Office of the Superintendent
of Financial Institutions Canada

255 Albert Street
Ottawa, Canada
K1A 0H2

Bureau du surintendant
des institutions financières Canada

255, rue Albert
Ottawa, Canada
K1A 0H2

www.osfi-bsif.gc.ca

Guideline

Subject: **Legislative Compliance Management (LCM)**

Category: **Sound Business & Financial Practices**

No: E-13 **Date: March 2003**

Introduction and Purpose

This Guideline replaces the Interim Guideline issued in May 2000. It conveys OSFI's expectations of federally regulated financial institutions (FRFIs)[1] regarding controls through which they manage regulatory risk inherent in their activities worldwide.

Regulatory risk is the risk of non-compliance with applicable regulatory requirements. For the purpose of this Guideline, applicable regulatory requirements include those in (a) the FRFI's governing federal legislation (i.e., *Bank Act, Cooperative Credit Associations Act, Trust and Loan Companies Act*, and *Insurance Companies Act)*, regulations and regulatory directives (referred to collectively as "Governing Legislation") and, since non-compliance by a FRFI or subsidiary with regulatory requirements applicable to its activities may have a critical impact on the FRFI's reputation and/or safety and soundness, regulatory requirements also include those in (b) other legislation, regulations and regulatory directives applicable to activities of the FRFI or its subsidiaries worldwide (referred to collectively as "Other Legislation").

The term "Legislative Compliance Management" (LCM) in this Guideline refers to the set of key controls through which a FRFI manages regulatory risk.

OSFI considers effective LCM to be essential to a FRFI's well being. An effective LCM process will provide a means by which the institution satisfies itself that it is in compliance with Governing Legislation and Other Legislation.

[1] FRFIs include banks; cooperative credit associations; trust and loan companies; life insurance companies; property and casualty insurance companies; fraternal benefit societies; bank and insurance holding companies; and authorized foreign banks and foreign insurance companies (life, property and casualty) including foreign fraternal benefit societies in respect of their business in Canada (Branches). FRFIs operating as Branches in Canada should read references in this document to the "Board of Directors" as references to their Principal Officer or Chief Agent, as applicable.

Demonstrated effective management of compliance with applicable requirements of governing federal financial institutions legislation also provides OSFI with reasonable assurance upon which to base the Superintendent's annual statutory report to the Minister of Finance on FRFIs' compliance with their governing statutes.

OSFI's key expectation in respect of LCM, which underlies the guidance in this document, is that FRFIs will establish and maintain an enterprise-wide framework of regulatory risk management controls, and that these controls include oversight by functions (groups or individuals) that are independent[2] of the activities they oversee. OSFI expects each FRFI to take an approach to regulatory risk management that suits its circumstances, having regard to its size, complexity, geographical location(s), nature of business, structure and ownership. Accordingly, references in this Guideline to oversight functions are not intended to prescribe legal constructs or organizational models.

[2] OSFI recognizes that in smaller FRFIs, one person may have more than one set of oversight responsibilities.

Table of Contents

Supervisory Framework

One of OSFI's statutory objects is to determine whether a FRFI is in sound financial condition. As outlined in the *Supervisory Framework*, OSFI applies a risk-based approach to assessing a FRFI's safety and soundness on a consolidated basis. Resources are focused on areas of higher risk and information from other regulators is used as appropriate. For each activity that OSFI identifies as significant[3], OSFI assesses the level of risk, including regulatory risk, and considers the impact of risk mitigation by evaluating the quality of risk management. Institutions that are well managed relative to their risks will require less supervision.

OSFI expects there to be two levels of control in the management of risk, including regulatory risk: 1) day-to-day controls, for which business operations management is responsible, that include policies, procedures, processes and appropriate staffing in all business operations; and 2) independent oversight, which is provided by risk management control functions (RMCFs) and ensures that risks are being managed effectively.

