Guideline

Title	Regulatory Compliance Management (RCM) – Guideline (2014)
Category	Sound Business and Financial Practices
Date	November 30, 2014
Sector	Banks Foreign Bank Branches Foreign Insurance Branches Life Insurance and Fraternal Companies Property and Casualty Companies Trust and Loan Companies
No	E-13

Table of Contents

I. Purpose and Scope of the Guideline

II. Definitions

- (i) Regulatory Compliance Management (RCM)
- (ii) Regulatory Compliance Risk
- (iii) RCM Framework

III. RCM Framework – Overview

IV. RCM Framework

- (i) Role of the CCO
- (ii) Procedures for Identifying, Risk Assessing, Communicating, Managing and Mitigating Regulatory Compliance Risk and Maintaining Knowledge of Applicable Regulatory Requirements
- (iii) Day-to-Day Compliance Procedures
- (iv) Independent Monitoring and Testing Procedures
- (v) Internal Reporting

- (vi) Role of Internal Audit or Other Independent Review Function
- (vii) Adequate Documentation
- (viii) Role of Senior Management

V. OSFI's Supervisory Assessment

(formerly Legislative Compliance Management (LCM))

I. Purpose and Scope of the Guideline

The purpose of the RCM guideline is to communicate OSFI's expectations with respect to the management of regulatory compliance risk by federally regulated financial institutions (FRFIs)[1].

This guideline revises and replaces the 2003 LCM Guideline to better align it with guidance provided by more recently updated OSFI Guidelines[2].

The guideline also elaborates on a number of principles regarding key controls as part of RCM.

> OSFI recognizes that FRFIs may have different RCM practices depending on a variety of factors, including their: size; ownership structure; nature, scope and complexity of operations; corporate strategy; risk profile; and geographical locations.

II. Definitions

(i) Regulatory Compliance Management (RCM)

The term "Regulatory Compliance Management" (RCM) in this guideline refers to the set of key controls through which a FRFI manages regulatory compliance risk.

(ii) Regulatory Compliance Risk

For the purposes of this guideline, regulatory compliance risk is the risk of a FRFI's potential non-conformance with laws, rules, regulations and prescribed practices ("regulatory requirements") in any jurisdiction in which it operates. It does not include risk arising from non-conformance with ethical standards. Regulatory requirements are applicable to the FRFI or a subsidiary worldwide that require the FRFI or subsidiary to do (or prohibit it from doing) certain things or to act or conduct its affairs in a particular manner.

(iii) RCM Framework

A RCM framework refers to the structures, processes and other key control elements through which a FRFI and its subsidiaries manage and mitigate regulatory compliance risk inherent in their activities enterprise-wide[3].

III. RCM Framework – Overview

OSFI considers an effective RCM framework to be an essential component of an overall risk management program that provides the means by which a FRFI satisfies itself it is in compliance with applicable regulatory requirements. Non-compliance with applicable regulatory requirements can have significant negative effects on a FRFI's reputation and/or safety and soundness and may lead to increased regulatory intervention.

The RCM framework should enable a FRFI to apply a risk-based approach for identifying, risk-assessing, communicating, managing and mitigating regulatory compliance risk. The framework should also include a definition of regulatory compliance risk appropriate for the FRFI.

Overall responsibility for assessment and management of regulatory compliance risk within the FRFI should be assigned to an individual who is independent from operational management, has sufficient stature, authority, resources and support within the FRFI to influence the FRFI's activities, and who should be designated, at least functionally, as the FRFI's Chief Compliance Officer (CCO) or equivalent. Although most FRFIs will have a dedicated CCO position, OSFI recognizes that this individual may have other responsibilities as well, especially in the case of small, less complex FRFIs.

Staff assigned to compliance responsibilities, including the CCO, should have the appropriate skills and knowledge of the business and regulatory environments that are essential to effective RCM.

See further, Role of CCO, below.

OSFI assesses the quality of RCM at the following levels of control:

- operational management[4] for a given business activity which is primarily responsible for the controls used to manage the regulatory compliance risks within the activity on a day-to-day basis; and
- independent, enterprise-wide oversight of operational management by oversight functions[5][6].

