

# Credit Union Enterprise Risk Management: Building an Effective Foundation

By Mark Prentice  
Vice President of Products, Vital Insight



“I take risk management very seriously and believe that risks should be managed, not avoided. Implemented successfully, ERM enables management to effectively deal with uncertainty and associated risks,”<sup>B</sup>

**Rodney E. Hood**  
**Vice Chairman**  
**National Credit Union**  
**Administration (NCUA)**

## Summary

Understanding and managing risk has long been a fundamental principle for all financial services organizations, including Credit Unions. Until recently risk management was primarily viewed and managed in organizational silos, without fully incorporating or understanding the interconnectivity and impact risks have throughout an enterprise. Recent events including corporate scandals, government intervention, and the Corporate Credit Union Stabilization efforts are advancing the concepts of ERM. ERM is being adopted as not simply a principle, but a fundamental strategic and operational part of a viable and successful business. Credit Unions executives are becoming acutely aware of the importance of ERM.

ERM is now a hot topic among Credit Unions, but continual questions arise regarding definition, implementation, and execution. Although underlying ERM components (e.g., identifying risks, managing risks) have been part of many Credit Unions for a long time, the integration of these components into frameworks and programs often seems like a daunting task. While ERM program execution should be tailored to the organization’s strategy and objectives, all ERM programs should follow a set of defined phases.

There are a number of ERM frameworks that help define the components and phases of an ERM program. The COSO ERM Framework<sup>A</sup>, for example, outlines ERM components needed to achieve business objectives. While frameworks are important for summarizing high level objectives, organizations struggle to answer the question – “What do I do now?”

In this paper, we will use Vital Insight’s Five Phases to Effective ERM<sup>®</sup> as a guide to the overall ERM program (see figure F1), and focus specifically on the phases that integrate ERM functions into the existing organizational foundation. Although all of the phases are important to establishing an effective ERM program, this paper primarily focuses on the first phase entitled “Understand Your Business”.

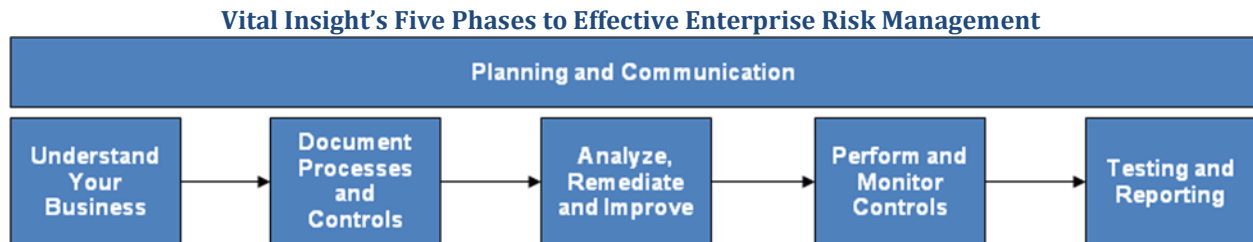
---

## Contents

- I. Five Phases to Effective Enterprise Risk Management (ERM)**
- II. Phase 1 Understand Your Business: Laying the Foundation**
  - a. Step 1 – Initial Planning**
  - b. Step 2 – Define the Organization**
  - c. Step 3 – Assess Risk (Process Prioritization)**
  - d. Step 4 – Prioritize Risk Events**
- III. Conclusion**

## Five Phases to Effective Enterprise Risk Management

Vital Insight's Five Phase approach to ERM defines the high level phases for implementing an ERM program. This approach assumes that certain activities are already in place (e.g., management's understanding of the business, performance and monitoring of controls), while others (e.g., risk assessments, establishing risk tolerances) are new or require refinement. The five phase approach also assumes that ERM is an integrated function requiring resources from many business areas (e.g., ERM professionals, Internal Audit, Business Process Owners).



