

# Enterprise Risk Management

An Approach to Implementation in Credit Unions

# ACKNOWLEDGEMENT

Special thanks to the members of the Colorado Credit Union Working Group On ERM—a group of seven credit unions in the state of Colorado (both state and federally chartered) that developed this white paper in order to share information on best practices related to Enterprise Risk Management (ERM).

The working group would like to extend their thanks to the Credit Union Association of Colorado, SunCorp and RSM McGladrey, Inc. for their support in the development and distribution of this white paper.

## Colorado Credit Union Working Group On ERM

### ***Scott Collins***

Chief Financial Officer, Credit Union of Denver

### ***Tony Ferris***

Rochdale Group Consultants—Bellco Credit Union

### ***Betsy Guerrero***

Chief Financial Officer, Westerra Credit Union

### ***Schwan Hardi***

Internal Audit and Fraud Manager, Credit Union of Colorado

### ***Cyndi Koan***

Executive Vice President, Public Service Credit Union

### ***Wanda Matsuda***

Vice President, Enterprise Risk Management & Compliance, Westerra Credit Union

### ***Clint Schneider***

Vice President, Chief Audit & Risk Officer, Ent Federal Credit Union

### ***Michelle Tygart***

Staff Attorney/Assistant Vice President, Enterprise Risk Management, Public Service Credit Union

### ***Carol Ward***

Vice President, Enterprise Risk Management, Elevations Credit Union

### ***David E. Maus (Working Group Sponsor)***

Chief Executive Officer, Public Service Credit Union

# TABLE OF CONTENTS

|  |    |
|--|----|
| Why ERM?   | 1  |
| ERM Overview—"The Basics"                              | 2  |
| Move from "Current State" to Desired ERM Culture       | 4  |
| Risk Assessment  | 5  |
| Risk Management/Monitoring/Reporting                   | 8  |
| Exhibit 1: ERM Maturity Model                          | 11 |
| Conclusion   | 12 |
| Glossary   | 13 |
| Other Resources  | 15 |
| Appendices   | 16 |
| Appendix A Sample                                      | 16 |
| Appendix B Sample ERM Board Policy (1)                 | 17 |
| Appendix C Sample ERM Committee Charter                | 17 |
| Appendix D Sample Risk Assessment Rating System        | 19 |
| Appendix E Sample Risk/Heat Map                        | 20 |
| Appendix F Sample Risk Matrix for Monitoring/Reporting | 20 |
| Appendix G Sample Seven Risk Domains Dashboard         | 23 |

# WHY ERM?

*Some believe that, in many organizations, management of risk is too focused on operational and compliance issues, and, therefore, fails to identify and monitor emerging strategic risks that could affect long-term viability. Others believe risk management is too unstructured, resulting in overall weaknesses in managing risk.*

Whichever the case, we know the evolution of ERM in credit unions is ongoing and dynamic. This document is designed to educate and provide guidance to credit unions as they evaluate options and opportunities to develop their ERM approach and culture. Concepts from a document entitled Enterprise Risk Management–Integrated Framework, developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), were used for many core elements in this paper. Recognized as the leading guidance on Enterprise Risk Management, the document provides a framework to identify, assess and manage risk, and can assist boards and management in understanding an enterprise-wide approach.

## What is Enterprise Risk Management?

Fundamentally, credit unions are in the business of managing risk. Examples include asset liability management, vendor management, business continuity planning, auditing, strategic planning, and project management. In most credit unions, these risks tend to be managed individually, in a silo approach; and while an effective ERM program does not replace these existing risk management practices, it can serve to form a common sharing of risk-related information resulting in a comprehensive view of risk across the organization. This creates increased transparency and understanding of all risks organization-wide, and allows for gaps in risk management to be identified. Successful ERM programs, therefore, result in credit unions assessing risks globally, with a forward-looking perspective, resulting in more effective risk management on an enterprise-wide basis.

Enterprise Risk Management is not:

- A finite project or a one-time event.
- A risk checklist, spreadsheet to complete or a software program to implement.
- A risk audit, audit of controls or compliance assessment.
- One individual's job or responsibility.

Enterprise Risk Management is a collaborative process to identify, manage and monitor organizational risks and opportunities, both internal and external, to ensure achievement of the credit union's strategic objectives and continued financial stability and viability. It is more than just identifying control weaknesses; rather, it facilitates identification of potential events that, if they were to occur, could result in negative or damaging consequences for the organization. It is also designed to ensure that risk is managed within the credit union's appetite or tolerance

level. The goal of ERM is not to eliminate risk. Instead, an effective ERM process will create an environment where risk is embraced and allows the board and management to make holistic, "risk-intelligent," strategic decisions. ERM, therefore, is a strategic tool rather than just a compliance tool.

## What are the Benefits to Credit Unions?

A comprehensive ERM program will:

- Provide a comprehensive view of organizational risk, and a framework to consider how risks interrelate, resulting in enhanced decision-making.
- Improve communication and result in deeper, richer discussions about risk throughout the organization, thus positioning the credit union to take advantage of opportunities.
- Establish a philosophy regarding risk and a risk culture, including aligning risk appetite and strategy, allowing for risk optimization within defined risk tolerance levels.
- Allow management to identify and deal effectively with emerging risks, thus reducing surprises and potential losses.
- Facilitate effective allocation of resources via risk/reward analysis, elimination of redundant risk management activities, and identification of process improvement opportunities.

## What Makes an ERM Program Successful?

The keys to a successful ERM program include:

- Obtaining board and management buy-in and active involvement.
- Beginning with a simple approach, focusing on identified problem areas, and allowing the program to evolve over time.
- Establishing realistic expectations for implementation. Immediate success is rare; ERM must be viewed as a long-term cultural change.
- Realizing that there is not a "one-size-fits-all" approach; but, rather, a progression and maturity based on the size and complexity of the credit union.
- Focusing on material risks to avoid getting bogged down.
- Assigning an individual or team to "champion" the initiative and ensuring they are provided with adequate time, support and resources to focus on the initiative.
- Working in conjunction with the credit union's overall strategic plan and organizational culture, ensuring that organizational goals, strategies and products are consistent

with risk tolerances that have been established by the board and senior management.

## Board Fiduciary Responsibility

Regulatory expectations of effective risk management require an informed board of directors to guide the credit union's strategic direction, within the parameters of its risk tolerances. The board of directors has a fiduciary responsibility to understand the risk position of the credit union and to understand how the strategic direction they are setting impacts the credit union's risk position. Regulatory expectations are that risk-monitoring systems, which enable the board to hold management accountable for operating within risk tolerance levels and require that management actively informs the directors of material risks, are in place.

## Regulator Expectations

NCUA letters to credit unions have risk management at the core of their message. They outline regulators' expectations for effective risk management. An effective ERM program, therefore, proactively incorporates the risk concepts and messages delivered in NCUA letters to credit unions.

The guidance from regulators, to adopt an institution-wide ERM program, is a challenge to most credit unions' conventional business models. Credit unions, as well as other financial institutions, traditionally look to financial indicators (commonly referred to as "lagging indicators") to make strategic decisions. This methodology has been very successful; however, the current economic environment, along with the changed expectations of regulators, requires financial institutions to anticipate future risks in order to survive. Identifying and assessing emerging risks through the use of leading indicators, to make both business and strategic decisions, is key to a successful ERM program.

# ERM OVERVIEW—"THE BASICS"

*A successful ERM program is a forward-thinking approach that allocates resources to the areas exhibiting weakness or adverse trends. Practical application requires implementation from the top down. The credit union's board of directors must adopt the vision of the program, as well as a comprehensive policy, which must then be supported by the senior management team, and implemented organization-wide through active committees, procedures and internal controls. Employing sufficient staff, with access to necessary resources, is also integral to the process.*

## Getting Started

Effective integration of risk management activities, that are in line with both strategic initiatives and regulatory expectations, can be a daunting task for any organization. This section will outline a basic framework and implementation plan, followed by some concepts to consider and address as the plan is developed. Subsequent sections will elaborate on these topics and provide practical examples of the concepts presented in the overview and the steps touched on in this section.

## Common Characteristics

From a practical standpoint, the actual scope, roles and desired ERM culture (or model) should be commensurate with the size and complexity of the credit union. However, it is anticipated that certain "best practices" will be employed in developing and

implementing an effective ERM program. These common characteristics include performing an initial evaluation; developing an action plan; identifying, measuring and monitoring risk; and periodically evaluating the effectiveness of the process, vision and integration throughout the organization.

## Initial Evaluation

The first step in implementing an effective ERM program is for management and the board of directors to jointly assess the existing risk management process, evaluating its effectiveness and identifying its deficiencies in order to develop a shared vision. Based on the size and complexity of the credit union, some will likely be further along the ERM Maturity Model spectrum than others. (A sample ERM Maturity Model can be found in Exhibit 1 on page 19.) A key component of the vision is buy-in and support from the board of directors and senior management.

