant reports by senior management resulting from the application of these mechanisms. In this regard, the board of directors must also ensure that the roles and responsibilities given to board members, senior management and individuals performing a supervisory role at the institution are clearly defined in order to foster an adequate separation of supervisory responsibilities from management responsibilities.

[8] *Guideline Governing Integrity and Competency Criteria*, June 2012.

[9] "Board" may refer to a committee to which certain functions have been delegated.

The board of directors must be composed of members whose qualifications and skills meet the requirements of their position. The board's mission must be provided in writing and cover the roles and responsibilities assigned to board members.

Although the board members are collectively responsible for the decisions made and the financial institution's results, the chair of the board plays a key role in ensuring that the institution runs smoothly. In this regard, to ensure the board of directors remains independent and can effectively fulfil its duties, it is important that the role of chair of the board be separate from that of the institution's president and chief executive officer.

Elected by a majority of the board members, the chair should have the trust of his or her colleagues as well as the executives, managers and, where applicable, the institution's partners or shareholders. The chair must provide leadership by presiding meetings where discussions are free and transparent, allowing everyone to put forward their points of view. From this perspective, the chair must exercise good judgement in dealing with potentially diverging opinions within time constraints while ensuring rapid and informed decision-making.

Under sound governance practices, board members are also urged to conduct a regular assessment of the work carried out by the board and its committees as well as a self-assessment. This type of exercise maintains and strengthens the effectiveness of the board of directors.

The board of directors is generally responsible for setting up a corporate culture, governance framework and strategic objectives in keeping with the financial institution's long-term interests.

More specifically, the customary roles and responsibilities of the board of directors are to:

- actively participate in the choice, review and assessment of objectives, strategies and business plans;
- obtain reasonable assurance on a regular basis that the financial institution maintains control over its environment and risk management;
- review and approve policies developed for supervisory functions, major initiatives and significant activities[10];
- review and approve the organizational structure and governance framework;
- ensure that its members, senior management and individuals with supervisory functions act with integrity and are competent[11];
- develop and approve a remuneration policy for board members, senior management and other key positions that is in line with the institution's long-term interests;

[10] An activity is considered significant where it contributes to the achievement of the institution's objectives and strategies.

[11] Autorité des marchés financiers. *Guideline Governing Integrity and Competency Criteria*, June 2012

- undertake succession planning for board members, senior management and other key positions;
- regularly review the financial institution's performance as it relates to its objectives, strategies and business plans.

Audit Commitee[12]

Legislation[13] requires financial institutions to set up an audit committee within the board of directors. The main functions of this committee generally consist in reviewing the financial statements and the internal control and risk management mechanisms[14] implemented by senior management to ensure that the principal risks are properly managed and reported to the relevant persons.

Along the same lines, the audit committee should:

- be separate from the other committees;
- be chaired by a person who is independent and is not the chair of the board of directors or any other committee;
- be made up exclusively of independent or non-executive members; and
- include members who, for example, have experience in audit practices, financial information, accounting or risk management.

It is expected that the audit committee will obtain independent and objective assurance of the effectiveness of the governance, risk management and internal control processes, primarily from the internal audit but also from the external audit, especially with respect to the financial statements. To do so, the audit committee should:

- verify the auditors' independence and objectivity vis-à-vis senior management;
- promote an environment conducive to transparent discussions between senior management and the auditors;
- understand the audit strategy and ensure that the main audit risks are taken into account[15];
- oversee the auditors' work and assess the effectiveness of the audit.
- surveiller les travaux des auditeurs et évaluer l'efficacité de l'audit.

The audit committee's obligations regarding the internal audit are generally to:

---

[12] The term covers both *comité de vérification* and *comité d'audit* in French.

[13] *An Act respecting insurance*, CQLR, c. A-32, section 298.1;
An Act respecting financial services cooperatives, CQLR, c. C-67.3, section 253.1;
An Act respecting trust companies and savings companies, CQLR, c. S-29.01, section 282.