OSFI expects the RCM framework to be reviewed and updated regularly, at least annually, to address: any need for improvement, new and changing regulatory compliance risk, new business activities and any changes to corporate structure. The review methodology should include a mechanism that holds individuals or areas accountable for their assigned duties or functions.

OSFI will administer its RCM supervisory program in a manner appropriate to the circumstances of each FRFI. Each FRFI, regardless of the size, is expected to have risk management controls that are proportionate to its identified risks.

IV. RCM Framework

Key controls, including oversight functions, are the basic elements of a sound RCM framework. At a minimum, OSFI expects the RCM framework to include the following, administered through a methodology that establishes clear lines of responsibility and a mechanism for holding individuals accountable: (i) role of the CCO; (ii) procedures for identifying, risk assessing, communicating, effectively managing and mitigating regulatory compliance risk and maintaining knowledge of applicable regulatory requirements; (iii) day-to-day compliance procedures; (iv) independent monitoring and testing procedures; (v) internal reporting; (vi) role of Internal Audit or other independent review function; (vii) adequate documentation; and (viii) role of Senior Management[7]. Each of these items is described in further detail below.

OSFI expects FRFIs to establish and maintain an effective enterprise-wide RCM framework. RCM controls should include oversight by individuals or oversight functions that are independent of the activities they oversee.

(i) Role of the CCO

The CCO should be responsible for assessing the adequacy of, adherence to and effectiveness of the FRFI's day-to-day controls, and for opining on whether, based on the independent monitoring and testing conducted, the RCM controls are sufficiently robust to achieve compliance with the applicable regulatory requirements enterprise-wide.

The CCO should have a clearly defined and documented mandate, unfettered access, and for functional purposes, a direct reporting line to the Board, or Branch Management.

See further, Compliance Reports to Senior Management, below.

Where an institution lacks a particular oversight function, or such oversight function is not sufficiently independent or does not have enterprise-wide responsibility, OSFI expects other functions, within or external to the FRFI, to provide an appropriate level of independent oversight.

(ii) Procedures for Identifying, Risk Assessing, Communicating, Managing and Mitigating Regulatory Compliance Risk and Maintaining Knowledge of Applicable Regulatory Requirements

Reasonable[8] procedures should exist to assure that appropriate individuals are provided with current and accurate information needed to identify, assess, communicate, manage and mitigate regulatory compliance risk, and maintain knowledge of applicable regulatory requirements. The procedures should enable a FRFI to take a risk-based approach to managing regulatory compliance risk so that appropriate resources are allocated to higher risk areas. The information provided should be updated, as necessary, to reflect new and changing regulatory requirements. In addition, such procedures should assure that information is updated when changes with respect to products, services, strategic plans, other activities and corporate structure are made.

(iii) Day-to-Day Compliance Procedures

Appropriate procedures should exist in operational management[9] to reasonably assure that a FRFI is complying on a day-to-day basis with the regulatory requirements applicable to the activities of the FRFI. Such procedures should be tailored to the business activities. They should be incorporated into, and maintained in, relevant business operations. The procedures should also include a monitoring and testing component using a risk-based approach to reasonably assure the adequacy of, adherence to, and effectiveness of such procedures in business operations.

(iv) Independent Monitoring and Testing Procedures

The adequacy of, adherence to, and effectiveness of day-to-day compliance procedures should be independently[10] overseen by the CCO[11], using a risk-based approach. Where appropriate in the circumstances of the FRFI, independent monitoring and testing[12], wherever it is conducted within the FRFI, should be sufficiently consistent enterprise-wide to enable the aggregation of information to identify any patterns, themes or trending in compliance controls that may indicate weaknesses. Compliance control processes should include verification of key information (including significant remediation activities) used in compliance reporting.

The adequacy of, adherence to and effectiveness of compliance oversight should be validated by Internal Audit or other independent review function[13]. Such validation should be on a rotational or other regular basis, and should be undertaken using a risk-based approach. This includes testing of both operational and independent oversight levels of compliance controls. Such review function should be independent of the activities it reviews, have appropriate skills and a good knowledge of the business and regulatory environments.