## Action Plan

Once the assessment is completed and an ERM vision is formed, senior management, in conjunction with the board, should develop an appropriate action plan to implement the vision. This plan should address expected timelines and assign duties to the individuals who will be responsible for moving the vision forward. Some credit unions have found it beneficial to designate a Risk Officer<sup>1</sup> and form a cross-departmental, risk management or risk oversight committee. The roles of the Risk Officer and the committee should be clearly defined and be consistent with the overall ERM vision and corporate culture.

## Risk Assessment

At a minimum, an effective ERM program should assess the risk associated with the following seven risk domains defined by NCUA:

- Strategic Risk
- Transaction Risk
- Credit Risk
- Interest Rate Risk
- Liquidity Risk
- Compliance Risk
- Reputation Risk

For each domain, the assessment should define the key metrics that will be used to evaluate the risk, develop a risk profile for each metric, and track these metrics over time. The actual metrics that will be measured will vary depending on the specific needs of the credit union; however, best practices suggest that there should be more than one metric for each risk domain. Ideally this process would not only measure current risk profiles, but also provide early warning indicators to identify emerging risks as well. In defining and developing the metrics and their profiles, it may be helpful to perform a risk assessment to inventory risks related to each domain. This will help to determine from where the organization's risks are originating. In general, a risk profile would include:

- Developing probability and impact assessments;
- Identifying inherent and residual risk (impact on earnings and capital);
- Tracking the metrics over time and classifying both direction and magnitude of risk; and
- Developing appropriate action plans.

## Managing/Monitoring/Reporting

Reports, conveying the risk associated with each of the core risk domains, should be generated periodically, for the board and senior management. Policies and procedures that identify frequency of reporting, types of reports to be generated, appropriate risk tolerances, and adequate mitigation measures should be developed.

In addition, emerging risk evaluation and discussion should be integrated into the reporting and monitoring process. The board and management should proactively measure and discuss potential risks to the organization based on changes in both the internal and external environment.

## Re-evaluate

As mentioned previously, an ERM program is not a static project. Changes in the size and complexity of the credit union, as well as changes in risk tolerances over time, dictate that it be dynamic. Periodically, management and the board should perform new self-assessments to ensure their program is both, appropriate and effective, and to make necessary adjustments and enhancements as warranted.

While larger, more complex credit unions will generally visualize and develop ERM programs that are more robust and further along the risk maturity model spectrum, a best practice of any ERM program should be to communicate the expectation of risk awareness and evaluation across the entire organization.

*The first step in implementing an effective ERM program is for management and the board of directors to jointly assess the existing risk management process, evaluating its effectiveness and identifying its deficiencies in order to develop a shared vision.*

<sup>1</sup> Best practices implementation does not require the Risk Officer to be a separate position. It is acceptable to assign the duties to an existing employee or outsource some or all of the responsibilities as long as it meets the needs of the credit union.

# MOVE FROM “CURRENT STATE” TO DESIRED ERM CULTURE

## Initial Evaluation

The ERM implementation process begins with the board of directors performing a self-assessment of the current environment. This initial evaluation should, at a very high level, determine where the directors, senior management and the organization, overall, are in understanding roles and responsibilities as they relate to ERM. The initial evaluation can also help to identify where, in the ERM Maturity Model, the credit union currently operates. A high-level evaluation could be completed using an assessment tool, such as the sample questionnaire provided in Appendix A. Significant components of the initial evaluation might include:

- **Alignment of Board of Directors and Senior Management**—This includes the willingness to accept risk, the integration of risk appetite into strategic planning, and the understanding and agreement regarding high level/key mitigation strategies and tactics as defined by board-approved policies.
- **Assessment of Communication on Risk between Board and Senior Management**—Can it be described as transparent, effective, informative, clear, candid and timely?
- **Sufficiency and Effectiveness of Key Risk Measures/Metrics**—Are they adequate in providing an understanding of current and changing risks, as well as management’s risk perspective and remediation of significant weaknesses?
- **Assessment of Use of Early Warning Indicators**—Are they used by senior management and, where appropriate, the board to identify and monitor risk?

## From Evaluation to ERM Culture


Once the board and senior management have completed the initial evaluation, there should be a good understanding of the credit union’s risk management philosophy, and whether there is uniform understanding between senior management and directors regarding risk tolerances, roles/responsibilities for risk management, and ongoing oversight and monitoring.

*“Risk tolerances are the acceptable levels of variation relative to the achievement of objectives...Operating within risk tolerances provides management greater assurance that the entity remains within its risk appetite, which, in turn, provides a higher degree of comfort that the entity will achieve its objectives.” COSO ERM Integrated Framework*

Upon completion of the initial evaluation, the credit union’s formal and informal policies, processes, practices and risk management techniques should be identified. Senior management’s next step is to develop the guiding vision for the evolution to the desirable future state of ERM. As with any strategic planning effort, formulation of an ERM vision should guide the creation of specific business objectives designed to pave the way to a desirable ERM culture that will be endorsed by senior management and the board of directors.

## Defining the ERM Program

An ERM program should encompass management’s assessment of the people, technology and process capabilities already in place and functioning, as well as promote the new capabilities that the credit union may need to develop. It may acknowledge the

A photograph showing several people rappelling down a rock face. They are wearing safety gear and are positioned at different heights, with ropes visible. The background is a clear blue sky.

*Over time, the initial ERM program should be updated and enhanced periodically in order to ensure that it continues to keep pace with the evolution of the credit union’s strategic plan, and with emerging internal and external risks.*

current state of ERM development within the credit union and should also provide the direction to move to a more mature model within a given time period. Once the program is defined, specific business objectives should be developed to support implementation through analysis of roles/responsibilities and modifications to organizational governance structure and processes. This includes implementation or modification to policies, procedures, processes, methodologies, tools, techniques, information flows, communications and technologies.

### Developing and Implementing Action Plans

Key ERM business objectives should be supported by specific, actionable implementation plans. At a minimum, an ERM program should include consideration of deployment plans, training sessions, reinforcement mechanisms, and monitoring/re-evaluation for success of all major segments.

While not a regulatory requirement, credit unions are encouraged to establish some form of ERM governance, such as a risk management/oversight committee. Committee coordination can

greatly facilitate a single framework for managing risk, and a common language and tools for implementation across the credit union. The structure of this committee should be tailored according to the culture of the credit union. For example, a sample charter for a cross-departmental ERM committee is provided in Appendix C. In contrast, in Appendix D, there is a sample Risk Oversight/ERM Committee Charter describing the responsibilities envisioned for a committee comprised of senior executives. These are illustrative examples provided to encourage creative development of an appropriate oversight structure that may be unique to each credit union.

Over time, the initial ERM program should be updated and enhanced periodically in order to ensure that it continues to keep pace with the evolution of the credit union's strategic plan, and with emerging internal and external risks. Key roles/responsibilities and governance infrastructure may need to be refined or refocused. At the outset of this project, senior management should establish project milestones and provide targeted opportunities for reassessment of the program's implementation efforts.

## RISK ASSESSMENT

### Importance of the Business Model

The cornerstone of an ERM program is the credit union's business model. The business model should define activities the credit union will undertake, the products and services it will provide, how it will conduct business, and in which markets it will operate. It should define the vision, mission and values, and it should be consistent with the credit union's appetite for risk.

To ensure the credit union's ongoing success, senior management must determine and articulate the barriers and uncertainties inherent in the business model. These barriers and uncertainties constitute risks.

### Conducting a Risk Assessment

To effectively understand and manage these risks, the credit union should conduct a risk assessment. Failure to perform an effective risk assessment increases the likelihood that the credit union will be unprepared to anticipate or manage risk occurrences that could adversely affect the achievement of goals and, more significantly, earnings and net worth.

Capital, or net worth, constitutes the reserve of funds available to manage and absorb risks to the institution. In the broadest sense, the amount of capital a credit union has accumulated is an important determinant of the amount of risk it can assume.

Although a variety of approaches can be used to conduct a risk assessment, each approach generally contains the following components:

- **Business Model**—A comprehensive understanding of the credit union's business model (i.e., strategic plan, products, services, business lines/processes and functions, etc.).
- **Inherent Risks**—Awareness of the inherent risks associated with credit union services and operations (e.g., credit risk, interest rate risk, transaction risk, reputation risk, liquidity risk, etc.).
- **Risk Identification**—Identifying events that may have a negative impact on the credit union and the achievement of its business objectives, on and off its balance sheet.
- **Analysis and Prioritization**—Risks must be evaluated using a scoring system to measure likelihood and impact of occurrence, etc. Awareness of risk management systems, i.e., strategies, internal controls, monitoring and reporting, to manage risk to an acceptable level in accordance with board of directors and senior management tolerance criteria.

