NAFCU CREDIT UNION COMPLIANCE 101:

Building Blocks for Compliance Skills

NAFCU

National Association of Federally-Insured Credit U

Sneak Peek

Risk Management Systems for Natural Person Credit Unions

NCUA recognizes that not all credit unions have the resources or expertise to implement a formal ERM framework, nor the range and level of risk to warrant one. The agency expects a natural person credit union to implement sound risk management processes tailored to its individual business model and risk tolerance.

Generally, a natural person credit union must ensure its risk management framework is consistent with its size, diversity and depth of risk exposures. The framework must be aligned with the credit union's business model and operate within its risk tolerances. For smaller, less complex natural person credit unions, examiners will ensure that the risk management process in place is sufficient to manage the major risks present in the credit union's business strategy and objectives, and reflects a reasonable cost-benefit balance. For larger, more complex natural person credit unions, examiners will ensure that the credit union has implemented a comprehensive risk management approach.

While NCUA does not require formal ERM frameworks for natural person credit unions, it encourages credit unions of all sizes to explore the benefits of incorporating core ERM principles and components into the risk management processes.

Formal Enterprise Risk Management Frameworks

ERM is a comprehensive risk-optimization process that integrates risk management throughout an organization. Typical risk management processes in a credit union involve an internal auditor making assessments and reporting findings to executive management or committees. This traditional approach focuses on identifying potential or established risks, and implementing controls to avoid or minimize that risk.

ERM frameworks are implemented across an organization, reducing the silo effect of having a single area or individual monitoring risk. The goal of an ERM framework is to strategically align an organization's risk-taking with its goals and objectives. ERM encourages organizations to take a broad look at all risk factors, understand the interrelationships among those factors, define acceptable levels of risk for the organization and continuously monitor to ensure that the defined risk thresholds are maintained. When properly implemented, ERM can facilitate business decisions, enabling a credit union to move faster and create opportunity while strategically managing risk.

NCUA's supervisory letter focuses on the ERM framework advanced by the Committee on Sponsoring Organizations of the Treadway Commission (COSO),[1] though the agency does not require organizations to use this specific model. The supervisory letter recognizes there is no "off-

[1] COSO is a joint initiative of private sector organizations that provides thought leadership on executive management and governance entities. The COSO ERM framework was released in 2004 and is widely recognized and accepted throughout the financial services industry. In October 2014, COSO announced its intention to update the 2004 framework. That project was still ongoing at the time this handbook was published.

the-shelf" framework that works for all credit unions and that a tailored approach for every credit union is best. Notwithstanding, COSO defines ERM as follows:

> Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

From this definition, the supervisory letter breaks down certain fundamental concepts of ERM. It defines ERM as a process that is:

- Ongoing and applied throughout an organization.
- Effected by people at every level of an organization.
- Applied in strategy setting.
- Takes an organization-level portfolio view of risk.
- Designed to identify potential events that could affect the organization and to manage risk within the organization's appetite.
- Able to provide reasonable assurance to an organization's management and board of directors.
- Geared to achieve objectives in one or more separate but overlapping categories.

No matter the framework chosen or designed by a credit union, the ERM framework must establish core principles, controls and due diligence within the credit union. ERM can be resourced internally, through paid consultants or a combination of internal and external resources. Regardless of the shape the framework takes, there are several basic components or principals that are likely to be evident in all ERM frameworks.

Eight Core Enterprise Risk Management Components

NCUA's supervisory letter on ERM discussed eight basic components as identified in the COSO framework. It also encouraged credit unions of all sizes to consider incorporating these principles into its enterprise-wide risk management processes.

Established Risk Culture. This is the "tone at the top" that sets the basis for how risk is viewed and addressed by an organization's stakeholders at all levels. The organization should define an enterprise-wide philosophy for risk management and risk appetite that is grounded in integrity, ethical values and has a good grasp of how various stakeholders are affected by the organization's decisions. Ideally, this would be manifested as consistent support for the ERM framework throughout the organization, from the chairman's office to staff members on the front lines. A strong buy-in from all levels of a credit union is critical when transitioning from a traditional risk management program to an ERM framework.

Clear Objectives. An ERM program encourages management to set clear objectives in four categories: strategic, operations, reporting and compliance. Strategic objectives are high-level goals, aligned with and supporting the mission of the credit union. Operations objectives are the effective and efficient use of a credit union's resources. Reporting objectives are primarily centered on the usefulness and reliability of a credit union's reporting. Compliance objectives seek to ensure a credit union is in compliance with appropriate applicable laws and regulations. Without clear objectives, the credit union cannot identify potential events affecting its achievement.

Event Identification. The organization with an ERM framework identifies internal and external events affecting achievement of objectives and distinguishes its risks from its opportunities. A positive example of event identification might be creating a "leading indicator" for each uncertainty or potential event, along with parameters that would trigger a risk management response. It is important for an ERM to distinguish between risks and opportunities, and ensure opportunities are channeled back to management's strategy or objective-setting processes. Examples of events could include major business decisions, portfolio or IT changes, selection of key partners or regulatory or market changes.

Risk Assessment. The organization continuously analyzes risk, considering the likelihood and impact of various scenarios, and uses the results of the analysis as a basis for determining how to manage those risks. For example, manager surveys may be used to develop a risk "heat map" that shows the level of risks.

Risk Response. Management evaluates possible responses to risks, selects a response and develops a set of actions that aligns risks with the organization's risk tolerances and risk appetites. Responses could include avoiding, accepting, reducing or sharing risk, depending on the cost and benefits associated with that risk. Ideally, risk information might be centralized and reported at the right time, in the right form to the right people, allowing management to make timely and effective decisions about risk.

Control Activities. To effectively respond to risks, an organization establishes and implements a set of policies and procedures. For example, policies and procedures may include requirements that: the ERM program exist independently of the risk-taking and operational functions; senior management be responsible for ERM reporting directly to the board of directors or board committee with oversight; and staff understand the difference between risk avoidance, risk reduction, risk sharing and risk acceptance.

Information and Communication. The organization identifies and communicates relevant information in a form and time frame that enables stakeholders to carry out their responsibilities. Key information about strategy and decisions should be communicated clearly and broadly throughout an organization. A robust and reliable reporting regimen should be evident.