AUTORITÉ
DES MARCHÉS
FINANCIERS

IMPLEMENTATION FRAMEWORK

Credit unions not members of a federation, trust companies and savings companies wishing to adopt a standardized approach for calculating operational risk capital charges

January 2011

Table of Contents

INTRODUCTION

On Month XX, 2011, the *Autorité des marchés financiers* (the "AMF") published its *Adequacy of Capital Guideline* (the "Guideline") for credit unions not members of a federation, trust companies and savings companies. The Guideline is based on the approach described in Basel II[1] and makes it possible to adapt the minimum capital requirements to the risk profile of each institution.[2] The Guideline contains the requirements pertaining to the simpler approaches under the Basel II framework, that is, the standardized approach to credit risk and the basic indicator approach and standardized approach to operational risk.

Thus, an institution that wishes to implement the standardized approach to operational risk will have to show that it satisfies the requirements for use of this calculation method, as described primarily in chapter 6, as well as in chapters 8 and 9 of the Guideline.[3]

To this end, the AMF is publishing this implementation framework[4] which sets out the principles for governance as well as for "data maintenance"[5] that institutions implementing this approach must apply. These principles will be used to assess the extent to which the institution initially satisfies the requirements of the Guideline and continues to do so. Compliance with these principles will be a significant factor for the AMF in deciding whether or not to authorize an institution to implement the standardized approach to operational risk.

Institutions that implement the basic indicator approach (BIA) and are therefore not subject to the AFM's operational risk assessment process are nevertheless encouraged to adopt the sound practices set out in this document.

---

1 The Guideline incorporates the framework of the Bank for International Settlements (BIS), originally published in June 2004 and revised in November 2005 and in June 2006, which is entitled "*International Convergence of Capital Measurement and Capital Standards"*.

2 In this implementation framework, the generic terms "financial institution" and "institution" refer to all credit unions and companies covered by the scope (chapter 1) of the Guideline.

3 Under the Guideline, all institutions implementing the standardized approach should be able to track and report relevant operational risk data including material losses by significant business line. The AMF understands that the sophistication of this tracking and reporting mechanism should be appropriate for the size of the institution, taking into account its reporting structure as well as its operational risk exposure.

4 In order to ensure harmonization in the application of the new approach proposed by the Basel Committee, the implementation framework follows the example of the implementation notes entitled "Data Maintenance at TSA & AMA Institutions" and "Corporate Governance at TSA & AMA Institutions", published in May 2006 by the Office of the Superintendent of Financial Institutions. Indeed, the financial institutions contemplated in the Guideline must apply standards and sound practices equivalent to those of other institutions that operate in the same markets.

5 The term "data maintenance" incorporates the key components of the data management process, including data collection, data processing, data access and retrieval, and data storage and retention.

1. GOVERNANCE AT INSTITUTIONS IMPLEMENTING THE STANDARDIZED APPROACH TO OPERATIONAL RISK

1.1 Introduction

In 2009, the AMF established two guidelines for financial institutions explicitly informing them of its expectations regarding governance[6] and integrated risk management.[7] The purpose of this section is to provide details on the notion of governance in connection with the use of the standardized approach to operational risk, particularly as regards the powers conferred on the board of directors, senior management, operational risk management functions, reporting and internal audits.

1.2 Governance Principles

An institution's operational risk management framework consists of those policies and practices that govern the identification, measurement, assessment, control, monitoring, and reporting of its operational risk.

An institution must ensure that appropriate controls are in place to ensure adherence to the Guideline's standardized approach requirements.

1.2.1 Board of Directors

The board of directors must be actively involved, as appropriate, in the oversight of the operational risk management framework (paragraph 660 of the Guideline). Thus, the board of directors should:

- have a clear understanding of the institution's operational risk profile, including the internal and external sources of operational risk to the institution;
- examine and approve an appropriate operational risk tolerance level for the institution, which may include a range of qualitative or subjective statements, as appropriate, for the types and/or level of operational risk the institution may take on;
- have a clear understanding of the impact of applying the standardized approach to operational risk;
- review policies for the management of significant operational risk exposures and management practices;
- review operational risk reports, as appropriate;

6 *Autorité des marchés financiers*, Governance Guideline, April 2009.