There can be many levels of risk assessments, ranging from a broad assessment of the credit union (enterprise level) to a more focused assessment of a business product, unit or function (business level).



## Enterprise Level Assessment

A logical starting point in the risk assessment process is to conduct an enterprise level risk assessment for the credit union. This can then lead to, and be followed by, risk assessments at the business unit or process level. The primary focus and goal of the enterprise level assessment is to establish an initial high level basis for determining whether the credit union has reasonably effective risk management practices throughout the credit union, and to identify any significant inherent risks requiring immediate and/or additional mitigation efforts. The desired outcome of the enterprise level risk assessment is to establish a basis for determining that:

- Management has processes for identifying, assessing and managing top risk exposures related to core strategic objectives.
- Risks being taken in pursuit of objectives are effectively monitored to ensure they are within acceptable levels within the defined risk appetite of the credit union.
- Management has processes in place to identify emerging risks and related changes in risk prioritization in a rapidly changing environment.

The process first involves reviewing the credit union's strategic plan and identifying key strategic objectives that further translate into business initiatives and goals integral to the credit union's success. Next, select the most important elements of the credit union's strategy and goals and align with the senior management and related business units that are primarily responsible for achievement of the goals. Pertinent questions that may be asked at this time are: (1) why are these initiatives important to the success of the credit union, (2) which of these initiatives are most important and, (3) what risk management information is available? An initial determination should also be made as to which of the internal and external inherent risk factors associated with the credit union industry, e.g., credit risk, interest rate risk, liquidity, reputation risk, transaction risk, etc., may present material barriers to achievement of strategic and/or business unit objectives.

Through interviews, surveys or cross-functional meetings with senior and line management, specific material risk events that might arise from the risk factors identified can be discussed and documented. Examples of questions that could be asked to spur discussion and brainstorming to identify risks include:

- What are the greatest risks, inherent and emerging, that could keep the credit union from achieving its strategic objectives? What processes help identify these?

- What assumptions are integral to the credit union's strategic plan? What if those assumptions are incorrect?
- What internal or external risks, if not effectively managed (controlled or monitored), would have a significant impact to the credit union's strategy, earnings, reputation, etc.?
- Can management tolerate the risks if they were to occur at a significant level of impact?
- Where are opportunities within the credit union to improve risk management?

At this point an initial determination should also be made, largely based on management's opinion, as to the potential likelihood and impact of the identified risk events occurring, and then evaluating the effectiveness of mitigation and controls. A scoring system, rating likelihood and impact factors, less a mitigation-effectiveness score that rates control strength, could be applied against an inherent risk score—one that rates effectiveness of controls, processes or other mitigation strategies. This could be the standard framework for ultimately determining residual risk. (See the Response Effectiveness Rating criteria referenced in Appendix E.) The residual score for risk items can then be reviewed to determine where risk mitigation efforts are best focused to get the most risk-reducing impact. Creating a risk heat map (see Appendix F) by graphing each risk, based on its probability and impact, can visually show which risks might warrant further review to identify additional risk mitigation strategies.

Once the major risks at an enterprise level are identified, analysis should be completed to ascertain what, if any, risk mitigation plans/strategies, risk tolerance levels and information systems have been implemented to: (1) monitor and measure the risks against strategic objectives, and (2) reduce either the likelihood or the impact of the risks to the credit union within defined tolerances. Integral to this process is identifying the degree of monitoring and the type reports that are available to manage current and emerging risks. An initial determination regarding frequency of preparation and audience distribution should also be made to answer the question: "Is timely, relevant, risk information being provided to key decision makers, such as senior management and the board of directors?"

The initial enterprise level risk assessment will provide a determination of the credit union's overall awareness of key strategies and objectives, the ability to recognize current and emerging risks, and the effectiveness of current risk management systems and strategies. This assessment can then be used to further evaluate and develop risk mitigation action plans where potential deficiencies or limitations with risk management processes and

*The cornerstone of an ERM program is the credit union's business model.*

reporting may have been observed. Mitigation options include: (1) risk transfer, (2) avoidance, (3) reduction, or (4) acceptance. The assessment also produces documentation of the most important goals in the business plan, along with attendant risk factors, specific risks and risk mitigation strategies. This information can be used to prioritize and conduct a more detailed business level risk assessment, taking the same process to the next level of detail in the credit union and conducting a functional evaluation.

The risk assessment process generally includes the following steps:

### **Risk Identification**

- *Organizational Structure*—Review and understand the credit union's organizational structure and business unit/functional areas (i.e., commercial lending, mortgage lending, loan operations, compliance, operations, IT, card services, etc.), including line and senior management responsible for the business units or functional areas.
- *Key Processes and Responsibilities*—For each business unit/functional area, identify and document key processes and responsibilities necessary to the area's accomplishment of department/business objectives and goals. Reference resources may include internal audit working—papers/process—flows and information technology data maps.
- *Risk Events*—For the key processes and regulatory compliance areas noted, identify and document, what are believed to be, the more significant/material external (economic, natural, political/regulatory) and internal (infrastructure, personnel, process) factors that present significant risks to the achievement of objectives within all business /functional areas. Other sources available for risk identification include industry guides, internal audit documentation, examination reports, etc. Begin associating the risks identified with the applicable regulatory risk domain(s), such as credit risk, interest rate risk, transaction risk, etc. This can be done by considering what can go wrong in a business process or compliance area and, then, relating these items to the inherent risk domain definitions. This will lead to, and facilitate, risk aggregation by inherent risk domain and business functional area.

### **Risk Evaluation**

- *Risk Measurement*—Analyze and quantify the risks identified for each business/functional area and key process based on qualitative or quantitative scoring methodologies, and considering the potential impact and inherent likelihood of occurrence absent any controls or other risk mitigation efforts (i.e., worst-case scenario). Factors contributing to inherent likelihood determination can include credit union historical loss experience, transaction volumes, personnel expertise, industry experience and uniqueness/complexity of processes and systems. Predominant factors to consider and measure are financial impact and reputation impact. Quantitative measurement is preferable to facilitate a numeric presentation of the highest risk areas in the credit union. (See sample quantitative measurement system in Appendix E.)
- *Prioritizations*—Assess and prioritize risks by aggregating and ranking risk scores by business/functional units, compliance areas and inherent risk categories. This compilation provides a portfolio view of key risks at a business unit level and an initial summary of which categories present the most significant risk to the credit union. To the extent possible, link the risks to the credit union's key strategic objectives identified during the enterprise level assessment. Management can now use this information to make decisions for evaluating strategic components of risk management to determine residual risk.

### **Risk Management**

- *Risk Management Practices and Monitoring*—For the business units presenting significant risk to the credit union, evaluate the risk management systems (i.e., policies and procedures, internal controls, measurements, etc.) to limit or otherwise mitigate the risks identified. Additional sources of information that may be helpful during this analysis include internal or external audit reports, examination reports and regulatory supervisory letters. A determination should be made as to the amount of residual risk (unmitigated risk) remaining after considering risk management practices, and whether the risk is within acceptable tolerance levels.

Once risk management practices have been designed and employed, a monitoring process should be implemented to ensure that they are operating as intended.

# RISK MANAGEMENT/MONITORING/REPORTING

Regulators are tasked with evaluating the effectiveness of credit unions' risk management programs. An effective ERM program requires directors be informed and that they set direction for defining the credit union's risk tolerances. To this end, board-approved policies, creating the basis for monitoring and reporting, should be in writing. Control limits should be established, monitored and reported to the board on a regular basis; and although there is no regulatory guidance on specific measurement standards, risks should be measured consistently across the organization. Risks should be measured in terms of impact on net income, net worth, or on another standard that can be consistently applied to all risk areas of the credit union. NCUA appears to be moving in the direction of measuring risks in terms of the potential impact on net worth.

## Set Measurable Target Ranges

As the credit union develops policies and defines risk tolerances, the board and management need to remain cognizant that the established target ranges must be measurable. The more specificity that exists in the policies, the easier it will be to monitor. However, policies that contain too much detail may restrict management's ability to respond appropriately, quickly and effectively. As outlined previously in this document, each credit union should establish its own risk tolerances based on product mix, size, business model, net worth and strategic direction. The sophistication of monitoring and reporting processes needs to be reflective of the credit union's complexity. After risks have been identified and quantified, the ongoing process of measuring and monitoring risk levels becomes an essential component of an effective ERM program.

Leading indicators are key to monitoring the credit union's emerging risks and allow the credit union to make well-educated "predictions" of where its risks will be in the short-term.

