DRAFT

AUTORITÉ DES MARCHÉS FINANCIERS

OPERATIONAL RISK MANAGEMENT GUIDELINE

October 2016

TABLE OF CONTENTS

Preamble

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

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

AMF Note

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

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

Scope

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

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

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

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

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

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

Coming into effect and updating

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

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

Where an institution has already implemented such a framework, the AMF may verify that the framework allows the institution to satisfy the prescribed legal requirements.

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

Introduction

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

Since operational risk is inherent in all business activities, an entire institution is exposed to this type of risk, particularly through insufficient or ineffective control of people, processes, systems or external events.[5] The use of new technology as well as the sustained paces of structural change increase the exposure of financial institutions to such risks.

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

In addition, the management of risks inherent to people, processes and systems helps determine the level of tolerance to operational risk and the oversight of risks according to business lines, along with the optimization of processes and information systems, as recommended in the *Integrated Risk Management Guideline*.[7]

Given the general nature of this guideline, it will henceforth be the umbrella guideline for more specific guidelines on topics related to operational risk, including business continuity management,[8] outsourcing risk management[9] and financial crime risk management.[10] As a result, any new prudential framework regarding the risks inherent to people, processes, systems or external events will clarify the broad principles set forth herein.

---

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

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

5 The Basel Committee defines operational risk as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk. Bank for International Settlements. *Principles for the Sound Management of Operational Risk*, June 2011.

6 Autorité des marchés financiers. *Governance Guideline,* April 2009. An updated *Governance guideline* was published for comments on March 31, 2016.

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

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

9 Autorité des marchés financiers. *Outsourcing Risk Guideline*, April 2009, updated December 2010.

10 Autorité des marchés financiers. *Financial Crime Risk Management Guideline*, June 2012.

It is important to note that this guideline does not consider either the modeling or quantification of operational risk since this issue is specifically discussed in the framework relating to the capital requirements of the various entities referred to above. Furthermore, the prudential orientations regarding operational risk management should be seen as complementary to the calculation of operational risk capital requirements rather than a consequence of that activity, as suggested by the Basel Committee[11].

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

1. Operational risk management

The AMF expects a financial institution to adequately manage its operational risk in relation to its strategy and risk appetite. Such management should take account of the operational risk exposure of all people, activities, processes and systems of the institution as well as those of third parties.

Operational risk management

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

This awareness initiative should be aimed notably those involved in the implementation of various products, activities, processes and systems within the institution.

Awareness should also target stakeholders outside the institution, including key service providers, since outsourcing exposes an institution to operational risks (e.g. cyber-risk exposure). Also, the culture can be strengthened by providing ongoing training on how to deal with operational risks for individuals in charge of all units.[12]

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

Operational risk management should also bring to light situations where the conduct of players associated with particular products, activities, processes or systems does not ensure the fair treatment of consumers.[13] As an example, a security breach caused by an accidental disclosure of a customer's personal information or the deliberate leaking of confidential information constitutes the forms of operational risk that might affect the fair treatment of consumers, which could ultimately achieve the reputation of an institution.

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

Such changes can require a review of operational risk tolerance levels. However, it is expected that this type of decision will be the result of discussions among all stakeholders. In this regard, board approval will be required.

12 In the context of this guideline, a unit corresponds to the institution's smallest component to which operational or administrative responsibility is given.

13 Autorité des marchés financiers. *Sound Commercial Practices Guideline,* June 2013.

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

Identification and assessment of operational risk

The AMF expects all stakeholders to contribute to the identification and assessment of the operational risk inherent in their respective business sectors. To standardize the identification of this type of risk, institutions should set up a common taxonomy and identification tools giving decision-making bodies a comprehensive view of the exposure to operational risks.

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

- risk self-assessment exercises;
- control effectiveness analysis;
- loss events analysis both within and outside the institution;
- risks analysis specific to each product, process and system in place;
- scenario analysis based on experts' opinions;
- exposure quantification models.

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

In view of the expectations set forth by the AMF in its *Outsourcing Risk Guideline*, the operational risks inherent in all major outsourcing agreements should be identified and assessed. Moreover, financial institutions should also ensure that their key service providers use best operational risk management practices.

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

Oversight and disclosure

The AMF expects operational risk reports to reflect the actions taken by institutions to determine the significant sources of unmitigated risk and ultimately to comply with their tolerance level to such risks. In particular, it is expected that the effectiveness and efficiency of control measures in place will be monitored and that main actions proposed to mitigate the frequency and impact of operational incidents will be disclosed.[14]

Best practices militate in favour of setting up a register to record incidents where pre-established operational risk limits or tolerance levels are exceeded. An institution should ensure that the procedure for updating the register is consistent across all units according to pre-established policies.

Based on an analysis of the most significant incidents in the register, operational risk reports should allow the board of directors and senior management to pinpoint the main sources of unmitigated operational risk. Such reports should include the source, whether internal or external, as well as all expected impacts.[15] They should also incorporate the recommendations made by both the AMF and the audit functions, where applicable, about operational risk management as well as the corresponding action plans approved by decision-making bodies.

Furthermore, the board of directors and senior management should determine the most adequate means of presenting the effectiveness of their operational risk management to interested parties.