### Phase 1 Understand Your Business: Laying the Foundation

The Understand Your Business Phase is the most important phase in the ERM program. During this phase, Organizations define the ERM environment, prioritize processes, perform risk assessments, and analyze risk. Unlike the other phases in the five phase approach, the Understand Your Business phase introduces concepts and activities new to many organizations (e.g., Risk Assessments). All other phases in the five phase approach are based on concepts and activities already resident in many organizations (e.g., process documentation, control testing). The Understand Your Business phase is made up of four steps, including Initial Planning, Defining the Organization, Assessing Risk, and Evaluating Risk Events.

#### Step 1 – Initial Planning

The Initial Planning step is the most important step of an effective ERM program. Proper planning will help ensure that the tone at the top is set, appropriate policies are put in place, and resources are aligned. Unlike some of the other steps, planning will continue throughout the program. The activities discussed in the Initial Planning step below are primarily activities used to effectively begin the program.

##### Objectives:

1. Determine the State of Current ERM Program
2. Determine the Scope of the ERM Program
3. Establish ERM Objectives and Policies
4. Develop a Timeline for Implementing or Enhancing the ERM Program
5. Define Roles and Responsibilities

Who: Project Sponsor, Key Management Personnel

##### Key Activities:

1. Determine State of the Current ERM Program.
  - Profile the current state of the organization as it relates to risk management activities
  - Review current risk and compliance programs and approaches (e.g., Internal Audit, Regulatory Compliance)
  - Analyze metrics that currently support, or could support risk management (e.g., historic risk exposure, regulatory issues)

## Credit Union Enterprise Risk Management: Building an Effective Foundation

- Determine whether risk management processes are in place due to external regulator (e.g., NCUA) influence
  - What efforts have been performed to date, both at the enterprise and departmental levels?
2. Determine the Scope of the ERM Program
    - Analyze and prioritize business areas based on available metrics (e.g., revenue, expense, head count, historic risk exposure, regulatory issues)
    - Identify business areas that may contain high risk
    - Based on previous internal and external reviews, determine the internal controls maturity in prioritized business areas
  3. Establish ERM Objectives and Policies
    - Develop a business case for ERM that defines measurable benefits to the organization
    - Review current policies to support the ERM program (e.g., Internal Audit Policies, Regulatory Policies)
    - Prepare changes to existing policies and identify new policies to develop
  4. Develop a Timeline for Implementing or Enhancing the ERM Program
    - Determine a timeline for implementing changes to the existing program or establishing a new program
    - Develop a software implementation timeline that meets existing operational guidelines
    - Establish educational programs and timelines (e.g., How to Implement Effective ERM Programs, Benefits of ERM, Adjusting to Change with ERM)
    - Develop reporting framework, including contents, audience, and release timelines
  5. Define Roles and Responsibilities
    - Evaluate necessary roles in the ERM program (e.g., stakeholders, risk managers, system managers)
    - Identify ERM program stakeholders
    - Determine whether cross-functional teams are needed to share information across the organization (e.g., Internal Audit, Regulatory Compliance)
    - Develop and assign roles to individuals and groups in the organization

### Step 2 – Define the Organization

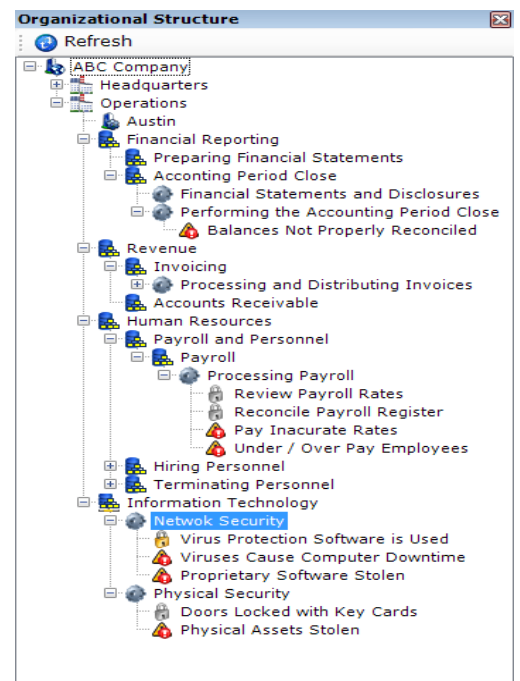
The Organization definition step focuses on compiling key information about the state of the organization and defining an Organizational Structure. Organizational Structure design is a continuous process. Design, management, and maintenance of a complex Organizational Structure are enhanced by using a software product to manage documentation, change management, and security.