Examples of leading indicators within credit unions may include:

- A narrowing interest rate spread between 10-year Treasury notes and the federal funds rate, resulting in a decrease in net interest margin.
- An increasing average level of initial, unemployment claims. This may be an indicator of higher unemployment within the credit union's membership, leading to potential increases in loan defaults, loan charge-offs and bankruptcy filings, as well as diminished loan approvals.
- Declining member credit scores, as well as downward trending property values. These can be leading indicators of future loan portfolio problems, including defaults, charge-offs and bankruptcies.

## Committee Monitors and Reports Results to Board

Once the credit union establishes a baseline risk profile, ongoing monitoring and reporting must be implemented. As many credit unions have found success with the adoption of Asset Liability (ALCO) and Audit committees, optimizing ERM success should include the implementation of a Risk Committee. The Risk Committee is charged with the ongoing monitoring of the credit

union's risk profile and identifying potential impacts to the credit union by identifying emerging risks through leading indicators. This committee reports a summary of the results to senior management, as defined within adopted policies. Heat Maps and Risk Dashboards are excellent tools to communicate the summary of both present and emerging risks.

After the initial assessment, subsequent assessments should be compared to previous assessments to determine if the risk profile has changed. Over time, trends identifying which risks are unchanged, increasing or decreasing will emerge. Each assessment should also identify if the risk being measured falls within the limits established by the board of directors.

## Measuring and Monitoring Risk

Consistent, timely and accurate measurements will help credit union management determine if risk levels are stable, increasing or decreasing. Credit union management and the board of directors should establish an early warning process to alert management when the credit union is approaching a risk limit. Similarly, the reports should indicate when it might be appropriate for the credit union to consider taking on additional risk.

A process needs to be established to identify new and emerging risks. As the credit union expands field of membership and adds new products, locations or other operational changes, potential new risks must be identified and incorporated into the monitoring process. The Risk Committee may wish to include regular updates from all functional areas of the credit union; allowing the opportunity to assess changes in relation to the credit union's risk tolerance, and to incorporate them into the monitoring process.

The 5300 Call Report is a standard report prepared by all credit unions. This report is utilized by examiners as a supervisory tool and as an early indicator of potential risks and shifts in the credit union's risk profile. In moving to a more complex ERM program, the credit union will also require more complex indicators. The 5300 Call Report is both a stable and quantitative indicator of potential risk, and when reviewed in conjunction with leading indicators and monitoring of the credit union's internal changes, provides a comprehensive overview of the credit union's current and emerging risk.

When developing risk-monitoring reports, credit unions should consider 5300 Call Report data as a good standard measure of high-level risks. Monitoring reports need to encompass the seven risk domains defined by NCUA (credit risk, interest rate risk, liquidity risk, transaction risk, compliance risk, strategic risk and reputation risk).

Many credit union activities may be impacted by a combination of risks. Credit unions with large portfolios of fixed rate, sub-prime mortgage loans would want to measure, at a minimum, credit risk, interest rate risk and liquidity risk. It is important to look at individual risks as well as layered risks, especially when measuring the change in direction of the credit union's risk profile. Depending on the credit union's complexity and risk profile, additional risks such as concentration risk, servicing risk and premium risk may need to be included in monitoring reports.

Because Enterprise Risk Management can seem overwhelming, one of the biggest challenges can be determining how to begin. Examiners will typically look at the seven domains of risk in two categories:

- Market risks, which are more easily measured and are relatively objective measures; and
- Institutional risks, which are more subjective and more difficult to measure.

Market risks include credit risk, interest rate risk, and liquidity risk. Because these are more easily quantified, it is recommended that credit unions build their monitoring reports with these risks and then expand to the more subjective risk measures. Most credit unions can look to existing Asset/Liability Management (ALM) and liquidity policies for existing limits established by the board of directors. An ALM policy may limit fixed rate investments to 10% of assets. This could become one of the interest rate risk targets that would be measured and reported. However, this may need to be translated to the standard measure selected by the credit union. For example:

|                       |              |
|-----------------------|--------------|
| • Credit Union Assets | \$50,000,000 |
| • Total Net Worth     | 5,000,000    |
| • 10% of Assets       | 5,000,000    |

The risk policy might state that no more than 100% of net worth may be invested in fixed rate investments.

As credit unions become more complex, their level of analysis should become more sophisticated. Credit unions utilizing income simulation modeling or other modeling tools, for example, may find it useful to run several "what if" scenarios to determine the impact on net income or net worth in each scenario. Ideally, risk measures should be tied to the impact on net income or a change in the impact to net worth.

The Financial Performance Report (FPR), available on NCUA's website, provides each credit union with five quarters of data as well as a comparison to peer. The FPR can be a useful tool as the credit union begins to evaluate the existing risk in its balance sheet and develops monitoring reports.

How to measure and monitor institutional risks, including transaction risk, compliance risk, strategic risk and reputation risk, will vary based on the complexity of the credit union. For example, transaction risk includes fraud. For credit unions with credit card portfolios, measuring the risk of a compromised card base is complex, but quantifiable. Factors to consider are:

- The cost of communicating to the members.
- The cost of reissuing cards.
- Actual losses due to fraudulent charges.
- The loss of interest income.
- Increased charge-offs.
- Lost interchange income while cards are blocked.
- Staff time.

What is more difficult to quantify and measure is the potential risk to reputation. What is the impact if news of the card breach makes it into the media? How much trust and future business is lost? Each credit union will have to develop a methodology for estimating the potential impact of institutional risks. The key to effective monitoring is that the selected methodology is consistent and identifies changes in the credit union's risk profile over time.

## Mitigating Risk Through Policies, Processes and Control Systems

Once risks have been identified and compared to defined risk tolerance levels, mitigation may be accomplished through a variety of strategies. Generally risk is managed or transferred through policies, processes and control systems.

- **Managed Risk**—Effective control systems can be among the most effective, and least costly, methods for mitigating potential risks.

In the investment example on page 15, one of the strategies for mitigating interest rate risk is to limit fixed rate investments to 10% of assets. Further mitigation might include limiting maturities on fixed rate investments to a shorter term (e.g., three years).

Managing credit risk can also be an effective mitigation strategy. A credit union may choose to mitigate credit risk by establishing a policy that would limit the amount of loans originated to borrowers with FICO scores below 640. Based on historical analysis of charge-offs, and considering current environmental factors, the credit union would be able to quantify the anticipated loss ratio on this pool of sub-prime paper and calculate the impact on net income and, ultimately, net worth.

- **Transfer Risk**—Another effective mitigation strategy is to transfer the risk. This is often accomplished by outsourcing a function. For example, outsourcing data processing, or purchasing insurance, effectively transfers a portion of the credit union's risk to a third-party vendor. All credit unions purchase surety bonds to transfer litigation risk to

the insurance company. Other insurance, such as collateral protection insurance, can be utilized to mitigate some types of default risk.

Risk can also be transferred or limited by contract terms. Limitation of liability, indemnification, confidentiality and warranties can help limit exposure to risks with vendors and business partners.

***In summary, every credit union should:***

- Develop, implement and periodically re-assess methodologies for measuring risk that are commensurate with the complexity of the credit union.
- Prepare comparative analysis reports that identify movement in the credit union's risk profile.
- Provide analysis summaries to senior management or the board of directors as appropriate.
- Take appropriate action in accordance with changes in the risk profile.

- Regularly review mitigation efforts and evaluate their effectiveness.

## **Transitioning through the ERM Maturity Model Spectrum**

While risk management, in any given credit union, will vary depending on size and complexity, it should be reemphasized that ERM is a continual, evolving process. When setting the groundwork for an ERM program, and trying to determine the adequacy of current risk management practices and where the credit union wants to be, it might be helpful to refer to the ERM Maturity Model on page 18. Although it may be unrealistic to expect all credit unions to migrate fully to the optimized model, the maturity model is helpful in determining what steps can be taken to move in that direction. The remainder of this section provides an overview of the ERM Maturity Model and how to determine the credit union's position in the risk management spectrum.



