REGULATORY GUIDELINE

Regulatory Compliance Management

SYSTEM COMMUNICATION NUMBER
Guideline 2020-02

ISSUE DATE
MARCH 2020

TABLE OF CONTENTS

I. Purpose and Scope of the Guideline 1
II. Definitions 1
Regulatory Compliance Management 1
Regulatory Compliance Risk 1
RCM Framework 1
III. RCM Framework - Overview 2
IV. RCM Framework 3
Role of the Chief Compliance Officer 3
Procedures for Identifying, Risk Assessing, Communicating, Managing and Mitigating Regulatory Compliance Risk and Maintaining Knowledge of Applicable Regulatory Requirements 3
Day-to-Day Compliance Procedures 4
Independent Monitoring and Testing Procedures 4
Internal Reporting 4
Role of Internal Audit or Other Independent Review Function 6
Adequate Documentation 6
Role of Senior Management 6
Role of the Board 7
V. The Corporation's Supervisory Assessment 7

I. PURPOSE AND SCOPE OF THE GUIDELINE

This is a Regulatory Guidance Document (Guideline) as contemplated by the Standards of Sound Business Practice (the Standards). It supplements and expands upon section 2.3, *Compliance* of the Standards and must be adhered to by Saskatchewan credit unions.

The Standards specify the principles and requirements to assist senior management in effectively managing the compliance risks faced by the credit union.

The purpose of this Guideline is to communicate the Corporation's expectations with respect to the management of regulatory compliance risk by credit unions. This Guideline complements the Corporation's Supervisory Framework and Assessment Criteria.

The Guideline also elaborates on a number of principles regarding key controls as part of Regulatory Compliance Management (RCM).

The Corporation expects credit unions to adopt a suitable approach to RCM practices that considers size; structure; nature, scope and complexity of operations; corporate strategy; and risk profile.

II. DEFINITIONS

REGULATORY COMPLIANCE MANAGEMENT (RCM)

The term Regulatory Compliance Management in this Guideline refers to the set of key controls through which credit unions manage regulatory compliance risk.

REGULATORY COMPLIANCE RISK

For the purposes of this Guideline, regulatory compliance risk is the risk of a credit union's potential non-conformance with laws, rules, regulations and prescribed practices ("regulatory requirements") in any jurisdiction in which it operates. Regulatory requirements are applicable to a credit union that require it to do (or prohibit it from doing) certain things or to act or conduct its affairs in a particular manner.

RCM FRAMEWORK

A RCM framework refers to the structures, processes and other key control elements through which credit unions manage and mitigate regulatory compliance risk inherent in its activities enterprise-wide[1].

[1] "Enterprise-wide" means throughout all business activities applicable to credit unions. The expectations in this Guideline apply on an enterprise-wide basis.

III. RCM FRAMEWORK - OVERVIEW

The Corporation considers an effective RCM framework to be an essential component of an overall risk management program that provides the means by which credit unions are satisfied they comply with applicable regulatory requirements. Non-compliance with applicable regulatory requirements can have significant negative effects on a credit union's reputation and/or safety and soundness and may lead to increased regulatory intervention.

The RCM framework should enable credit unions 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 credit unions.

Overall responsibility for assessment and management of regulatory compliance risk within the credit union should be assigned to an individual who is independent from business line management. This individual will have sufficient stature, authority, resources and support within the credit union to influence its activities, and should be designated, at least functionally, as a Chief Compliance Officer (CCO) or equivalent. The Corporation recognizes that this individual may have other responsibilities as well.

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 an effective RCM.

See further, *Role of CCO* below.

The Corporation assesses the quality of RCM at the following levels of control:

- business line management[2] 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 business line management by oversight functions[3&4].

The Corporation 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.

The Corporation will administer its RCM supervisory program in a manner appropriate to the circumstances of credit unions. Credit unions are expected to have risk management controls that are proportionate to its identified risks.

---

[2] Business line management should satisfy itself that credit union line staff understand the regulatory compliance risks inherent 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.

[3] As stated in the Supervisory Framework, there are six oversight functions that may exist in credit unions: Financial; Compliance; Risk Management; Internal Audit or other independent review function; Senior Management; and the Board.

[4] Credit union RCM frameworks are expected to be appropriate given the nature, size and complexity and inherent risks of the organization. Where credit unions lack some of the oversight functions, they are not sufficiently independent, or they don't have enterprise-wide responsibility, the Corporation expects other functions, within or external to the credit union, to address these gaps. References in this Guideline to oversight functions are not intended to prescribe legal constructs or organizational models.

IV. RCM FRAMEWORK

Key controls, including oversight functions, are the basic elements of a sound RCM framework. At a minimum, the Corporation 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; (viii) role of senior management[5], and (ix) role of the board[6]. Each of these items is described in further detail below.

The Corporation expects credit unions 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.

ROLE OF THE CCO

The CCO, or equivalent, should be responsible for assessing the adequacy of, adherence to and effectiveness of credit union day-to-day controls, and for providing an opinion to the board 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.

See further, *Compliance Reports to Senior Management and the Board*, below.

Where credit unions lack a particular oversight function, or such oversight function is not sufficiently independent or does not have enterprise-wide responsibility, the Corporation expects other functions, within or external to the credit union, to provide an appropriate level of independent oversight.