[14] These two functions could also be assumed by a risk management committee if such a committee exists.

[15] The risk of the auditors coming to improper conclusions and giving erroneous opinions based on their work.

- approve and review the internal audit charter setting forth the mission, powers and duties of the internal auditing function;
- approve the internal audit plan based on risk;
- approve the budget and provisional internal audit resources;
- approve appointment, renewal, dismissal and remuneration decisions involving the person in charge of the internal audit;
- ensure it receives information provided by the person in charge of the internal audit regarding progress on the audit plan or any other issue involving the internal audit;
- ask senior management and the person in charge of the internal audit for information to help determine whether the internal audit framework and resources are adequate.

By maintaining a good relationship with the internal audit, the audit committee will be able to ensure that its charter, activities and procedures are appropriate, understood and always meet its needs and those of the board of directors.

As regards external audits, the audit committee should, in general terms, be responsible for the following:

- scope of the audit plan;
- skills and resources of the external auditor;
- recommendations concerning the appointment, renewal, removal and remuneration of the external auditor;
- periodic review of the effectiveness and quality of the work performed by the external auditor;
- independence of the auditor as well as the auditor's internal quality control practices and policy;
- compliance with accounting and actuarial practices as well as assurance that they are conservative and appropriate;
- ensuring receipt of all material correspondence between the external auditor and senior management regarding audit findings, in accordance with current Canadian generally accepted accounting principles;
- quality of the financial statements, including a fair presentation of the institution's financial position.

The audit committee should also be able to meet regularly with the persons involved in the internal audit, risk management, compliance, actuarial practices, etc. It should also set up a private meeting with them at least once a year which senior management does not attend in order to confirm their independence within the financial institution and discuss certain issues and any points of disagreement with senior management, among other things.

2.2 Senior management's roles and responsibilities

Senior management generally carries out all functions related to the management and operation of the organization in a manner which is consistent with the strategy, risk appetite and tolerance, and policies approved by the board of directors.

Senior management of a financial institution plays a key role in the governance structure. It is not only the architect of the systems and processes essential to the governance framework, it also ensures that the various management and reporting mechanisms are effective.

The main roles and responsibilities of senior management are to:

- plan, conduct and control the financial institution's activities;
- develop strategies, business plans, operational objectives, organizational structure and controls;
- ensure that the organizational structure and control measures are effective and regularly report to the board of directors;
- develop policies for approval by the board of directors;
- develop and promote sound management and governance practices;
- promote a corporate culture based on ethical conduct, sound risk management and compliance practices, and the fair treatment of consumers;
- monitor the achievement of operational objectives, strategies and plans approved by the board of directors.

A financial institution's decision-making bodies are the pillars on which a formal governance structure that meets the AMF's expectations stands. The following section describes the requirements for setting up such a governance framework.

3. Governance framework

The AMF expects financial institutions to develop and set up a governance framework based on their nature, size, complexity and risk profile.

The governance framework sets forth and formalizes the strategies, policies and procedures to be put in place in order to define and organize the various aspects of effective and efficient governance described in the previous section which will ensure the sound and prudent management necessary to protect the interests of policyholders or depositors.

Drawing up a governance framework must take into consideration the specific characteristics of the entity, whether it is a co-operative, mutual organization and company and whether or not it is a member of a financial group, as well as the activities carried out through subsidiaries across their operating territory.

A financial institution's governance framework should also reflect changes made over time. The quality of governance practices is important for maintaining market confidence and, in this regard, they should evolve in a manner which reflects new practices, including those involving technology and industry standards.

Through the governance framework, the board of directors demonstrates its determination to apply rigorous governance principles within the financial institution.

However, the governance framework must be flexible and transparent enough to favour appropriate, timely decision-making in order to achieve the financial institution’s strategic goals. It must also be developed based on the nature, size, complexity and risk profile of the financial institution and take into account various other factors such as the ownership structure, organizational structure and available resources.