***As the credit union expands field of membership and adds new products, locations or other operational changes, potential new risks must be identified and incorporated into the monitoring process.***

# EXHIBIT 1

# ERM MATURITY MODEL

| Key elements |               | Description   |  |
|--------------|---------------|---|--|
| WEAK         | Limited       | Risk activities are ad hoc with no organizational risk objectives or tolerances defined.  | <ul style="list-style-type: none"> <li>» Limited risk experience</li> <li>» Risk responses are reactionary</li> <li>» No risk policy</li> <li>» No risk function</li> <li>» Success is based on individual employee response of risk</li> </ul>  |
| WEAK         | Fragmented    | Risk functions are handled disparately across the organization by individual business units. Risk factors are limited to business continuity, information security, financial and compliance within business silos. | <ul style="list-style-type: none"> <li>» Risk expertise is limited predominately to BCP, ALM, Information Security &amp; compliance</li> <li>» Risk communication is silo'd within individual areas</li> <li>» Risk management is reactionary</li> <li>» Risk management responses are procedural in nature</li> <li>» Limited risk controls testing</li> </ul>  |
| MODERATE     | Comprehensive | Risk is evaluated organization-wide and attempts to assess all risk types. Limited integration with strategic and business decision making. Risk evaluation is limited to qualitative measures.                     | <ul style="list-style-type: none"> <li>» Risk function has been established</li> <li>» Organizational understanding of risk management</li> <li>» Criteria for measuring likelihood and impact are established</li> <li>» Risk tolerances have been established for significant risk factors</li> <li>» Comprehensive collection and communication of organizational risks</li> <li>» Ongoing risk priority plans are developed and managed</li> <li>» Risks are internal in nature with limited predictability</li> <li>» Risks are measured in qualitative terms</li> <li>» Annual assessment of risk environment is performed</li> <li>» Risk management process, methods controls are tested</li> </ul>  |
| STRONG       | Integrated    | Risk management practices are tightly integrated with strategic and business decision making. Risks are aggregated by risk type.  | <ul style="list-style-type: none"> <li>» Part of strategic planning framework</li> <li>» Integration with traditional risk management activities</li> <li>» Balanced qualitative and quantitative risk measures</li> <li>» Risk tolerance is formulated and managed as part of organizational goals</li> <li>» Strong risk management culture organizationally</li> <li>» Strong board and staff understanding</li> <li>» Risk measures are calculated and aggregated across organization</li> <li>» Risk profile is communicated organizationally</li> <li>» Methodology for evaluating inherent and residual risk is present</li> <li>» Risk program is forward looking</li> <li>» Predictive indicators and organizational influencers have been established</li> <li>» Continuous assessment methodology has been established</li> </ul> |
| STRONG       | Optimized     | Risk management is utilized for predictive modeling and value creation through opportunity exploitation. Risks are well defined and quantitative. Risk management is institutionalized.                             | <ul style="list-style-type: none"> <li>» ERM value is quantified and measured in both strategic benefits and bottom line dollars</li> <li>» Risk management expertise and organizational linkage has been institutionalized</li> <li>» Strong risk management benchmarking and best practices have been established</li> <li>» Integrated risk management application has been implemented</li> <li>» Capital allocation models have been developed and installed to maximize risk-adjusted returns</li> </ul>   |

### **Limited**

A Limited risk management program is described as ad-hoc, with no organizational risk objectives or tolerances defined. Due to the amount of regulation and oversight that credit unions have, it is unlikely that any successful credit union falls into the “Limited” category. However, in general, moving from “Limited” to “Fragmented” would basically entail addressing some of the core risks that all credit unions face and are required to address, i.e., ALM, Compliance and Business Continuity Plans (BCP). Some key steps in moving from “Limited” to “Fragmented” on the maturity model scale include:

- Educating the board and management on strong risk management practices.
- Performing a self-assessment.
- Implementing policies and procedures that measure and monitor key risks on an ongoing basis.

### **Fragmented**

Typically, in a “Fragmented” risk profile, the risk expertise is limited and primarily focused on ALM, BCP and Compliance. Risk tends to be handled (soloed) within individual business units. Overall, risk management is reactionary, and responses are procedural in nature. Although “Fragmented” is an improvement over “Limited”, it is still considered a weak risk management profile and efforts should be made to move up to the “Comprehensive” level.

There are several steps that can be taken in order to strengthen the credit union’s risk management profile. These primarily entail formalizing the risk management process by formulating an ERM vision, establishing a risk management committee, and appointing a risk officer. In addition, the credit union should create and analyze likelihood and impact assessments, establish appropriate risk tolerances for significant risk factors, and perform a risk assessment at least annually.

### **Comprehensive**

In a “Comprehensive” program, senior management and the board of directors have formalized the risk function, risk tolerances have been established, and there is a clear understanding of the risk management process across the organization. Most of the risk is measured in qualitative terms and is internal in nature with limited predictability. Credit unions with “Comprehensive” risk management programs have made conscious efforts to evolve their ERM culture and actively improve the ability to monitor and respond to the various risks facing them.

### **Integrated**

In order to have a truly strong ERM program, credit unions should look to move towards an “Integrated” model. As the name describes, risk management practices are integrated with the strategic plan and business decision-making. Risks are aggregated by risk type and incorporate both, qualitative and quantitative, risk measures. A key feature of an “Integrated” ERM program is that it is forward looking with established, predictive indicators.

### **Optimized**

When the ERM function is “Optimized,” it is used for predictive modeling and value creation through opportunity exploitation. Risk can be measured in terms of strategic benefit and bottom-line dollars. This is the model that brings value to the institution, not only by avoiding catastrophic events, but also by modeling and exploring new business lines that can generate increased revenue for the credit union and added value for the members. Credit unions that have “Optimized” the ERM function have truly institutionalized risk management within the organization.

## **CONCLUSION**

Risk is inherent in the operation of a credit union. Credit unions should not strive to eliminate risk, but rather, they should ensure that risk is identified and managed within risk tolerance levels. An Enterprise Risk Management program forms a bond and a common sharing of risk related information to provide a comprehensive view of risk across the organization. A successful ERM program requires involvement from all areas, beginning with the board of directors and filtering down throughout the credit union; in alignment with the overall strategic plan and organizational culture; and ensuring that organizational goals, strategies, and procedures are consistent with acceptable risk tolerances and appetite. As outlined, the credit union’s board of directors and senior management can begin this endeavor by assessing the credit union’s current state and determining its risk appetite.

Once the assessment has been completed and risk tolerances have been defined, the credit union must identify the current and emerging risks it faces. This is an ongoing process in a successful ERM program, which must be reported to senior management and the board of directors as defined within adopted policies.

While implementing an ERM program is a significant undertaking, the credit union’s rewards for taking calculated risks are stable profitability and increased net worth through avoiding excessive losses, minimizing earnings uncertainty, and a clearer understanding of the ramifications of short- and long-term decisions and strategies.

# GLOSSARY

**Compliance Risk**—The risk to earnings or capital arising from violations of, or conformance with, laws, rules, regulations, prescribed practices, internal policies and procedures, or ethical standards. Compliance risk may also arise in situations where ambiguous or untested laws or rules govern certain credit union products or activities of the members. Compliance risk exposes the credit union to fines, civil money penalties, payment of damages, and the voiding of contracts. Compliance risk can lead to a diminished reputation, limited opportunities, reduced field of membership expansion potential, and lack of contract enforceability. Compliance risk goes beyond a failure to comply with consumer protection laws. It encompasses all laws as well as prudent ethical standards, contractual obligations, and exposure to litigation.

**COSO**—The Committee of Sponsoring Organizations is a voluntary private-sector organization committed to guiding executive management and governance entities towards more effective, efficient and ethical business operations.

**Credit Risk**—The risk to earnings or capital arising from an obligor’s failure to meet terms of any contract with the credit union or otherwise fail to perform as agreed. Credit risk exists in all activities where the credit union invests or loans funds with expectation of repayment.

**Enterprise Risk Management (ERM)**—A process effected by the 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 the risk appetite, to provide reasonable assurance regarding the achievement of objectives. *Source: COSO –Enterprise Risk Management–Integrated Framework, 2004*

**Sample workable definition for credit unions:**

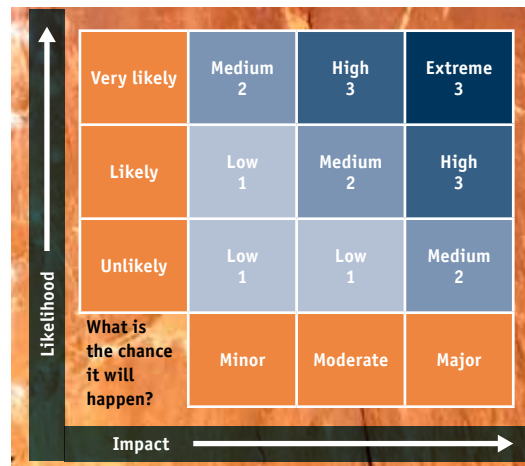
*Enterprise Risk Management (ERM) is a collaborative process to identify, manage and monitor organizational risks, both internal and external, so as to ensure achievement of the credit union’s strategic objectives and the credit union’s continued financial stability and viability.*

**ERM Dashboard**—A means of communicating a summary of the credit union’s top risks to directors and senior management. A risk dashboard may include the current measurement compared to prior measurements, the trend in the risk level, (e.g., increasing or decreasing), comparison to approved tolerance limits, and emerging risks that could impact the credit union.

**Heat/Risk Map**—A snapshot of the portfolio of identified risk in terms of severity and frequency of each exposed risk. A tool utilized to assess and evaluate risks based on the likelihood and impact of a process and/or event.