#### Objectives:

1. Prepare Organizational-level Documents
2. Document Policies and Standards
3. Build the Initial Organizational Structure
4. Refine the Organizational Structure (continuous)
5. Integrate Internal Control Information

Who: Project Sponsor, ERM Lead/Staff, Internal Audit Lead/Staff, Process Owners

Ex. Organizational Structure



## Credit Union Enterprise Risk Management: Building an Effective Foundation

---

### Key Activities:

#### 1. Prepare Organizational-level Documents

- Review existing documents and identify gaps<sup>1</sup>
- Update existing documents and develop new documents (if current documents do not exist)

<sup>1</sup>There are many documents that include important organizational information. Some example documents may include:

- Organizational Charts
- Business Impact Analyses
- Business Continuity Plans
- Policy and Procedure Table of Contents
- Annual Internal Audit Planning/Scoping Documents

#### 2. Document Policies and Standards

- Identify and obtain all existing organization standards and policies (includes control objectives the organization wants to operate against)
- Define specific dates for creation, issuance, and review intervals can be added if desired
- Identify policy owners, if desired

#### 3. Build the Initial Organizational Structure (preferably developed using a software package)

- Identify key business areas (e.g., Business Units, Lines of Business)<sup>2</sup>
- Identify business cycles/functional areas<sup>2</sup>
- Identify business processes<sup>2</sup>
- Prepare hierarchal structure of the Organizational Structure components
- Assign ownership for all Organizational Structure components
- Obtain stakeholder approval for initial design

<sup>2</sup>Use existing data from internal and external sources if available (e.g., Internal Audit, NCUA Reviews)

#### 4. Refine the Organizational Structure

- Define change control mechanisms for identifying, preparing, and approving changes
- Identify gaps in the Organizational Structure
- Continued Organizational Structure refinement
- Ensure all changes are properly reviewed and approved

#### 5. Integrate Internal Control Information

- Identify and gather all existing Process, Control and Risk information
- Map Controls to applicable Processes in the Organizational Structure
- Associate Controls to Control Objectives (if available)
- Associate Controls to Risk Events to track mitigation (where available)
- Review resulting Organizational Structure data (use outputs from software packages if available)

### **Step 3 – Assess Risk (Process Prioritization)**

The Assess Risk step is used to help prioritize business processes using a combination of operational and financial indicators. The resulting operational and financial assessment results provide business process prioritization, and help guide the scope of the ERM Program.

### Objectives:

1. Establish Risk Tolerances
2. Collect Data

## Credit Union Enterprise Risk Management: Building an Effective Foundation

3. Define Risk Factors / Indicators
4. Perform Process Risk Indicator Analysis
5. Perform Financial Account Risk Assessment
6. Evaluate and Report Assessment Results

Who: Project Sponsor, ERM Lead, Management

Key Activities:

1. Establish Risk Tolerances
  - Review existing audit reports (internal, external, regulatory) and policy information providing guidance on tolerances
  - Develop operational tolerances to determine what constitutes High, Medium, and Low risk
  - Determine financial account tolerances and metrics (e.g., materiality levels)
  - Document and obtain management approval on defined tolerances
2. Collect Data
  - Develop and distribute risk questionnaires
  - Conduct group sessions
  - Review existing internal and external audit reports (e.g., NCUA)

NOTE: There are a number of methods to collect risk information (e.g., surveys, group working sessions, one-on-one and group interviews). Certain methods work better for different organizations. Soliciting anonymous feedback could also be a method to use for data collection.