It must allow a financial institution to co-ordinate the initiatives intended to improve its management practices based on more subjective factors such as its culture and values. Once established, the governance framework allows the strategy and objectives to be aligned with the institution’s risk culture and ensures the sound and prudent management of its operations at all times with integrity and in accordance with the law.

An effective governance framework generally ensures that the risk management and control procedures function properly. This requires strict coordination between three separate groups of activities which can be broken down into three lines of defense.

First line of defense

Operational managers constitute the first line of defense involving the day-to-day management of risk since they develop and implement the controls and oversee their integration into the systems and processes. Their duties in this regard are to:

- identify, assess, manage and control risk;
- lead the development and implementation of internal control procedures;

- monitor the application of the procedures by those involved;
- point out risk exposures taking into account the financial institution's risk appetite and risk tolerance levels and related policies and controls;
- ensure that the activities are compatible with the objectives set.

The operational managers must also implement the remediation of deficiencies and fulfil their duties in accordance with the risk culture established by the board of directors.

Second line of defense

These supervisory functions are created by senior management to ensure the proper design, effectiveness and adequate operation of the first line of defense. They are involved in setting up and/or overseeing operational controls and vary depending on a financial institution's typology and characteristics. A second line of defense should generally include supervisory functions covering among other things risk management, compliance, finances and, where applicable, actuarial practices[16].

The duties include:

- supporting senior management in setting up internal control mechanisms to mitigate risk;
- adequately and effectively monitoring internal control;
- issuing instructions and providing training about risk management procedures;
- reviewing compliance with laws and regulations;
- reporting to the board of directors; and
- uncovering deficiencies and taking corrective action on a timely basis.

The functions involved in the second line of defense should be independent from the management of operations. 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 and its degree of independence. For example, some financial institutions could ensure independence by merely separating duties or setting up mechanisms to such effect.

Third line of defense[17]

Internal auditing is a supervisory function independent of the first two lines of defense which should provide the board of directors and senior management with global and objective assurance, through a risk-based approach, regarding the effectiveness of

[16] Given their special importance for the prudential regulation of financial institutions, the main components of the second line of defense relating to the internal control mechanisms, risk management functions and compliance will be discussed in separate sections of this guideline.

[17] IIA Position Paper. *The Three Lines of Defense in Effective Risk Management and Control*, January 2013.

governance, risk management procedures and internal control mechanisms and their adequacy given the financial institution's activities.

This global assurance covers the following:

- effectiveness and efficiency of operations;
- safeguarding of assets;
- reliability and integrity of financial and operational information;
- compliance with laws, regulations, policies, procedures and contracts;
- all components of the risk management and internal control referential (control environment, risk identification, assessment and treatment, information and communication, etc.);
- the financial institution's entire group, including divisions, subsidiaries, operational units and departments.

As mentioned above, the next three sections will discuss internal control, risk management and compliance in greater detail.

4. Internal control

> The AMF expects financial institutions to implement internal control mechanisms that meet targeted objectives and support the achievement of those objectives.

Internal control is generally a set of control mechanisms implemented in a financial institution to give its decision-making bodies reasonable assurance that the objectives relating to the following will be reached:

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

Internal control is an essential component of an effective governance structure since it helps to detect functional weaknesses, which could be a major source of risks for a financial institution. As a result, the control mechanisms of which it consists should be designed and implemented to ensure the financial institution's key policies and processes are operationally, technologically and financially effective, ensure the reliability of accounting and financial reports, and ensure the presence of adequate measures for the sound and prudent management of a financial institution.

Since internal control involves all levels of the financial institution, staff involved must be aware of the importance of internal control mechanisms and receive for that purpose clear communications from senior management. It is therefore essential that the pertinent information be identified, gathered and communicated in a form and timeframe that enables the individuals concerned to adequately assume their responsibilities.