**Impact**—The result or effect of an event measured against earnings or net worth/capital.

**Inherent Risk**—The risk to a credit union in the absence of any actions management might take to alter either the risk’s likelihood or impact. The natural risk of a process or event can be calculated as the impact score multiplied by the likelihood score.



**Interest Rate Risk**—The risk that changes in market rates will adversely affect a credit union’s capital and earnings. Interest rate risk arises from: (1) difference between the timing of rate changes and the timing of cash flows (re-pricing risk); (2) changing rate relationships among different yield curves affecting credit union activities (basis risk); (3) changing rate relationships across the spectrum of maturities (yield curve risk); and (4) interest related options embedded in credit union products (options risk). Not only can a move in interest rates affect the price of investments, it can also have an effect on the value of the loan portfolio and on fee income. The assessment of interest rate risk should consider risk from both an accounting perspective (i.e., the effect on the credit union’s accrual earnings, including held-to-maturity and available-for-sale accounts) and the economic perspective (i.e., the effect on the market value, or net economic value, of the credit union’s loans and investments).

**Lagging Indicator**—Economic and financial market indicators that tend to change only after an economy has already changed or has begun to follow a particular pattern or trend. They trail behind (usually by six months) the overall economic cycle instead of moving with it (as coincident indicators do) or moving ahead of it (as leading indicators do). Major lagging indicators include the unemployment rate, outstanding consumer loans, outstanding business loans, business spending, business profits, book value of business inventories, unit labor costs, and consumer price index (CPI).

**Layered Risk**—The aggregate of individual risk factors or categories that expose the organization on the enterprise level. Risk based on the accumulated combination of risk factors.

**Leading Indicators**—Statistics that predict trends in the economy or a particular industry. For example, the number of



building permits issued is a leading indicator for the housing sector because permits must be obtained before building begins. A move in a leading indicator for one time period is often not meaningful; but a string of increases or decreases, especially in conjunction with confirming data, points to a recovery or downturn. The Index of Leading Economic Indicators, as published by The Conference Board, includes the following 10 Economic Indicators:

1. The interest rate spread between 10-year Treasury notes and the federal funds rate.
2. The inflation-adjusted M2 measure of the money supply.
3. The average manufacturing workweek.
4. Manufacturers' new orders for consumer goods and materials.
5. The S&P 500 measure of stock prices.
6. The vendor performance component of the NAPM index.
7. The average level of weekly initial claims for unemployment insurance.
8. Building permits.
9. The University of Michigan index of consumer expectations.
10. Manufacturers' new orders for nondefense capital goods.

**Likelihood**—The possibility that a given event will occur or how frequently an event may occur in a given time period.

**Liquidity Risk**—The risk to earnings or capital arising from a credit union's inability to meet its obligations when they come due, without incurring material costs or unacceptable losses. Liquidity risk includes the inability to manage funding sources, including unplanned decreases or changes. Liquidity risk also arises from the credit union's failure to recognize or address changes in market conditions that affect the ability to liquidate assets quickly and with minimal loss to value.

**Mitigation**—An organization's ability to lessen or "manage down" the impact or likelihood of a circumstance or event.

**Reputation Risk**—The risk to earnings or capital arising from negative public opinion or perception. Reputation risk affects the credit union's ability to establish new relationships or services, or to continue servicing existing relationships. This risk, which occurs in activities such as asset management decisions and transactions, can expose the credit union to litigation, financial loss or a decline in membership base. Reputation risk exposure appears throughout the credit union organization. The officials, management and staff must accept responsibility to exercise an abundance of caution in dealing with members and the community.

**Residual Risk**—The remaining risk after management has taken the action to alter the risk's likelihood or impact. The amount of risk that is unmitigated. It can be calculated as the inherent risk score multiplied by the effectiveness of response score.

**Risk**—The possibility that an event will occur and adversely affect the achievement of the objectives.

**Risk Appetite vs. Risk Tolerance**—Both risk appetite and risk tolerance set boundaries of how much risk a credit union

is prepared to accept. Risk appetite is the amount of risk, on a macro level, that an enterprise is willing to accept. Risk tolerances are the acceptable level of variation relative to the achievement of a specific objective. For example:

- **Risk Appetite**—Statement that the credit union does not accept risk that could result in significant fraud losses.
- **Risk Tolerance**—Statement that the credit union does not wish to accept risks that would cause credit card fraud losses to exceed 1% of ROA.

**Strategic Risk**—The risk to earnings or capital arising from poor or adverse management decisions, improper implementation of decisions, or lack of responsiveness to industry or environmental changes. This risk is a function of the compatibility of a credit union's strategic plan, the business strategies developed to achieve those goals, the resources deployed to accomplish these goals, and the quality of implementation. The tangible and intangible resources needed to carry out business strategies include communication channels, operations systems, delivery networks, monitoring systems, and managerial capacities and capabilities.

**Transaction Risk**—The risk to earnings or capital arising from fraud or error that results in an inability to deliver products or services, maintain a competitive position, and manage information. This risk is a function of internal controls, accounting systems, information/computer systems, employee integrity, and operations processes. This risk arises on a daily basis in all credit unions as they process transactions. This includes risk related to technology, which has both internal and external risks. Internal risks include data integrity, system availability, redundancy, volume volatility, and operational functionality to the credit union membership. External risks arise from the inability to protect membership data, disruption in e-commerce services, social engineering on credit union personnel, or an inadequate disaster recovery program.

# OTHER RESOURCES

**Some additional resources that are available to further expand knowledge related to ERM include:**

- North Carolina State University, College of Management, Enterprise Risk Management Initiative <http://mgt.ncsu.edu/erm>
- Committee of Sponsoring Organizations of the Treadway Commission (COSO) <http://www.coso.org/-ERM.htm>
- Risk & Insurance Management Society, Inc. <http://www.rims.org/resources/ERM/Pages/default.aspx>

# APPENDICES

## Appendix A

## Sample

### Enterprise Risk Management Self-Assessment Questionnaire

The following is a list of questions that can be presented to board and executive management to help stimulate meaningful discussion regarding the evaluation and assessment of where the credit union currently stands in the development of its enterprise risk management framework.

1. Who owns Enterprise Risk Management?
  - Who has overall responsibility and accountability for Enterprise Risk Management, according to the board? According to management?
  - Is the credit union positioned to accept that ERM responsibility lies with the board and its committees/delegates (overall risk management oversight) and management (risk ownership and mitigation/management)?
2. Is the risk appetite of the credit union defined?
  - What is the risk appetite of the credit union?
  - Is there alignment of board and management on risk appetite?
  - Is that clearly established and understood by the board and management?
3. Is ERM addressed in strategy setting for the credit union?
  - Is the credit union's willingness to accept and manage risk (risk appetite) used for guidance in strategic planning?
  - Does the strategic plan include risk management components?
4. What does ERM currently look like in the credit union?
  - What is the existing Enterprise Risk Management framework in the credit union to identify, prioritize, mitigate and monitor risks?
  - What are the components of that framework?
  - Does it meet the needs of the credit union to provide information necessary to effectively manage risks?
5. How does the board assess management's effectiveness in ERM?
  - Is there awareness by the board of the inherent risks in the strategic plan?
  - Does the board have sufficient information to be aware of current critical risks?
  - Does management keep the board apprised of emerging risks and significant changes in the risk outlook for the credit union?
  - Is the board aware of management responses? Are they in agreement with same?
6. How is the changing economic environment incorporated into ERM by board and management?
  - Is management developing metrics and analytics that incorporate external factors in ERM evaluation and prioritization?
  - Do board and management periodically conduct discussions and brainstorming of "what if" scenarios (occurrence of significant potential risk events, both positive and negative risk events) and possible responses?

## Appendix B

## Sample ERM Board Policy (1)

### Enterprise Risk Management Policy

The Board of Directors recognizes that one of THE CREDIT UNION's primary responsibilities is to manage the risk associated with the successful operation of a financial institution. This Enterprise Risk Management (ERM) Policy ensures that THE CREDIT UNION actively identifies inherent risk on an institution-wide basis, analyzes responses to mitigate these risks, reports risks to Senior Management and the Board, and incorporates risk analysis in all aspects of the planning process to include strategic planning, development of business initiatives, and implementation of new products, systems and procedures.

The Board authorizes the President to appoint the individual or department responsible for the ongoing ERM process at THE CREDIT UNION. Responsibilities of the individual(s) or department include, but are not limited to:

- Conduct an institution-wide risk assessment no less frequently than annually.
- Conduct regularly scheduled meetings with the key personnel to identify potential changes in THE CREDIT UNION'S risk vulnerabilities.
- Provide information uncovered throughout the ERM process to be included in THE CREDIT UNION'S Strategic Planning Process
- Conduct ongoing ERM Training for those individuals with ERM responsibilities and to all staff for the general understanding of the ERM process.
- THE CREDIT UNION'S Board of Directors will be trained, on no less than an annual basis, on chosen ERM topics specific to strategic initiatives and related risk.