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

- ensure that the operational risk management and measurement processes and systems are sound and remain effective over time;

- be notified about, and review any material strategic changes that could affect the institution's operational risk profile (e.g.: a merger or acquisition or reliance on outsourcing, etc.).

1.2.2 Senior Management

Senior management should play an active role in the oversight and management of the operational risk management framework. Senior management is accountable to the board of directors for the effective implementation of an operational risk management framework that is appropriate to the institution's risk profile.

In virtue of its responsibilities, senior management should:

- have a clear understanding of the institution's operational risk profile, including the internal and external sources of operational risk to the institution;

- establish an appropriate operational risk tolerance level for the institution, which may include a range of qualitative or subjective statements, as appropriate, for the types and/or level of operational risk the institution may take on;

- have a clear understanding of the impact of applying the standardized approach to operational risk;

- specifically define the hierarchy, resources, responsibilities and reporting requirements to unequivocally ensure accountability for the implementation and management of the operational risk management framework;

- ensure that the operational risk management framework is appropriate to the institution's needs, is consistently applied across the institution and remains effective over time;

- approve the policies, procedures, standards and supporting documentation relating to the operational risk management framework;

- review reports on the status of the institution's operational risk exposures and management activities, including the status of significant operational risk events;

- ensure the operational risk management framework, and adherence to it, is subject to regular independent reviews.

1.2.3 Operational Risk Management Function

Financial institutions that use the standardized approach are expected to have an operational risk management function (ORMF) that is responsible for the institution-wide design and implementation of the institution's operational risk management framework. In this respect, a "function" is defined as a specific organizational unit made up of one or more persons entirely dedicated to operational risk management.[8]

Operational risk management should include the following responsibilities:

- developing strategies to identify, assess, measure, control, mitigate and monitor operational risk;
- establishing and documenting institution-wide policies and procedures relating to the institution's operational risk management framework and management of operational risk exposures, as appropriate;
- establishing means to rigorously track relevant operational risk data, including material losses;
- designing and implementing a risk-reporting system for operational risk;
- ensuring that adequate processes and procedures exist to provide appropriate oversight of the institution's operational risk management practices.

In order to ensure compliance, the institution should have a documented set of internal policies, controls and procedures concerning the operational risk management framework that includes policies for the treatment of non-compliance issues and exceptions. The operational risk management function and business units must be subject to review testing and verification by internal audit (or another independent function) to assess the effectiveness of the internal controls of the operational risk management framework.

1.2.4 Reports

Effective management of operational risk includes regular and timely reporting to the board of directors, senior management and business unit operational management. The nature and scope of reporting should be tailored to the needs of those receiving the report. The frequency and content of internal operational risk reporting should reflect the nature, scope, and complexity of the risk profile of the institution. For example, senior management and the board of directors may require information on trends, levels of exposure and key issues on a regular basis. Conversely, business unit operational management will require detailed information more frequently to effectively manage day-to-day operational risk. Institutions should have practices for taking appropriate action based on the operational risk reporting.

[8] Paragraph 663(a) of the Guideline states that due to the size and complexity of an institution that uses the standardized approach, it may not always be in a position to have a specific organizational unit dedicated to operational risk management. In larger and more complex institutions, the ORMF may be supported by additional independent organizational units having expertise related to specific operational risk exposures, such as outsourcing and business continuity. Section 6.3.1 of the Guideline provides greater detail on the AMF's expectations regarding the standardized approach.

The operational risk reporting should include the following fundamental information:

- operational risk capital charge;
- operational risk data, including material losses by business line;
- results of relevant assessments of business environment factors, risk and control self-assessments or other internal control factors.