LCM Framework

OSFI expects LCM to provide a control framework for the mitigation of regulatory risk in a FRFI. This framework should include an enterprise-wide definition of regulatory risk. It should outline the process through which it is to be identified and assessed, and outline the key controls through which it is to be managed/mitigated throughout the FRFI and its subsidiaries.

The LCM framework should include both day-to-day and independent oversight levels of control. The respective oversight roles and responsibilities of RMCFs should be defined and communicated clearly. The board of directors (board), senior management, compliance and internal audit or other independent review function, however constituted, are important RMCFs in effective LCM.

OSFI expects the LCM framework to include the following key controls: identification, assessment, communication and maintenance of applicable regulatory requirements; day-to-day compliance and oversight procedures that include monitoring and reporting procedures through which significant problems are identified, escalated and resolved; internal audit or other independent validation of the effectiveness of and adherence to the LCM framework and key controls; compliance oversight and internal audit or other independent review function reports to the board; adequate documentation; and control updates to address changes in products, activities or corporate structure. Lines of responsibility should be clear and control methodology should include a mechanism for holding individuals accountable.

[3] "Significant" as used by OSFI in "Significant Activities" is defined in the *Supervisory Framework*. Qualitative and quantitative factors are used to assess the significance of an activity to the achievement of the institution's business objectives and strategies.

The key controls are more fully discussed below.

OSFI expects that the exact approach chosen by a FRFI for LCM will depend on a range of factors including its size, complexity, geographical location(s), nature of business, structure and ownership. Regardless of where LCM responsibilities reside in a FRFI, or how they are constructed, OSFI will focus on the effectiveness of regulatory risk management, that is, its control effect or outcome, rather than its form.

Key LCM Controls

Key LCM controls are the basic elements of a sound risk control framework. At a minimum, OSFI expects key LCM controls to include the following, administered through a methodology that establishes clear lines of responsibility and a mechanism for holding individuals accountable:

Identification, Assessment, Communication and Maintenance of Applicable Regulatory Requirements

In this Guideline, a regulatory requirement is a provision in Governing Legislation or Other Legislation that requires the FRFI or subsidiary to do (or prohibits it from doing) certain things or to act or conduct its affairs in a particular manner. The methodology for identifying, assessing, communicating and maintaining knowledge of applicable regulatory requirements should ensure that appropriate individuals have the information they need to manage regulatory risk effectively. The information should be current and accurate, and reflect new and changing requirements as well as those applicable to new and changing products, activities and corporate structure.

Compliance Procedures

Appropriate procedures for complying with regulatory requirements applicable to activities of the FRFI and its subsidiaries on a day-to-day basis should be incorporated into and maintained in relevant business operations. These should, like compliance oversight procedures, include monitoring and reporting procedures.

Monitoring Procedures

Procedures should exist for regularly monitoring adherence to controls established in business operations, evaluating the effectiveness of the controls and the LCM framework, and monitoring material exposures to regulatory risk. Monitoring methodology should include verification of key elements of pertinent information that is to be reported up through those having day-to-day compliance responsibilities to senior management and to the board, and it should extend to significant remediation activities.

Reporting Procedures

Procedures should exist to ensure that sufficient pertinent and timely information about regulatory risk management effectiveness is communicated to senior management and to the board. Reports should include significant results of monitoring, and findings of compliance oversight and internal audit or other independent review function. Content and frequency of normal course reports should be approved by the chief compliance officer (CCO) (more fully discussed below), and should be sufficient to enable the CCO, senior management and the board to discharge their LCM responsibilities.

Strong reporting procedures often include regular formal and informal meetings and other communications within and between functions and management groups throughout a FRFI enterprise, in addition to formal documentation.

Compliance Oversight Function Reports to the Board of Directors

OSFI expects the CCO to report material compliance issues to the board on a timely basis. Normal course reports should be made on a regular basis that is approved by the board, but no less frequently than annually. These should cover material results of enterprise-wide compliance oversight. At a minimum, they should provide information about material LCM framework weaknesses, instances of non-compliance and related remedial action plans, and material exposures to regulatory risk.