This exercise should ensure that internal control mechanisms adequately meet the objectives set by the institution. More specifically, the assessment of the effectiveness of internal control functions could include the following:

- the strategy adopted regarding the control mechanisms;
- how far their implementation has progressed;
- information about the resources required;
- the situation per sector and business unit;
- a description of the problems and deficiencies encountered.

Furthermore, depending on the nature, size and complexity of the financial institution's activities, effective control mechanisms should cover the following:

- the appropriate segregation of duties, where necessary;
- the policies for approving decisions and verifying the authenticity of authorized signatories;

- the presence of controls adapted to each appropriate level of the organization;
- training relating to internal control, particularly for employees with important responsibilities or those involved in high-risk activities;
- consistency of the internal control overall and for each individual mechanism;
- verifications and tests conducted by independent parties (internal or external auditors) as to the effectiveness of the control mechanisms already in place.

As for the board of directors, it is generally given a specific role—that of conducting a periodic comprehensive assessment of the internal control mechanisms and, consequently, approval of the major changes made to it. This assessment ensures that operations meet the objectives set by the financial institution.

As part of the review of internal control, the board of directors could for example base its assessment on the following sources:

- reports from senior management pertaining in whole or in part to the financial institution's operations and financial condition, risk management system, compliance and other control mechanisms or any departure from them;
- reports from the supervisory functions;
- internal and external audit opinions on the adequacy of the financial institution's controls;
- the external audit report on the audited financial statements, including any communications with senior management;
- opinions solicited by the board of directors from legal counsel;
- for insurers, the actuary's report on provisions and reserves and the Dynamic Capital Adequacy Test (DCAT);
- the recommendations, observations or opinions of the financial institution's regulator.

As applicable, it is the board's responsibility to ensure that senior management takes prompt action to correct any material control problems identified in connection with the assessment and ensure that they are adequately monitored.

In the following section we will discuss risk management, an important part of the second line of defense and one of the foundations of the AMF's prudential oversight.

5. Risk Management

The AMF expects financial institutions to set up a risk management framework supported by sound governance involving the board of directors and senior management.

Risk management is a structural, consistent and ongoing process allowing potential events to be identified, assessed, managed and controlled while taking account of opportunities and threats which could affect the achieving of defined objectives. The aim is to ensure to the extent possible that a financial institution can reach its goals. Effective risk management ensures that the most important risks are watched carefully and includes systematic monitoring of emerging risks.

To do so, the financial institution should have effective strategic management, an efficient operations management system and a proactive and integrated risk assessment system. In the case of institutions that are members of a group, the risk management function[18] could already be present within the group and may not require the creation of an additional independent supervisory unit within the entity.

Regardless, as a second line of defense, it is important that the individual in charge of risk management:

- be independent from the business units involved in risk-taking;
- have the power and resources necessary to obtain all information required to monitor and manage risks;
- be in a position to influence strategic decisions involving risk-taking;
- have free access to the board of directors.

Effective and efficient risk management procedures should:

- allow current and emerging risks to be controlled;
- set risk appetite and risk tolerance levels based on strategic goals and capital availability and supervise the financial institution’s position with respect to approved variables.

It is therefore essential that the financial institution be able to identify all material risks to which it is exposed, evaluate the potential impact of these risks and implement measures to effectively manage them.

The implementation of sound governance at a financial institution is therefore contingent on the contribution of various mechanisms which, in addition to internal control and risk management, include compliance, one of the most important foundations of our oversight and another important function of the second line of defense.

[18] The AMF’s *Integrated Risk Management Guideline*, in effect since April 1, 2009 and revised on May 1, 2015, provides more information about this function, describing the roles and responsibilities of the board of directors, senior management and the risk management officer.

6. Compliance

The AMF expects financial institutions to set up a compliance function[19] in charge of establishing a compliance management policy and procedures involving legal, regulatory and normative requirements covering all their activities and ensure that they are updated periodically.

