AUTORITÉ DES MARCHÉS FINANCIERS

OPERATIONAL RISK MANAGEMENT GUIDELINE

December 2016

Contents

Introduction

Operational risk management has been of growing interest in the financial sector for close to two decades. The Basel Committee on Banking Supervision (the "Basel Committee")[1] 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.[2] In response to these increasing concerns of international bodies, several members of the Organisation for Economic Co-operation and Development (OECD) have published guidance regarding operational risk management.

Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.[3] The use of new technology and the sustained pace of structural change increase financial institutions' exposure to such risks.

The AMF therefore considers operational risk to be 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 internal stakeholders[4] and primarily the board of directors, senior management and the different lines of defence.[5]

In addition, the management of risks inherent to people, processes, systems and external events helps determine the level of tolerance to operational risk and the oversight of risks according to business sector[6], 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 areas 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.

It is important to note that this guideline does not consider either the modeling or quantification of operational risk since these issues are 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]

---

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

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

3 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.

4 According to ISO 9001: 2015, the expression "stakeholders" includes any person or organization that may be affected by a decision or activity. In addition, Principle 5, adopted by the G7 countries to protect the financial system against cyberattacks, cites examples of both internal and external stakeholders, such as law enforcement, regulators and other public authorities, as well as shareholders, third-party service providers and consumers, as appropriate. [G7, *Fundamental Elements of Cybersecurity for the Financial Sector*, Principle 5, October 2016].

5 Autorité des marchés financiers. *Governance Guideline*.

6 For the purposes of this guideline, a unit corresponds to the institution's smallest component to which operational or administrative responsibility is given. A business sector can consist of one or more units.

7 Autorité des marchés financiers. *Integrated Risk Management Guideline*.

8 Autorité des marchés financiers. *Business Continuity Management Guideline*.

9 Autorité des marchés financiers. *Outsourcing Risk Management Guideline*.

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

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

1. Governance of financial institutions

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 reliable governance structure as set forth in the *Governance Guideline* and the *Integrated Risk Management Guideline* is essential to the sound management of operational risk.

1.1 Roles and responsibilities of the board of directors

In keeping with the operational risk management framework and the expectations in the *Governance Guideline and the Integrated Risk Management Guideline*, the board of directors should:

- approve and periodically re-examine the operational risk management framework;
- ensure the promotion of an operational risk management culture within the financial institution;
- ensure the effectiveness of the operational risk management framework and its consistency with the integrated risk management framework;
- supervise senior management to ensure that the operational risk management framework is being applied;
- approve and re-examine the operational risk tolerance level, supported principally by the work of the internal audit function.

1.2 Roles and responsibilities of senior management

In keeping with the operational risk management framework and the expectations in the *Governance Guideline* and the *Integrated Risk Management Guideline*, senior management should:

- implement and maintain policies, processes and systems reflecting the operational risk management framework in accordance with operational risk tolerance levels;
- ensure that adequate mechanisms are set up for reporting situations where operational risk tolerance levels are exceeded;
- establish hierarchical responsibilities and reporting in order to delineate the allocation of duties and promote and maintain accountability;
- ensure appropriate co-ordination and effective communication[12]. between, on the one hand, the chief risk officer and the operational risk officer and, on the other hand, between these two individuals, business line managers and outsourcing officers;[13]
- ensure the availability, sufficiency and adequacy of operational risk management resources;
- ensure that targeted risk management training is given to managers and their teams.

The board of directors and senior management has primary responsibility for defining the operational risk management framework and promoting a risk management culture. However, they can rely on the support of the various lines of defence to validate and verify that operational risk management is being applied to all of the institution's activities, processes and systems. To do this, they must ensure that each line of defence has the necessary resources and that their work is co-ordinated appropriately.

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

1.3 Roles and responsibilities of the lines of defence

> In order to optimize operational risk management, a financial institution should have a sound governance structure that is based on the three lines of defence model.[14]

The three lines of defence model delineate between the roles and responsibilities of the various operational risk management stakeholders. It should be established in light of the financial institution's nature, size, risk profile and operational complexity.