1.2.5 Internal Audit[9]

Internal audit (or another independent function) is expected to assess the effectiveness of the institution's internal controls over the operational risk management processes and measurement systems intended to ensure adherence to the standardized approach. The scope and frequency of internal audit reviews should be commensurate with the operational risk within an activity.

Internal audit activities should include, but not be limited to:

- assessing the effectiveness of the institution's internal controls, including their design, intended to ensure adherence to the standardized approach;
- determining the scope and frequency of internal audit activities in a manner consistent with the audit methodology and principles;
- assessing the adequacy of resources and skills required to perform the audit work;
- conducting periodic assessments of the effectiveness of the institution's internal controls over the operational risk management processes on an institution-wide basis. These assessments must include both the activities of the business units and of the operational risk management function.

[9] In accordance with the Guideline, external audit reviews of an institution's operational risk assessment system are not mandated by the AMF.

2. DATA MAINTENANCE BY INSTITUTIONS WISHING TO APPLY THE STANDARDIZED APPROACH TO OPERATIONAL RISK

2.1 Introduction

Institutions applying the standardized approach must ensure that the operational risk data is consistent and provides a sound, reliable and representative basis for management of the institution's operational risk exposure.

This section sets out the key principles of data maintenance for institutions wishing to apply the standardized approach to operational risk. It also provides principles for certain internal operational risk data categories, namely, gross income data and operational loss data.[10]

2.2. Data Maintenance Principles

2.2.1 Senior Management Oversight

An institution wishing to apply the standardized approach to operational risk should adopt processes for managing all key aspects of information technology and data management that are appropriate to the nature, scope and complexity of its data maintenance requirements. It should assess the scope, plans and risks associated with timely execution of data maintenance projects, if any.

In this context, the responsibilities of senior management should include, but not be limited to:

- reviewing and approving organizational structure and functions to facilitate development of appropriate data architecture to support implementation of the standardized approach;

- establishing an institution-wide data management framework defining, where appropriate, the institution's policies, governance, technology, standards and processes to support data collection, data maintenance, data controls and distribution of processed data, i.e., information;

- ensuring data maintenance processes provide security, integrity and auditability of the data from its collection through to its archiving or logical destruction;

- instituting internal audit programs, as appropriate, to provide for periodic independent assessment of data maintenance processes and functions;

- ensuring that policies, procedures and allocation of responsibilities are in place to allow for appropriate institution-wide monitoring of the application of the data management framework, including ongoing updates to procedures and documentation, as necessary.

[10] This section does not provide principles for using the data elements in the quantification of operational risk capital.

2.2.2 Data Collection

Within the scope of the Guideline, “data collection” (also referred to as “data acquisition” and “data input”) generally consists in determining the required data elements from among various internal and external source systems and then validating, extracting and transmitting the data to the appropriate operational databases or data repositories.

Data collection for operational risk typically involves identifying the appropriate data elements pertinent to the management of operational risk.

An institution’s data collection processes should:

- establish clear and comprehensive documentation for data definition, collection and aggregation, including data mapping to business lines,[11] data schematics where necessary, and other identifiers, if any;

- establish standards for data accuracy, completeness, timeliness and reliability;

- identify and document data gaps and, where applicable, document the manual or automated workarounds used to close data gaps and meet data requirements;

- establish standards, policies and procedures for the cleansing of data through reconciliation, field validation, reformatting, decomposing or use of consistent standards, as appropriate;

- establish procedures for identifying and reporting on data errors and data linkage breaks to downstream and/or external source systems.

2.2.3 Data Processing

The “data processing” component covers a wide range of data management tasks, including data conversion through multiple automated or manual processes, transmissions, source or network authentication, validation, reconciliation, etc.

An institution’s data processing should:

- limit reliance on workarounds and manual data manipulation in order to mitigate the operational risk related to human error and dilution of data integrity;

- ensure appropriate levels of validation, data cleansing and reconciliation for each process, as applicable;

- establish adequate controls to ensure processing by authorized staff acting within designated roles and established authorities;

[11] Business lines are described in Annex 6-1 of the Guideline.