PROCEDURES FOR IDENTIFYING, RISK ASSESSING, COMMUNICATING, MANAGING AND MITIGATING REGULATORY COMPLIANCE RISK AND MAINTAINING KNOWLEDGE OF APPLICABLE REGULATORY REQUIREMENTS

Reasonable[7] 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

[5] As defined in the Corporation's Corporate Governance Guideline and Prudential Standard.

[6] In this document, the term "board" refers to one of: the entire board or a committee of the board that has been delegated a particular element of board oversight.

[7] To be reasonable, the Corporation expects the measures used to be capable of achieving the prescribed outcome when considered by a reasonable person.

requirements. The procedures should enable credit unions 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.

DAY-TO-DAY COMPLIANCE PROCEDURES

Appropriate procedures should exist in business line management[8] to reasonably assure that credit unions are complying on a day-to-day basis with the regulatory requirements applicable to its activities. 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.

INDEPENDENT MONITORING AND TESTING PROCEDURES

The adequacy of, adherence to, and effectiveness of day-to-day compliance procedures should be independently[9] overseen by the CCO[10], using a risk-based approach. Where appropriate in the circumstances of the credit union, independent monitoring and testing[11], wherever it is conducted within the credit union, 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 reports to senior management and the board.

The adequacy of, adherence to, and effectiveness of compliance oversight should be validated by Internal Audit or other independent review function[12]. Such validation should be on a rotational or other regular basis that the board considers appropriate, 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.

INTERNAL REPORTING

(a) **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

---

[8] In a three lines of defence model, business line management is often referred to as the first line of defence.

[9] 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 credit union.

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

[11] Independent testing in the second line is not intended to duplicate the work of Internal Audit or an independent review or replace an Internal Audit standard.

[12] 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.

within the credit union. 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.

(b) **Compliance Reports to Senior Management and the Board:** Regular reports to senior management and the board should be in a manner and format that allow them to clearly understand the regulatory risks to which the credit union 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, the frequency[13] of which is approved by the board.

The CCO should establish the general areas of content addressed in, and frequency of, regular RCM reports made to the CCO by business line management. Content and frequency should be sufficient to enable the CCO, senior management and the board to discharge their RCM responsibilities. The board should review and determine the type, content and frequency of reports to be satisfied that it is receiving the necessary information to carry out its oversight role.

Examples of content that reports should cover include: results of enterprise-wide compliance oversight, material[14] RCM framework weaknesses, instances of material non-compliance, material exposures to regulatory risk (and their potential direct or indirect impact on the credit union), related remedial action plans, information about significant legislative and regulatory developments, industry compliance issues, emerging trends and regulatory risks.

The Corporation expects the CCO to report regularly to the board all material information derived from the independent monitoring and testing to assist the board 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 business line management. Reports should provide an objective view on whether the credit union is operating within the RCM framework and identify problems or issues for senior management and the board, as appropriate. The CCO should meet with the board on a regular basis, and have in camera meetings, as appropriate.

The CCO should also provide an opinion to the board 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, that the credit union is in compliance with applicable enterprise-wide regulatory requirements. The opinion should be supported by sufficient pertinent information that is verified or reasonably verifiable.

See further, *Role of CCO* above.

[13] Credit unions have the discretion to establish the frequency of such reports, but the Corporation expects that they will occur at least annually.

[14] The definition of "material" should be established in consultation with the board.

The Corporation expects the CCO to report to the board, 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.

(c) **Internal Audit or Other Independent Review Function Reports to Senior Management and the Board**: The Internal Audit or other independent review function should report significant review findings along with management's undertakings with respect to remedial action to business line management, senior management and the board. 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. These reports should also assist the board in assessing the reliability of RCM assurances provided to the board by the CCO and senior management.

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 to senior management and the board, 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".

Review findings that are considered significant should be reported, as appropriate, to business line management, the CCO, senior management and the board. Actions taken by business line management in response to significant review findings should be monitored as appropriate by senior management and the board.

ADEQUATE DOCUMENTATION

The Corporation 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, senior management and the board. Such documentation should also support the board's periodic assessment of the RCM framework.

ROLE OF SENIOR MANAGEMENT[15]

The Corporation expects senior management to implement the RCM framework that has been reviewed and discussed with the board. Senior management should take reasonable measures to assure that:

[15] The Corporation's Supervisory Framework states that the credit union's senior management and board is responsible for the management of the credit union and is ultimately accountable for its safety and soundness and compliance with governing legislation. The Corporation's Corporate Governance Guideline and Prudential Standard notes that the board is responsible for providing stewardship, including direction-setting and general oversight of the management and operation of the credit union, including its internal control framework. Therefore, senior management's and the board's responsibilities in respect of RCM should align with these expectations.

- 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 business line management, and has the capacity to offer objective opinions and advice to senior management and the board.

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

ROLE OF THE BOARD[16]

Please refer to the Corporate Governance Guideline and Prudential Standard for the Corporation's expectations of the board with respect to governance and oversight of risk.

V. THE CORPORATION'S SUPERVISORY ASSESSMENT

The Corporation conducts supervisory work and monitors the performance of credit unions 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 Corporation's intensity of supervision will depend on the nature, size, complexity and risk profile of the credit union, and the potential consequences of the credit union's failure.

When supervising credit unions, the Corporation assesses the RCM framework against the expectations of this Guideline.

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

[16] *ibid*, footnote 15.