Implementation Note

Subject: Corporate Governance at TSA & AMA Institutions

Category: Capital

No: A & A-1 Date: May 2006

I. Introduction

The purpose of this implementation note is to provide guidelines and practices for Corporate Governance at institutions[1] implementing the Standardized Approach (TSA) or the Advanced Measurement Approach (AMA) for operational risk. It expands on the minimum criteria set out in Chapter 6 of the Draft Capital Adequacy Requirements ("CAR") Guideline A and Chapter 7 of the Draft Capital Adequacy Requirements ("CAR") Guideline A-1.

Institutions that are implementing the Basic Indicator Approach (BIA), and are therefore not subject to OSFI's Operational Risk Assessment Process[2], are encouraged to adopt the key practices set out in this implementation note as appropriate.

This implementation note sets out principle-based requirements and expectations of the Board of Directors, Senior Management, Operational Risk Management Function, Reporting, and Internal Audit in the context of corporate governance for TSA and AMA institutions.

[1] Banks and bank holding companies to which the *Bank Act* applies and federally regulated trust or loan companies to which the *Trust and Loan Companies Act* applies are collectively referred to as "institutions".

[2] OSFI Implementation Note, "Operational Risk Assessment Process for TSA and AMA Institutions", September 2005.

Table of Contents

II. Background

As part of OSFI's Operational Risk Assessment Process[3], institutions are expected to meet the CAR requirements relevant to the operational risk approach being implemented, i.e., TSA or AMA. Further, on an ongoing basis, institutions will need to demonstrate to OSFI that their corporate governance[4], and risk management and control practices related to operational risk are commensurate with the nature, scope, complexity and risk profile of the institution.

The guidance outlined in this document is consistent with OSFI's assessment of the effectiveness of an institution's corporate governance and risk management and control practices as described in OSFI's *Supervisory Framework*, dated 1999, and *Corporate Governance Guideline*, dated January 2003. OSFI will use its reliance-based supervisory approach for assessing the appropriateness and effectiveness of operational risk management and control practices at TSA and AMA institutions, and for assessing their ongoing adherence to minimum requirements.

III. Guidelines & Practices

An institution's operational risk management framework consists of those policies and practices that govern the identification, measurement/assessment, control and monitoring, and reporting of its operational risk. It includes the oversight responsibilities of Senior Management and the Board, and others who have been delegated oversight responsibility relative to operational risk.

An institution must ensure that appropriate controls are in place to ensure ongoing adherence to all applicable CAR requirements relative to TSA or AMA, as appropriate.

1. Board of Directors

The Board of Directors ("Board") must be actively involved, as appropriate, in the oversight of the operational risk management framework (paragraph 660). Accordingly, the Board 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 tolerance or appetite, which may include a range of qualitative and/or subjective statements, as appropriate, for the types and/or level of operational risk the institution may take on,

[3] OSFI Implementation Note, "Operational Risk Assessment Process for TSA and AMA Institutions", December 2005

[4] OSFI's *Corporate Governance Guideline* describes corporate governance as the 'oversight mechanisms', including the processes, structures and information used for directing and overseeing the management of a company. In the *Supervisory Framework*, OSFI describes the role of six "Risk Management Control Functions" that may exist in an institution to provide independent oversight of the institution's operations. These include the Board of Directors, Senior Management, and Internal Audit. Reference to these independent oversight functions in this implementation note will be made in the context of the roles described in the Supervisory Framework.

- Have a clear understanding of the impact of applying the operational risk approach at the institution (i.e. TSA or AMA),
- Review policies for the management of significant operational risk exposures and management practices[5],
- Review operational risk reports, as appropriate, as noted in Section 4 below,
- Satisfy itself that the operational risk management and measurement processes and systems[6] are sound and remain effective over time, and
- Be notified and review any material strategic changes to the institution's operational risk profile. For example, following a merger or acquisition or off shoring of back-office services.

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 for the effective implementation of an operational risk management framework that is appropriate to the institution's risk profile.

Senior Management accountabilities include:

- Having a clear understanding of the institution's operational risk profile, including the internal and external sources of operational risk to the institution,
- Establishing an appropriate tolerance or appetite, which may include a range of qualitative and/or subjective statements, as appropriate, for the types and/or level of operational risk the institution may take on,
- Having a clear understanding of the impact of applying the operational risk approach at the institution (i.e. TSA or AMA),
- Establishing specific authority, resource, responsibility and reporting to ensure accountabilities for implementation and management of the operational risk management framework,
- Overseeing that the operational risk management framework is appropriate to the circumstances of the institution, and is consistently applied across the institution as appropriate and remains effective over time,
- Approving the policies, procedures, standards and supporting documentation relating to the operational risk management framework,

[5] Annex 8, paragraph (h), of the CAR guideline, states that an institution's business line mapping policy should be subject to Board approval. OSFI, however, recognizes that business line mapping is an operational activity and may not constitute the type of information typically approved by the Board. In this case, Senior Management approval of the business line mapping policy may be appropriate.