(v) Internal Reporting

1. **Reporting Procedures**: Reasonable procedures should exist to provide assurance that sufficient pertinent and verifiable information about the adequacy of, adherence to and effectiveness of RCM is communicated on a timely basis to Senior Management, and other individuals with RCM responsibilities as determined by Senior Management within the FRFI. Reporting procedures should include the aggregation of monitoring and testing results within and across areas of business activity pertinent to the RCM responsibilities of the report

recipients.

In addition to formal documentation, reporting procedures often include regular formal and informal meetings and other communications within and among management groups and oversight functions.

See further, Role of Senior Management, below.

2. **Compliance Reports to Senior Management**: Regular reports to Senior Management should be in a manner and formats that allow them to clearly understand the regulatory risks to which the FRFI is exposed, and the adequacy of key controls to manage those risks and facilitate the performance of their oversight responsibilities. Normal course RCM reports should be made on a regular basis[14].

   The CCO should establish the general areas of content addressed in, and frequency of, regular RCM reports made to the CCO by operational management. Content and frequency should be sufficient to enable the CCO and Senior Management to discharge their RCM responsibilities.

   Examples of content that reports should cover include: results of enterprise-wide compliance oversight, material[15] RCM framework weaknesses, instances of material non-compliance, material exposures to regulatory risk (and their potential direct or indirect impact on the FRFI), related remedial action plans, information about significant legislative and regulatory developments, industry compliance issues, emerging trends and regulatory risks.

   > OSFI expects the CCO to report regularly all material information derived from the independent monitoring and testing to assist Senior Management in overseeing the RCM framework and enterprise-wide state of compliance.

   The CCO should have reasonable processes in place to assess the accuracy and effectiveness of RCM information or analysis provided by operational management. Reports should provide an objective view on whether the FRFI is operating within the RCM framework and identify problems or issues for Senior Management.

The CCO should also opine on a regular basis, but at least annually, on the adequacy of, adherence to and effectiveness of the day-to-day controls, and whether, based on the independent monitoring and testing conducted within the FRFI, the FRFI is in compliance with applicable regulatory requirements enterprise-wide. This should be supported by sufficient pertinent information that is verified or reasonably verifiable.

See further, Role of CCO, above.

> OSFI expects the CCO to report, on a timely basis, material instances of non-compliance, compliance issues and any measures Senior Management is taking to remediate issues or implement new or revised controls.

3. **Internal Audit or Other Independent Review Function Reports**: The Internal Audit or other independent review function should report significant review findings along with management's undertakings with respect to remedial action. Reports should include the scope and results of RCM-related audits, including assessing the work of compliance oversight, together with management's response and remedial action plans, as appropriate. Such reports should also provide assistance in assessing the reliability of any RCM assurances provided.

(vi) Role of Internal Audit or Other Independent Review Function

The activities carried out by the CCO should be subject to periodic review by Internal Audit or other independent review function. The scope of work should consider the reliability of the RCM framework, which includes management's identification of material regulatory compliance risks and their corresponding controls, the accuracy of reporting on compliance, and an assessment of the effectiveness of the compliance oversight. Internal audit methodologies need to be supplemented by effective challenge and an attitude of "professional skepticism" by internal auditors[16].

Review findings that are considered significant should be reported, as appropriate, to operational management, the CCO and Senior Management. Actions taken by operational management in response to significant review findings should be monitored as appropriate by Senior Management.

(vii) Adequate Documentation

OSFI expects the roles and responsibilities of all individuals involved in RCM to be clearly documented. Both the day-to-day and independent oversight review levels of key control elements should produce sufficient documentation that demonstrates how regulatory compliance risk is managed and supports the flow of information reported to the CCO and Senior Management. Such documentation should also support the periodic assessment of the RCM framework.