3. Define Risk Factors / Indicators
  - Evaluate existing reports and policies on operational indicators (e.g, NCUA Risk Categories)
  - Define the risk indicators for performing operational risk assessments
  - Review and obtain management approval of risk indicators

### Example Risk Factor Assessment

Summary | Perform Risk Assessment | Configuration

<Back to Process Selection

#### Process Risk Factor Assessment

Selected Processes For Information Technology

- Physical Security
- Network Security

p-1523ac - Physical Security

Summary:

Assessed Rating: **8(8.0)**

Process Categories:

Process Weight:

Weighted Rating: **40(40.0)**

Select	Name	RiskTypeName	Likelihood	Impact	RiskRating	RiskM
<input checked="" type="checkbox"/>	Regulatory	None	H(3)	H(3)	H(9)	2
<input checked="" type="checkbox"/>	Compliance	SAS 104-112	H(3)	M(2)	M(6)	1

Print Export

Save Save and Next

4. Perform Process Risk Indicator Analysis (perform using that data collected in activity 2 above)
  - Assign risk indicators to business processes
  - Configure risk indicators with likelihood and impact ratings
  - Weight risk indicators in relation to other indicators for each process (optional)
  - Weight business processes in relation to others (optional)

## Credit Union Enterprise Risk Management: Building an Effective Foundation

### 5. Perform Financial Account Risk Assessment

- Determine appropriate level for Financial Account Risk Assessment (e.g., Financial Statement line item)
- Identify materiality base(s) for calculating account materiality
- Assign materiality bases and subjective factor ratings to each financial account<sup>3</sup>

<sup>3</sup>Factor ratings are assigned at the account level defined for the assessment (e.g., Financial Statement line item)

#### Example Account Risk Assessment

Account Name	Account ID	Balance	Risk Rating
Service Revenue	SERVICE_REVENUE	\$300,000.00	Medium
Equipment Revenue	EQUIPMENT_REVENUE	\$150,000.00	High
Interest Revenue	INTEREST_REVENUE	\$50,000.00	Medium
Equipment Expense	EQUIPMENT_EXPENSE	\$100,000.00	Low
Service Expense	SERVICE_EXPENSE	\$200,000.00	Medium
Sales Expense	SALES_EXPENSE	\$85,000.00	Low
Overhead	OVERHEAD	\$40,000.00	Low
Income Tax Expense	INCOME_TAX_EXPENSE	\$25,000.00	Medium
Bad Debt Expense	BAD_DEBT	\$10,000.00	High
Cash	CASH	\$350,000.00	Medium
Accounts Receivable	ACCOUNTS_RECEIVABLE	\$150,000.00	High
Inventory	INVENTORY	\$275,000.00	High
Prepaid Expenses	PREPAID_EXPENSES	\$40,000.00	Low
Other Current Assets	OTHER_CURRENT_ASSETS	\$35,000.00	Medium
Property Plant and Equipment	PPE	\$120,000.00	Medium
Accumulated Depreciation	ACCUMULATED_DEPRECIATION	\$5,000.00	Low
Goodwill	GOODWILL	\$20,000.00	Medium
Other Intangible Assets	OTHER_INTANGIBLE_ASSETS	\$5,000.00	Medium
Accounts Payable	ACCOUNTS_PAYABLE	\$250,000.00	Medium
Short Term Tax Liabilities	SHORT_TERM_TAX_LIABILITIES	\$20,000.00	Low
Other Current Liabilities	OTHER_CURRENT_LIABILITIES	\$10,000.00	Medium

### 6. Evaluate and Report Assessment Results

- Compile Operational and Account assessment results
- Perform analysis to identify and review high risk business areas
- Begin initial recommendations on how to mitigate/reduce high risk areas
- Prepare management level reports

## Step 4 – Evaluate Risk Events

The Evaluate Risk Events step identifies the actual risks in the Organization. The identified risks are aligned in the Organization with business units, cycles, and processes. The resulting risk events are configured to provide Inherent and Residual ratings that are managed and reported on.