## Appendix C

## Sample ERM Committee Charter

### Enterprise Risk Management Committee Charter

#### *Objectives*

The Enterprise Risk Management (ERM) Committee is responsible for establishing and maintaining a comprehensive Risk Management System for identifying, assessing and managing risk to assist the Leadership Team (LT) in managing risk with reasonable assurance in a rapidly changing environment.

In this regard, the specific objectives for the Committee include ensuring that:

- The LT and business unit management understand and accept their responsibility for identifying, assessing, reporting and managing risk.
- The LT and business unit management are strategically focused on enterprise-wide risk management.
- Processes and procedures are provided to the business units to facilitate achievement of their risk management responsibilities related to the risks identified and prioritized by the Committee.
- A framework is provided to business unit management to assess and manage risks which are not included in the scope of the ERM Committee, such as transaction risks and control risks.
- Risk assessments are performed periodically.
- Risk mitigation activities are successful in:
  - o Safeguarding assets.
  - o Maintaining appropriate standards regarding the environment and health and safety issues.
  - o Meeting legal and regulatory obligations.
  - o Reinforcing the values of the organization by focusing on member needs.
  - o Supporting the credit union in achieving its strategic plan and long-range desired results.

#### *Responsibilities*

The Committee's responsibilities include the following:

- Overall responsibility for the Enterprise Risk Management process, including developing and implementing the processes and procedures to identify, assess, respond to and report on the most significant risks identified in the risk assessment process.

- Ensure proper risk management by recommending to the Executive Leadership Team (ELT) ownership, roles, responsibilities and accountabilities related to risk management.
- Promote the Enterprise Risk Management model to the LT and educate them on the enterprise risk management process.
- Work with business units on monitoring and reporting to ensure compliance with the credit union's standards and reporting of the risks identified and prioritized by the Committee, as well as those risks which are not included in the scope of the ERM Committee.
- Report to the ELT and the Board of Directors regarding the:
  - o Progression of enterprise risk management and its implementation.
  - o Identified significant and material risk exposures across the credit union.
  - o Consolidated enterprise risk management plan encompassing analysis and recommendations.
- Request budget dollars for consulting, training, software, or other expenses determined necessary.

### ***Materiality and Focus***

The Committee is charged with ensuring that the competency for identifying, assessing and managing risk continues to evolve. To that end, it will focus primarily on the implementation and effectiveness of enterprise risk management.

The Committee should review those risks that may be deemed material through agreement between the Committee and Executive Leadership Team. Materiality considerations will be both qualitative and quantitative based upon both immediate and long-term exposure to the credit union.

The goal of the Committee is to encourage broader thinking by management in relation to risks so that greater focus is applied to continual evolution of the organization's competencies related to risk management.

### ***Structure***

The committee will consist of at least one Vice President from each division within the credit union as well as the Chief Financial Officer who will serve as the Executive Leadership Team liaison to the committee.

### ***Management Responsibilities with Enterprise Risk Management***

Heads of business units, business processes and functional departments are responsible for identifying, assessing, reporting and responding to risk relative to meeting the unit's objectives based on guidance from the ERM Committee. They ensure that processes utilized are in compliance with the entity's enterprise risk management practices and procedures and that their unit's activities are within established risk tolerance levels.

The Executive Leadership Team and Board of Directors are responsible for developing and refining the enterprise-wide appetite/tolerance for risk.

Appendix D

Sample Risk Assessment Rating System

Qualitative to Quantitative Conversion Factors

What is the magnitude of the risk exposure?

| Impact Rating | Description   | From        |             | To          |             | Drop-Down List Name |          | % of \$100M in Assets |          | % of \$10M in Capital |          |
|---------------|---|-------------|-------------|-------------|-------------|---------------------|----------|-----------------------|----------|-----------------------|----------|
|               |   | From        | To          | From        | To          | From                | To       | From                  | To       | From                  | To       |
| 5             | Catastrophic - Generally arising from an event out of CU control as CU does not intentionally assume this level of risk. Might result from a natural disaster or other "once-in-a-lifetime" event. Realization could impair CU's ongoing existence, jeopardize capital adequacy, and require extensive strategic changes. | \$1,000,000 | Infinity    | Infinity    | Infinity    | 5 - Catastrophic    | Infinity | 1.0000%               | Infinity | 10.0000%              | Infinity |
| 4             | Major - Largest risks CU knowingly assumes. Would have a major impact on profitability for a year but not jeopardize its capital position.  | \$500,000   | \$1,000,000 | \$1,000,000 | \$1,000,000 | 4 - Major           | 0.0500%  | 0.5000%               | 0.0500%  | 5.0000%               | 0.5882%  |
| 3             | Moderate - Significant risks that CU elects to assume, given effective responses. CU might expect to incur at least one of these losses each year. Would have a noticeable but not devastating impact on annual profitability and a relatively small impact on capital adequacy.  | \$100,000   | \$500,000   | \$500,000   | \$500,000   | 3 - Moderate        | 0.0250%  | 0.1000%               | 0.0250%  | 1.0000%               | 0.2941%  |
| 2             | Minor - CU realizes several losses in this category every year in the normal course of business.  | \$25,000    | \$100,000   | \$100,000   | \$100,000   | 2 - Minor           | 0.0050%  | 0.0250%               | 0.0050%  | 0.2500%               | 0.0588%  |
| 1             | Insignificant - This type of exposure is a part of normal business operations. CU incurs many losses in this category every year.   | -           | \$25,000    | \$25,000    | \$25,000    | 1 - Insignificant   | 0.0013%  | 0.0000%               | 0.0013%  | 0.0000%               | 0.0147%  |

How likely is the event to occur without the risk responses?

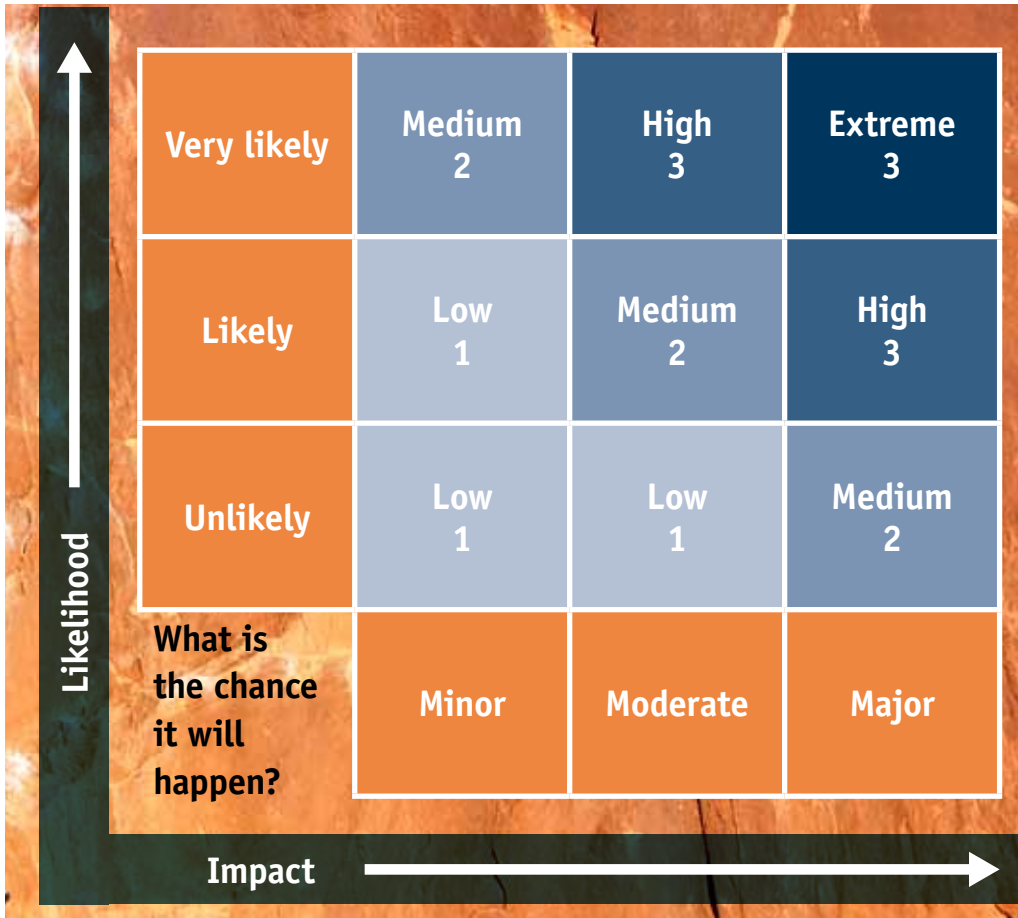
| Likelihood Rating | Description    | From | To   | Drop-Down List Name     |
|-------------------|----------------|------|------|-------------------------|
| 5                 | Almost Certain | 99%  | 100% | 1 - Extremely Effective |
| 4                 | Likely         | 95%  | 99%  | 2 - Very Effective      |
| 3                 | Possible       | 80%  | 95%  | 3 - Effective           |
| 2                 | Unlikely       | 60%  | 80%  | 4 - Somewhat Effective  |
| 1                 | Rare           | 0%   | 60%  | 5 - Ineffective         |