A compliance function[20] independent of the activities it oversees is a key component of a financial institution's second line of defense which is essential to its sound and prudent management. This function should ideally be carried out by a compliance officer or, if the institution does not have such a position, a member of senior management.

Senior management must set up a compliance management framework that is approved by the board of directors. The framework contains the basic principles allowing exposure to regulatory risks to be identified, assessed, managed, mitigated, monitored and communicated[21] at all levels of the financial institution. This ensures that knowledge about regulatory requirements is kept up-to-date and that the financial institution operates with integrity and in accordance with its legal obligations.

The compliance function also has an information, training and advisory role in terms of the board of directors, senior management and staff, particularly for employees involved in high-risk activities. The compliance function should:

- inform the board of directors and senior management about the financial institution's compliance with the laws, rules and standards, any inadequate processes and the latest developments in compliance;
- help train staff about compliance matters;
- act as a liaison for staff issues involving compliance;
- provide staff with advice about the appropriate application of laws, rules and standards in the form of policies, directives, procedures and other documents.

To be effective, the compliance function should have sufficient power and authority, an adequate position in the hierarchy, independence from operational management, the resources it requires and free access to the board of directors.

The compliance function should be entrusted to a member of senior management or an individual with enough authority to ensure his or her complete independence.

[19] The AMF's *Compliance Guideline*, in effect since April 1, 2009, provides more information about this function, describing the roles and responsibilities of the board of directors and senior management.

[20] A compliance function is not necessarily a particular unit within the financial institution. The staff in charge of compliance may be involved in operational units and report to the department responsible for the operations in question. However, where applicable, those units must be able to report to the compliance officer, who should be independent of operational management.

[21] Autorité des marchés financiers, *Compliance Guideline*, April 2009. The risk of non-compliance with the laws, regulations and guidelines to which financial institutions are subject.

For the first and second lines of defense to be effective, a third line of defense must be set up. This role is played by the internal audit function and will be discussed in the next section, which will also cover the role of the external auditors who constitute an objective and independent reinforcement of the third line of defense regarding financial information in particular.

7. Audit functions

7.1 Internal auditing

The AMF expects financial institutions to set up an independent internal audit function able to provide them with global and objective assurance of the effectiveness of their governance, risk management processes and internal control mechanisms and their adequacy in view of the financial institutions' activities.

An effective and efficient independent internal auditing function constitutes the third line of defense of the governance framework in that it gives the financial institution global and objective assurance regarding the degree of control over its operations, provides it with advice to increase operational efficiency and creates added value.

In terms of governance, the internal audit activity must carry out independent and objective assessments of the design, adequacy and operational effectiveness of the processes and make appropriate recommendations for improving them. The goal is to provide the board of directors and senior management with reasonable assurance that these processes are well designed, work well and contribute to the accomplishment of the following objectives:

- promoting appropriate ethics and values within the organization;
- ensuring effective organizational performance management and accountability;
- communicating risk and control information to appropriate areas of the organization; and
- coordinating the activities of and communicating information among the board, management, the external auditors and even the internal auditors.[22]

The internal audit activity must also evaluate the effectiveness and relevance of risk management processes and internal controls and promote continuous improvement, including the achievement the organization's strategic objectives in these two areas by the functions making up the first and second lines of defense.

To effectively fulfil its role as the third line of defense, the internal audit should have a high-level, dual-reporting relationship to ensure it is unbiased and confirm its objectivity within the financial institution. According to the International Auditing Standards, this function should report to the board of directors and/or audit committee on an operational level[23] and to senior management on an administrative level.[24]

[22] The Institute of Internal Auditors, Standard 2110.

[23] Senior management should facilitate the internal auditing of its daily operations such as budgeting, accounting, the administration of human resources, internal communications, the management of rules and procedures, etc.

[24] The Institute of Internal Auditors, Standard 1100.