#### Objectives:

1. Identify Risk Events
2. Align Risk Events
3. Configure Risk Events

Who: Project Sponsor, ERM Lead, Management

#### Key Activities:

1. Identify Risk Events
  - Determine whether there are existing events identified in the Organization (e.g., Internal Audit, Regulatory Reviews)

## Credit Union Enterprise Risk Management: Building an Effective Foundation

- Using the results in step 3 – Assess Risk, evaluate High risk process areas and identify risk events that exist in these areas first (Medium and even Low rated areas may have Risk Events) <sup>4</sup>
- Perform gap analysis to determine if high assessed processes do not have risk events identified.

<sup>4</sup>Organizations will determine (based on established risk tolerances) what assessment levels (e.g., High, Medium) constitute higher risk. Processes with an Assessment rating of High should contain Risk Events. In cases where processes are assessed High and no Risk Events are identified, the assessment should be reevaluated.

2. Align Risk Events
  - Associate Risk Events with Organizational Structure components (e.g., Business Units, Functional Areas, Processes)
  - Identify areas where the same Risk Event(s) exist in multiple areas in the Organizational Structure
3. Configure Risk Events
  - Review each Risk Event and configure Inherent Likelihood and Impact ratings

### Example Risk Event Assessment

The screenshot shows a 'Modify Risk' window with the following fields:

Section	Field	Value
Inherent Risk	Likelihood	Medium (2)
	Impact	Medium (2)
	Overall Inherent Risk	M(4)
	Risk Decision	Mitigate
Residual Risk	Reduction Likelihood	1
	Reduction Impact	0
	Residual Likelihood	L(1)
	Residual Impact	M(2)
Overall Residual Risk	L(2)	

Residual Risk Comment: Risk Mitigated by controls defined in the Payroll Master File Review Process.

## Conclusion

ERM is an organizational-wide program requiring many business areas to adapt, and sometimes change. Implementing an effective ERM program requires top-level management buy-in/direction, diligent planning, coordination, and execution. Although implementing ERM requires significant time and resources, organizations can make the process less daunting by using a well thought out phased approach. Using an approach similar to the one described in this document provides a foundation for a long-standing, successful, and effective ERM program.

There are many benefits to implementing an effective ERM program. The primary benefit of an effective ERM program is empowering management with an understanding of the organization's risks, and allowing management to make informed, proactive decisions when dealing with impending risks. Additional benefits include:

- Reducing internal and external audit and regulatory costs by deploying an integrated and shared approach to risks management
- Helping to identify operational improvements by detecting and removing redundant processes and/or controls
- Consolidating and managing risk, process, and control information centrally allowing management to fully understand organizational components and risks
- Helping organizations align risk appetite with strategic and operational objectives
- Enhanced decision making by being able to take into account potential risk impacts
- Improving risk response time by having an understanding of impact and a defined plan for remediating risks

To learn more about us and how we can help you, please call (888) 618-4825, or visit us online at [www.vitalinsight.com](http://www.vitalinsight.com).

## References

**A. According to COSO (<http://www.coso.org>)**

**Enterprise Risk Management — Integrated Framework (2004)**

In response to a need for principles-based guidance to help entities design and implement effective enterprise-wide approaches to risk management, COSO issued the Enterprise Risk Management – Integrated Framework in 2004. This framework defines essential enterprise risk management components, discusses key ERM principles and concepts, suggests a common ERM language, and provides clear direction and guidance for enterprise risk management. The guidance introduces an enterprise-wide approach to risk management as well as concepts such as: risk appetite, risk tolerance, portfolio view. This framework is now being used by organizations around the world to design and implement effective ERM processes.

**B. NCUA Media Advisory, February 20<sup>th</sup>, 2009**

Vice Chairman Hood Continues to Promote Risk Mitigation During His 2009 Risk Mitigation Summit.  
[http://www.ncua.gov/news/press\\_releases/2009/MA09-0223.htm](http://www.ncua.gov/news/press_releases/2009/MA09-0223.htm)