This model should also enable the institution to co-ordinate initiatives to improve its operational risk management practices in regard to more subjective factors, such as its culture and values.

The AMF has already articulated its expectations concerning the roles and responsibilities of the lines of defence in its Governance Guideline. Financial institutions should draw on these concepts and adapt them to their operational risk management context.

2. Operational risk management

> The AMF expects financial institutions to adequately manage operational risk in relation to strategy and risk appetite. Such management should take into account the institution's operational risk exposure inherent to people, processes, systems or external events as well as the exposure of third parties to these risks.

As recommended by the Integrated Risk Management Guideline, the adequate risk management begins with promoting 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 modeled on the extent of operational risk exposure and, accordingly, the commitment required by all levels of the institution to properly manage these risks.

This awareness should also extend to external stakeholders, including material third-party service providers, since outsourcing exposes an institution to operational risks (e.g., cyber-risk exposure). In addition, the culture can be strengthened by providing ongoing training on operational risks to individuals in charge of all business sectors.

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 is inherent in the people, processes, systems and external events of a financial institution and solicits the commitment of those in charge of the financial institution's activities, processes and systems.

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

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

Operational risk management should serve to validate the effectiveness of the 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 the situation, as applicable.

2.1 Identification and assessment of operational risk

> The AMF expects financial institutions to set up taxonomy of operational risks in order to standardize the identification, classification and assessment of these risks and ensure the adequate allocation of duties for mitigating and monitoring them.

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

- risk self-assessment;
- control effectiveness analysis;
- internal and external loss event analysis;
- risk analysis specific to each current product, process and system;
- expert-based scenario analysis;
- exposure quantification modeling.

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 business sectors in order to arrive at a comprehensive assessment of operational risk exposure.

In view of the expectations set forth by the AMF in its *Outsourcing Risk Management Guideline*, the operational risks inherent in all material outsourcing arrangements should be identified and assessed. Moreover, financial institutions should ensure that material third-party service providers are able to provide quality service.

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

2.2 Monitoring and reporting

> The AMF expects operational risk reports to reflect a financial institution's risk tolerance levels. They must also enable the institution to track changes in risk exposure and the effectiveness and efficiency of the measures put in place to manage such risks.

Best practices advocate in favour of setting up a register to record incidents where pre-established operational risk levels are exceeded. An institution should ensure that the procedure for updating the register or any other disclosure mechanism is consistent across all business sectors 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 identify the main sources of unmitigated operational risk. Such reports should include the source, whether internal or external, as well as all potential impacts.[15] They should also incorporate the recommendations made by both the AMF and the audit functions, where applicable, about managing operational risk as well as the corresponding action plans approved by decision-making bodies.

Furthermore, the AMF expects financial institutions to meet the disclosure and transparency expectations set out in the *Governance Guideline* by implementing the necessary mechanisms for promptly advising internal and external stakeholders likely to sustain serious harm due to a major operational incident (cyber incident, system failure, etc.).[16] Such an approach will enable the AMF, as a stakeholder, to be proactive in identifying practices that can undermine operational risk management.

[15] The *Business Continuity Management Guideline* recommends establishing processes for identifying major operational incidents.
[16] Refer to Principle 5 in *G7 Fundamental Elements of Cybersecurity for the Financial Sector*, October 2016.

2.3 Control and mitigation

> The AMF expects internal control mechanisms to efficiently mitigate the financial institution's operational risk exposure inherent to people, processes, systems or external events, according to their importance.

The AMF has indicated in its *Governance Guideline* that control mechanisms should give decision-making bodies reasonable assurance that the objectives relating to the following will be met:

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

The AMF expects these mechanisms to be adaptable to changes in the financial institution's business and in technology. In addition, financial institutions using insurance to transfer operational risk should ensure that it always complements their own control mechanisms for this type of risk.