For internal auditing to actively contribute to the effectiveness of the institution's governance mechanisms, certain conditions must be met regarding its organizational independence in its relationship with the board of directors and senior management. In this regard, the internal audit function must be in a position to:

- directly and regularly communicate with the board of directors and/or the audit committee and report directly to them;[25]
- report to a member of management with a sufficiently high position to encourage independence and ensure a comprehensive audit;
- access records, personnel and resources necessary to fulfil its mission;
- coordinate activities with external auditors to ensure proper coverage and minimize duplication of efforts;
- have staff that possess the knowledge, skills, and other competencies needed to perform their individual responsibilities;
- perform its work freely, objectively and make impartial decisions by not allowing the auditors to:
  - be involved in management functions or oversee operations;
  - assess specific operations over which they exercised authority or for which they were responsible the previous year;
  - subordinate their judgment on audit matters to others;

Although the AMF is aware that the level of maturity of the governance processes within a financial institution, the organizational role of the internal auditing activity and the qualifications of the auditors are all factors which influence the audit activities with respect to governance, the setting up of an internal auditing function should be part of the sound governance of any financial institution.

On the one hand, where institutions are members of a group, the internal audit function could act on behalf of the entire group so that an additional function need not be created. On the other hand, if some or all of internal auditing is outsourced or where a function other than the internal audit is responsible for supervisory independence, the board of directors is nonetheless responsible for overseeing its performance in order to obtain reasonable assurance of the effectiveness of its processes and activities.

7.2 External Auditors

The external auditors play a vital role in maintaining consumer confidence in financial disclosure by assessing the risk of significant anomalies, including in terms of the assertions and financial statements (fraud, errors, etc.) and ensuring that the financial statements are prepared and disclosed in accordance with applicable accounting rules and principles.

[25] The person in charge of internal auditing should meet privately with the board of directors and/or the audit committee at least once a year in the absence of senior management and confirm his or her independence from the financial institution annually.

Based on applicable best practices, the external auditors should:

- be supervised and evaluated by the audit committee/board of directors as to the quality the effectiveness of their work;
- be continually rotated to avoid the presence of situations which could affect their independence and objectivity;
- be designated, renewed, removed, supervised, evaluated and compensated following a decision of the audit committee/board of directors;
- have the necessary skills and integrity to perform their mandate;
- be able to address the audit committee/board of directors directly, in the absence of senior management;
- have free access to individuals and information in order to carry out their audit work;
- coordinate their work with that of the internal auditors to avoid duplication and maximize efficiency.

Provided there is effective coordination, the external auditors can be considered an additional line of defense,[26] giving the board of directors, management and shareholders assurance in addition to that provided by the internal auditors.

[26] The external auditors and regulators play an important role in a financial institution's overall governance and control. In this regard, they can be considered a fourth line of defense (Bank for International Settlements, Occasional Paper No. 11, *The "Four Lines of Defense Model" for Financial Institutions*, December 2015).

8. Remuneration policy

The AMF expects financial institutions to implement remuneration mechanisms which do not encourage excessive or inappropriate risk-taking and which take into account the long-term interests of the institution and its stakeholders.

Sound remuneration practices form an integral part of the good governance of any financial institution. The adoption and implementation of a remuneration policy is not intended to unduly limit or reduce an institution's ability to attract and retain qualified persons by requiring a particular form or level of remuneration. As it considers remuneration an element which forms part of effective risk management, the AMF wishes instead to promote the adoption by financial institutions of a remuneration policy which takes its risk appetite and long-term interests into account in order to avoid excessive risk-taking.

It is up to the board of directors to ensure that the remuneration policy is comprehensive enough to apply to board members and senior management, persons performing supervisory duties and employees playing a key role in risk-taking.

The board of directors should have the necessary competencies to make informed and independent decisions regarding the relevance of the remuneration policy. These competencies, whether through a remuneration committee or not, require on the one hand a sufficient understanding of the relationship between risk-taking and remuneration and, on the other hand, the participation of persons who are not part of senior management in order to foster objectivity in the decision-making process.