- institute appropriate change control procedures for changes to the processing environment, including, where applicable, change initiation, authorization, program modifications, testing, parallel processing, sign-offs, release and library controls;

- provide appropriate levels of disaster back-up and recovery capabilities to mitigate loss of data or data integrity.[12]

2.2.4 Data Access and Retrieval

From the AMF's supervisory perspective, a key component of data maintenance is the continued availability of an institution's data and information.

A financial institution should ensure that:

- databases and extract, query and retrieval subroutines are designed to meet the institution's own data requirements as well as its ongoing needs for supervisory assessments of various data, as appropriate;

- access controls and data and information distribution are based on user roles and responsibilities and industry sound practices in the context of effective segregation of duties, and are in compliance with the "need to know" principle, all of which is assessed by the institutions' internal compliance and audit functions;

- access to data or information is not restricted by any outsourcing arrangement[13] where data maintenance is outsourced to one or more external service providers. Notwithstanding these arrangements, an institution should be able to provide data or information to the AMF at no additional cost.

2.2.5 Data Storage and Retention

The data "storage and retention" component addresses the dual expectations of electronic data retention and archiving to meet the minimum historical retention criteria established under the Guideline, as well as the requirements of the institution itself.

An institution should:

- establish documented policies and procedures regarding storage, retention and archiving, including, where applicable, the procedures for logical and physical deletion of data and destruction of data storage media and peripherals;

- maintain back-ups of relevant data banks, databases and data files in a manner that can facilitate readily available information to meet information calls with respect to the ongoing supervisory assessment of compliance with standardized approach requirements;

[12] *Autorité des marchés financiers*, Business Continuity Management Guideline, April 2010.

[13] For more information on outsourcing, refer to the Outsourcing Risk Guideline published by the AMF in April 2009.

- ensure that the electronic versions of all relevant data and information are in a machine-readable format and can be made accessible.

2.3. Operational Risk Data Categories

Operational risk capital measurement is highly dependent on an institution's ability to maintain reliable operational risk data files for various operational risk data categories. These categories include gross income data, operational loss data and other qualitative data representing business environment and internal control factors.

As per paragraph 654 of the Guideline, an institution that applies the standardized approach is required to calculate its capital based on three years of gross income. In addition, for effective operational risk management, the institution is required to track and report its material losses.

In addition to the key data maintenance principles outlined earlier, specific principles for the standardized approach operational risk data categories have been set out below.

2.3.1 Gross Income Data

As per paragraph 653 of the Guideline, an institution that applies the standardized approach is required to use gross income to determine the operational risk capital charge. To maintain reliable gross income data for the calculation of the capital charge, and in accordance with the Guideline requirements relating to gross income, an institution should:

- document the mapping process to provide for the consistent mapping of gross income data;

- establish a system or process that facilitates the reconciliation of gross income reported in the disclosure form to the institution's reported financial results;

- ensure that the robustness of the system is commensurate with the complexity of the gross income data mapping process.

2.3.2 Operational Loss Data

All institutions applying the standardized approach must be able to track their material internal losses and related data elements by business line. The AMF recognizes that the industry practices for collecting internal operational loss data are emerging. It is expected that tracking systems will vary across institutions applying the standardized approach. As outlined in the Guideline, the sophistication of an institution's tracking system should appropriately reflect the size, reporting structure and the operational risk exposure of the institution.

Accordingly, an institution's tracking system will be assessed against its ability to capture its material operational losses on an institution-wide basis.

Those assigned to the processing of internal loss data (and its related data elements) should:

- ensure that the maintenance of internal loss data aligns with the established institution-wide data management framework;[14]
- determine and document the scope of internal loss data to be collected according to its operational risk management needs;
- establish and document the process for mapping internal loss data to business lines,
- develop and document standards to ensure a consistent process for the collection of internal loss data;
- incorporate internal loss data in its operational risk reporting to effectively support the ongoing management of operational risk;
- ensure periodic independent reviews of the processes involved in the collection of loss data.

[14] In accordance with the responsibilities of senior management.