Information about significant legislative and regulatory developments, industry compliance issues, emerging trends and regulatory risks should also be considered for inclusion, as it may assist the board in its decision making about strategic direction and controls.

Internal Audit or other Independent Review Function Reports to the Board

Reports to the board by internal audit or other independent review function should include the scope and results of LCM-related reviews and significant recommendations for correcting deficiencies along with management's undertakings with respect to remedial action where appropriate.

Like CCO reports to the board, independent review function reports should contain sufficient pertinent information to facilitate the board's periodic reassessment of the LCM framework. The reports should be provided on a rotational or other regular basis that the board considers appropriate.

Documentation

OSFI expects day-to-day and independent oversight levels of a compliance function to produce adequate documentation to demonstrate how regulatory risk is managed, to support the flow of reports up to senior management and the board, and to support the board's periodic reassessment of the LCM framework.

Regular Review and Improvement

OSFI expects key LCM controls and methodology to be reviewed and updated regularly, in order to address new and changing regulatory risks, products, activities and corporate structure.

Role of Board of Directors

OSFI expects the board, the FRFI's highest level of independent oversight of management and operations, to approve the FRFI's LCM framework and see that it is established and maintained; to obtain sufficient appropriately aggregated information to address issues that are material to the FRFI; and, to this end, establish thresholds for the type, content and frequency of reports that it should receive; to monitor remediation progress in respect of material problems; and to periodically reassess the effectiveness of the LCM framework.

OSFI also expects the board to see that the LCM framework is subject to internal audit or other independent review and validation on a rotational or other regular basis that the board considers appropriate; that material findings and recommendations are brought to the board's attention; and that material recommendations are acted upon.

Role of Senior Management

OSFI expects senior management to implement the LCM framework approved by the board. The LCM framework should be implemented throughout the FRFI in a manner that is tailored to the needs of each area. Senior management should ensure that appropriate policies and procedures are developed and applied effectively by appropriately qualified individuals, and all staff should understand their responsibilities for complying with such policies and procedures.

OSFI also expects senior management to ensure that significant recommendations concerning issues of non-compliance or control improvements made by compliance oversight and/or internal audit or other independent review function in the FRFI, are acted upon in a timely fashion.

Role of Compliance Oversight Function

OSFI expects a compliance oversight function to ensure that key day-to-day LCM controls throughout the enterprise are sufficiently robust to control compliance with Governing Legislation and Other Legislation and, where significant issues arise, escalate them to senior management and the board as appropriate. The function should be independent of the activities it oversees and capable of providing the board with the information it needs to obtain an enterprise-wide perspective on compliance issues.

Overall responsibility for the compliance oversight function should be assigned to a member of senior management who should be designated, at least functionally, as the FRFI's CCO. OSFI recognizes that the CCO may have other responsibilities as well, especially in smaller FRFIs.

The CCO should have sufficient stature and authority in the organization, as well as the necessary mandate, resources and access to the chief executive officer and the board, to achieve an appropriate control outcome. OSFI considers that appropriate skills and a good knowledge of the business and regulatory environments are essential to the effectiveness of the CCO and all others who have compliance oversight responsibility.

Role of Internal Audit or Other Independent Review Function

OSFI expects an internal audit or other review function to validate the effectiveness of and adherence to the LCM Framework throughout the enterprise by risk-based testing on a rotational or other regular basis that the board considers appropriate. Furthermore, the scope of work undertaken routinely by this function should include consideration of material regulatory risks and their corresponding controls. The review function should be independent of the activities it reviews, have appropriate skills and a good knowledge of the business and regulatory environments. Significant review findings and recommendations should be reported as appropriate to business operations management, senior management and the board. Actions taken in response to significant recommendations should be monitored.

- END -