In short, the board of directors should be satisfied with the overall consistency of the institution's remuneration policy with its risk appetite, risk tolerance levels and long-term interests. To this end, special care should be given to certain aspects of remuneration, and in particular:

- the proportion of fixed and variable components;
- the use of performance criteria;
- the structure of the remuneration of key employees involved in risk-taking;
- the individual remuneration of board members and senior management;
- the publication of reports or disclosure concerning the institution's remuneration practices.

The board of directors should also ensure that persons involved in drawing up the remuneration policy work closely with those in charge of risk management in order to promote the alignment of risk and remuneration which varies throughout the organization.

However, to maintain the integrity and objectivity of staff involved in supervisory duties and reduce the potential risk of conflicts of interest, the remuneration of these persons should:

- be primarily based on the actual achievement of objectives appropriate to their supervisory function;
- where applicable, not be tied to the performance of business units subject to supervision but rather, to the institution's overall performance;
- be generally adequate and generous enough to attract and retain individuals with the skills, knowledge and expertise required to perform their function;
- if this function is outsourced[27], be compatible with the objectives and parameters of the existing remuneration policy.

Finally, when variable remuneration components are present, they should be established using performance measures which take into account the creation of long-term value and the temporal horizon of the risks to which the institution may be exposed while avoiding the creation of incentives which could lead to inappropriate risk-taking. To this end, the performance criteria applicable to the variable components of remuneration should:

- be clearly defined and measurable objectively;
- be based on financial and non-financial criteria, as the case may be;
- take into account not only the individual's performance, but also that of the business unit, where applicable, and the financial institution's overall results;
- only use growth and volume as criteria if they are paired with other performance criteria.

Ultimately, to be effective and prevent conflicts of interest, establishment of the remuneration policy should be independent, then reinforced by objective monitoring of its application.

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

9. Disclosure and transparency

L'Autorité s'attend à ce que l'institution financière divulgue les principaux aspects de son cadre de gouvernance et soit suffisamment transparente envers toutes les parties prenantes en considération de la nature de leurs activités.

This disclosure should enable stakeholders to understand the financial institution's governance structure. Regardless the vehicle used to achieve this, transparency remains the key to satisfactory disclosure. The institution could use its annual report, website or any other support provided disclosure is done efficiently and in a timely manner, allowing stakeholders to come to an informed judgment of the ability of the board of directors and senior management to govern the financial institution.

To ensure this transparency, subject to commercially sensitive information and any confidentiality undertakings which may apply, the financial institution's communication strategy should include information that is relevant and useful to understanding the key aspects of the institution's governance. Accordingly, the disclosure of official information such as the organization's financial situation, performance and structure should be taken into account. In addition, any event or other material information which could affect one or more market participants should also be disclosed as soon as possible, within the timeframes prescribed by regulation.

As a general rule, the disclosure of information should be sufficiently complete and detailed for stakeholders to be able to come to a clear opinion on the institution's performance in terms of its ability to exercise good governance. Accordingly, as good practice, disclosure should also include elements such as information about the strategic goals, organizational structure, qualification of board members, remuneration policy, share ownership and voting rights, principal affiliations and alliances, and material transactions between related parties.

To achieve transparency, the following could also be disclosed: elements such as the independence criteria used and applied to key positions of responsibility, rules of conflict of interest, risk management systems, internal control, and reference to events during the reporting period.

Finally, as part of its supervisory role, the AMF might ask for additional information which could include sensitive information, such as the board's assessment of the governance framework, internal audit reports and details about the remuneration structure, and more specifically as it relates to risk-taking.

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 oversight work, assess the degree to which the principles set forth in this guideline are followed given the specific characteristics of each institution. The quality of the supervision and control carried out by the board of directors and senior management will also be assessed.

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