(viii) Role of Senior Management

OSFI expects Senior Management to oversee the RCM framework. Senior Management should take reasonable measures to assure that:

- the RCM framework is designed, implemented and maintained in a manner that is tailored to the needs of each business activity;
- compliance policies, procedures and practices are adequate and appropriate to control regulatory compliance risk and applied according to their terms by qualified individuals;
- compliance policies, procedures and practices are regularly reviewed so that they remain applicable in light of changing circumstances and regulatory compliance risks;
- all staff understand their responsibilities for complying with such policies, procedures and processes, and are held to account for performance of their responsibilities;
- key results of day-to-day compliance controls and independent oversight functions (including results that indicate the state of compliance with applicable regulatory requirements, remedial action taken, and regulatory compliance risk management) are reported to those who need to know; findings and recommendations made by the CCO or Internal Audit or other independent review function are acted on in a timely manner, and
- the CCO has the appropriate stature, authority, resources and support to fulfill the duties of the role, is sufficiently independent of operational management, and has the capacity to offer objective opinions and advice.

Senior Management should also proactively consider whether RCM deficiencies identified in one area of the FRFI's operations may also be present in other areas.

> Please refer to OSFI's Corporate Governance Guideline for OSFI's expectations of FRFI Boards of Directors in regards to operational, business, risk and crisis management policies.

V. OSFI's Supervisory Assessment

OSFI conducts supervisory work and monitors the performance of FRFIs to assess safety and soundness, the quality of control and governance processes, and regulatory compliance. Supervision is carried out within a framework that is principles-based and focused on material risks. The intensity of supervision will depend on the nature, size, complexity and risk profile of a FRFI, and the potential consequences of the FRFI's failure.

When supervising FRFIs, OSFI assesses their RCM frameworks against the expectations of this guideline. Such assessments may also be made in the case of applicants who seek Ministerial approval to incorporate or register new FRFIs.

> Regardless of where RCM roles and responsibilities reside in a FRFI or how they are constructed, OSFI's assessment will focus on the FRFI's ability to manage its regulatory compliance risk.

Footnotes

1 FRFIs are defined as banks, authorized foreign banks, trust companies, loan companies, cooperative credit associations and retail associations, domestic and foreign life insurance companies (including fraternal benefit societies) and domestic and foreign property and casualty insurance companies. FRFIs operating in Canada on a branch basis should read references in this document to "Senior Management" as references to Branch Management.

2 For example, OSFI's Corporate Governance Guideline.

3 "Enterprise-wide" means throughout all business activities applicable to the FRFI and its subsidiaries world-wide. The expectations in this guideline apply on an enterprise-wide basis. OSFI recognizes that internationally-active FRFIs may have to tailor global methodology to suit local environments.

4 Operational management should satisfy itself that FRFI line staff understand the regulatory compliance risks in the activity and that policies, processes and resources are sufficient and effective in managing those risks. Senior Management is responsible for overseeing the implementation of the RCM framework.

5 Oversight functions that may exist in a FRFI include: Financial; Compliance; Actuarial; Risk Management; Internal Audit; Senior Management; and the Board.

6 FRFIs' RCM frameworks are expected to vary based on the FRFI's nature, size and complexity and risks. Where a FRFI lacks some of the oversight functions, they are not sufficiently independent, or they don't have enterprise-wide responsibility, OSFI expects other functions, within or external to the FRFI, to address these gaps. References in this guideline to oversight functions are not intended to prescribe legal constructs or organizational models.

7 As defined on page 3 of OSFI's Corporate Governance Guideline.

8 To be reasonable, OSFI expects the measures used to be capable of achieving the prescribed outcome when considered by a reasonable person.

9 In a three lines of defence model, operational management is often referred to as the first line of defence.

10 In this context, independent means not directly involved in a revenue-generating function or in the management of any business line or product of the FRFI.

11 In a three lines of defence model, a compliance function would be considered a second line of defence.

12 Independent testing in the second line is not intended to duplicate the work of Internal Audit or replace an Internal Audit standard.

13 In a three lines of defence model, Internal Audit or other independent review function is referred to as the third line of defence. Using a three lines of defence model is a useful way of considering the adequacy of responsibilities and capabilities.

14 FRFIs have the discretion to establish the frequency of such reports, but OSFI expects that they will occur at least annually.

15 The definition of "material" should be established in consultation with Senior Management.

16 OSFI's March 2013 Advisory on Domestic Systemically Important Banks (D-SIBs) noted that "Canadian D SIBs are expected to have advanced practices in terms of the design and operation of oversight functions and internal controls. OSFI expects these practices to continue to improve as regulatory efforts become more intensive and leading international practices evolve."