[6] As per paragraph 663(a) of the CAR guideline, the term "system" does not necessarily refer to a technology application for managing operational risks, but refers to the collective policies and processes in place for identifying, assessing, monitoring and controlling operational risk across the institution.

- Reviewing reports on the status of the institution's operational risk exposures and management activities, including the status of significant operational risk events, and
- Ensuring the operational risk management framework, and adherence to it, is subject to regular independent reviews.

Senior Management of AMA institutions is expected to follow certain additional requirements. Senior Management should:

- Clearly understand the measurement systems and processes affecting the operational risk management framework and its impact on operational risk capital,
- Be satisfied that the measurement systems and processes include the key elements, including the use of internal data, relevant external data, scenario analysis and factors reflecting the business environment and internal control systems,
- Satisfy itself and assure the Board that the operational risk management framework and measurement systems are conceptually sound and meet the use test, such that the system is closely integrated with the institution's day-to-day risk management processes, and
- Be aware of emerging industry operational risk measurement and management practices.

3. Operational Risk Management Function

TSA and AMA institutions are expected to have an operational risk management function (ORMF) that is responsible for the enterprise-level design and implementation of the bank's operational risk management framework. In this respect, a function is defined as a specific organizational unit made up of one or more persons dedicated to operational risk management. However, paragraph 663(a) of the CAR guideline recognizes that the size and complexity of TSA institutions may not warrant the existence of a specific organizational unit dedicated to operational risk management[7]. 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.

The operational risk management responsibilities include:

- Developing strategies to identify, assess/measure, monitor and control/mitigate operational risk,
- Establishing and documenting firm-wide policies and procedures relating to the bank's operational risk management framework and management of operational risk exposures, as appropriate,
- Ensuring that there is a means to systematically track relevant operational risk data, including material losses,
- Designing and implementing a risk-reporting system for operational risk, and

[7] Institutions should refer to section 7.3.1 of the CAR Guideline A-1 and section 6.3.1 of the CAR Guideline A for clarification of OSFI's expectations in this regard.

- 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 functions and business units must be subject to review testing and verification by internal audit (or an equally independent function) to assess the overall effectiveness of their internal controls for its adherence to the operational risk management framework.

In line with paragraph 666(a) of the CAR Guideline, an ORMF at AMA institutions must be functionally independent. An AMA ORMF should be able to demonstrate that it can provide independent and objective assessments to the Board and Senior Management on the institution's operational risk exposures and the effectiveness of operational risk management practices. Therefore, in addition to the above, AMA ORMFs responsibilities should include:

- Designing and implementing the firm's operational risk measurement methodology,
- Ensuring that the operational risk measurement processes are closely integrated into the risk management processes of the institution, and
- Defining the roles of model development and validation, ensuring there is separation between the two roles.

4. Reporting

Effective management of operational risk includes regular and timely reporting to the Board, Senior Management and business unit management. The nature and scope of reporting should be appropriate to the needs of the audience receiving the report. The frequency and content of internal operational risk reporting should be reflective of the nature, scope, and complexity of the risk profile of the institution. For example, Senior Management and the Board may require information such as trends, levels of exposure and key issues on a regular basis. Conversely, 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.

The operational risk reporting should include the following fundamental information:

- Operational risk capital charge, as appropriate,
- Relevant operational risk data including material losses by business line, and
- Results of relevant assessments of business environment factors, risk and control self-assessments or other internal control factors.

5. Internal Audit[8]

Internal Audit (or an equally 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 TSA or AMA requirements. 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 the design elements of internal controls, intended to ensure adherence to TSA or AMA requirements,
- Determining scope and frequency of Internal Audit activities in a manner consistent with its audit methodology and principles,
- Assessing the adequacy of resources and skills required to perform this audit work, and
- 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.

In addition to the above, Internal Audit at AMA institutions should include the following activities:

- Assessing the effectiveness of the institution's internal controls over the operational risk models and risk measurement systems of the operational risk management framework, including data integrity and validation processes.

[8] As per the CAR guideline, external audit reviews of an institution's operational risk assessment system are not mandated by OSFI.