How effective are responses in reducing the impact or likelihood?

| Response Effectiveness Rating | Description         | From | To   | Drop-Down List Name     |
|-------------------------------|---------------------|------|------|-------------------------|
| 5                             | Extremely Effective | 99%  | 100% | 1 - Extremely Effective |
| 4                             | Very Effective      | 95%  | 99%  | 2 - Very Effective      |
| 3                             | Effective           | 80%  | 95%  | 3 - Effective           |
| 2                             | Somewhat Effective  | 60%  | 80%  | 4 - Somewhat Effective  |
| 1                             | Ineffective         | 0%   | 60%  | 5 - Ineffective         |

## Appendix E

## Sample Risk/Heat Map



## Appendix F

## Sample Risk Matrix for Monitoring/Reporting

### GUIDANCE

#### **Risks:**

- Identify current risks inherent in the balance sheet
- Identify various functional areas of the credit union
- Identify activity based risks
- Rate the unmitigated risks as High, Medium or Low
- Identify the mitigation efforts
- Measure the residual risk after mitigation efforts
- Track risks over defined periods in time

#### **Measures:**

- Complete this process for each risk identified
- Identify why issue is a potential risk
- Identify leading indicators that may affect risk
- Determine additional mitigation steps (if appropriate)
- Assign responsibility and timeframe for completion












## Appendix F (Page 3)


| Credit Risk                                |  |                        |                             |                        |                       |
|--|--|------------------------|-----------------------------|------------------------|-----------------------|
| <b>Description of risk</b>                 | Real estate Loan Portfolio is greater than 300% of net worth   |                        |                             |                        |                       |
| <b>Background</b>                          | Current conomic crisis has contributed greatly to increased delinquency and declining property values. Charge off ratio is expected to double over the next 12 months. Unemployment is increasing. |                        |                             |                        |                       |
|  | <b>Unmitigated Risk Factors</b>  |                        |                             |                        |                       |
|  | High Percentage of balance sheet in Real Estate Loans  |                        |                             |                        |                       |
|  | Real Estate values have declined 10%   |                        |                             |                        |                       |
|  | LTV's were 95% at origination  |                        |                             |                        |                       |
|  | Delinquency has increased to 3%  |                        |                             |                        |                       |
|  | Charge-Offs have increased to .5%  |                        |                             |                        |                       |
|  | <b>Mitigation</b>  |                        |                             |                        |                       |
|  | Aggressive collection practices  |                        |                             |                        |                       |
|  | Workout loan program   |                        |                             |                        |                       |
|  | Mortgage Insurance   |                        |                             |                        |                       |
|  | <b>Current Period</b>  | <b>Previous Period</b> | <b>Prior Year</b>           | <b>Trend Direction</b> |                       |
| <b>Net Worth</b>                           | \$1,500,000  | \$1,600,000            | \$1,700,000                 | ↓                      |                       |
| <b>Net Worth at risk before mitigation</b> | \$500,000  | \$450,000              | \$400,000                   | ↑                      |                       |
| <b>Impact of mitigation</b>                | \$100,000  | \$100,000              | \$100,000                   |                        |                       |
| <b>Net Worth at risk</b>                   | \$400,000  | \$350,000              | \$300,000                   | ↑                      |                       |
| <b>Net Worth not at risk</b>               | \$1,100,000  | \$1,250,000            | \$1,400,000                 | ↓                      |                       |
|  | <b>Insignificant</b>   | <b>Minor</b>           | <b>Moderate</b>             | <b>Major</b>           | <b>Critical</b>       |
| <b>Current Impact on Credit Union</b>      |  |                        | ✓                           |                        |                       |
|  | <b>Large Decrease</b>  | <b>Decreasing</b>      | <b>Stable</b>               | <b>Increasing</b>      | <b>Large Increase</b> |
| <b>Direction of Risk</b>                   |  |                        |                             | ✓                      |                       |
| <b>Additional Steps</b>                    | <b>Change Policy to limit LTV to 75%</b>   |                        |                             |                        |                       |
|  | Business Owner   | VP of Lending          | Due Date: December 31, 2010 |                        |                       |

Appendix G

Sample Seven Risk Domains Dashboard

| Credit Union  |  | ↑ Increasing           | } Direction of Risk Trends |              |                      |                                |
|---|--|------------------------|----------------------------|--------------|----------------------|--------------------------------|
| Seven Key Risks Area Dashboard  |  | ↓ Declining            |                            |              |                      |                                |
| June 30, 2010   |  | → Neutral              |                            |              |                      |                                |
|   | Risk Rating  | Current Quarter        | Previous Quarter           | One Year Ago | Trends in Risk Level | Comments and Policy Guidelines |
| <b>Credit Risk</b>  |  |                        |                            |              |                      |                                |
| <b>Delinquency (61+)</b>  | <br>Green   |                        |                            |              |                      |                                |
| <b>Mortgage Loan Portfolio - Median LTV</b>   |  |                        |                            |              |                      |                                |
| <b>Mortgage Loan Portfolio - Median FICO</b>  |  |                        |                            |              |                      |                                |
| <b>Interest Rate Risk</b>   |  |                        |                            |              |                      |                                |
| <b>NEV Ratio</b>  | <br>Green   |                        |                            |              |                      |                                |
| » Base Case   |  |                        |                            |              |                      |                                |
| » Shock up 300bp Scenario   |  |                        |                            |              |                      |                                |
| <b>NEV-%-Change in Shock up 300bp Scenario</b>  |  |                        |                            |              |                      |                                |
| <b>NII-%-Change in Shock up 300bp Scenario</b>  |  |                        |                            |              |                      |                                |
| <b>Liquidity Risk</b>   |  |                        |                            |              |                      |                                |
| » Loans to Assets   | <br>Green  |                        |                            |              |                      |                                |
| » Cash + Short Term Investments/Assets  |  |                        |                            |              |                      |                                |
| » Reg Shares + Share Drafts/Total Shares + Borrowings   |  |                        |                            |              |                      |                                |
| » Investments to Assets Ratio   |  |                        |                            |              |                      |                                |
| » Total Available Credit  |  |                        |                            |              |                      |                                |
| <b>Transaction Risk</b>   |  |                        |                            |              |                      |                                |
| <b>SAR Filings</b>  | <br>Green | <b>Number Filed</b>    |                            |              |                      |                                |
|   |  | <b>\$ Amount Filed</b> |                            |              |                      |                                |
| <b>Confirmed Fraud Cases (Non-Card)</b>   |  | <b>Number Filed</b>    |                            |              |                      |                                |
|   |  | <b>\$ Amount Filed</b> |                            |              |                      |                                |
| <b>Confirmed Card Fraud Cases</b>   |  | <b>Number Filed</b>    |                            |              |                      |                                |
|   |  | <b>\$ Amount Filed</b> |                            |              |                      |                                |
| <b>IT System Intrusion Attempts</b>   |  |                        |                            |              |                      |                                |
| <b>Compliance Risk</b>  |  |                        |                            |              |                      |                                |
| <b>CAMEL/Regulatory Examination Rating</b>  | <br>Green |                        |                            |              |                      |                                |
| <b>Current Regulatory Hot Spots:</b>  |  |                        |                            |              |                      |                                |
| » Misc Regulatory Updates   |  | Narrative Summary      |                            |              |                      |                                |
| » Legislation   | Narrative Summary  |                        |                            |              |                      |                                |
| <b>Strategic Risk</b>   |  |                        |                            |              |                      |                                |
| Strategic risk is the risk from poor or adverse business decisions, improper implementation of business decisions or lack of responsiveness to industry or environmental changes. | <br>Green |                        |                            |              |                      |                                |
| <b>Reputation Risk</b>  |  |                        |                            |              |                      |                                |
| <b>Member Service Quality - Overall Satisfaction Score</b>  | <br>Green |                        |                            |              |                      |                                |
| <b>Bauer Financial, Inc. - Rating</b>   |  |                        |                            |              |                      |                                |

|             |        |                              |
|-------------|--------|------------------------------|
| Risk Rating | Green  | Overall Low Level of Risk    |
|             | Yellow | Overall Medium Level of Risk |
|             | Red    | Overall High Level of Risk   |



**Enterprise Risk Management**  
An Approach to Implementation in Credit Unions