Control and mitigation

The AMF expects internal control mechanisms to efficiently mitigate the operational risk exposure inherent to people, activities, processes and systems related to a financial institution's operations.

The AMF has set forth its expectations regarding internal control mechanisms in its *Governance Guideline*. In relation to operational risk management, it is expected that such mechanisms will efficiently mitigate exposure to an institution's people, activities, processes and systems to operational risk. Such mechanisms should be adaptable, particularly based on how the institution's business evolves and technological change.

Regardless the mechanisms used by each institution, it is expected that their implementation will be uniform and adaptable to major changes in the activities, processes and systems related to its operations.

In addition, financial institutions using insurance to transfer operational risk should always use it as a complement to their own control mechanisms for this type of risk.

14 Autorité des marchés financiers. *Risk Data Aggregation and Risk Disclosure Guideline,* February 2016.

15 The *Business Continuity Guideline* recommends setting up procedures to identify major operational incidents.

2. Governance

Role of the board of directors and senior management

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

The implementation of a sound governance structure as set forth in the *Governance Guideline* and the *Guideline Governing Integrity and Competency Criteria*[16] is essential to the sound management of operational risk.

One of the roles of the board of directors is to ensure that senior management uses best efforts to make units aware of the importance of managing their operational risk exposure. Similarly, senior management must ensure that all stakeholders are given targeted training, particularly to the managers of such units. This way, the board of directors should ensure that senior management is supported by group expertise in managing operational risk.

The board of directors remains responsible for approving the operational risk management framework in accordance with their roles and responsibilities according to the *Governance Guideline*. It is also expected that the board of directors, supported by the work of the internal audit function, will ensure the effectiveness of the framework, its cohesion with the integrated risk management, as well as adaptation of the operational risk tolerance level.

Regarding the consistency of operational risk management with the integrated risk management framework, senior management should ensure that the individuals in charge of the different types of risk coordinate their efforts. Such coordination is also required in all units in order to avoid duplicating risk management efforts. The lines of defence should be called upon to validate and verify the integration of efforts to coordinate the management of different types of risk.

It is expected that senior management will then ensure that a procedure is set up for recording situations where operational risk limits are exceeded in an incident register. The register, along with any other mechanism used to report operational risks, should be used by all units and consulted by decision-making bodies as a source of information about required improvements to the management framework for this type of risk.

Also, in the event of a major organizational or technological change at an institution, the board of directors and senior management should ensure that the change complies with its tolerance level for operational risk.

It is also expected that senior management will ensure that exposure to operational risk resulting from key outsourcing agreements is considered by the persons in charge of operational risk management for the various units. The evaluation of any significant new outsourcing agreement should confirm the soundness of the operational risk management of the supplier or consultant in question.

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

The board of directors and senior management should base themselves on the different lines of defence to validate and verify that the operational risk management applies throughout all the institution's activities, processes and systems. To do so, they should ensure that each line of defence has the necessary resources to fulfil its duties and that their work is suitably coordinated.

Roles of the lines of defence

Since exposure to operational risk is inherent in all products, activities, processes and systems, the AMF expects an institution's governance structure to be strengthened by the ongoing participation of the different lines of defence with a view to optimizing their operational risk management.

Sound operational risk management should be ensured by the individuals in charge of the first line of defence in all products, activities, processes and systems related to their functions. In this regard, these individuals should have or acquire the necessary operational risk management skills, and their duties should be documented.

In addition, the individuals in charge of the first line of defence should report situations where their unit's risk tolerance levels have been exceeded using, for example, the operational risk incident register. These individuals are also responsible for dealing with the operational risks inherent in any new product, process or system implemented by their unit.

As for the second line of defence, it should be responsible for setting up a common taxonomy allowing operational risks to be identified and the governance mechanisms for this type of risk standardized. The individuals in charge of the first line of defence should in turn adopt this taxonomy and use it in their operational risk management.

It is essential that the second line of defence be independent of activities in order to adequately judge the effectiveness of the controls and other measures set up by the first line of defence to mitigate operational risk.

To make operational risk management more efficient, actors from the first two lines of defence should strive for constant communication, particularly when there are differences of opinion regarding the perception and treatment of operational risk for a particular unit. Regardless, it will be up to the chief risk officer to decide, for example, of the strategy to adopt where major differences persist.

The second line of defence should also coordinate its activities with all parties within the institution as regards the specific risks to people, processes and systems.

The draft updated *Governance Guideline* states that the second line of defence includes risk management oversight, among other functions. Accordingly, the oversight of operational risk management requires the setting up of a specialized function, ideally under the responsibility of the chief risk officer. Where such a position does not exist due to the institution's size, nature, complexity and risk profile, the function should be entrusted for example, to a member of senior management.

The third line of defence should be responsible for independently verifying the operational risk management carried out by the first two lines of defence. It is also expected that this line of defence will assess the role of senior management in promoting adequate operational risk management practices at all institution's levels, overseeing compliance with operational risk tolerance level, as well as ensuring the efficient cohesion of operational risk management with that of the institution’s other major risks.

3. Supervision of sound and prudent management practices

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

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

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