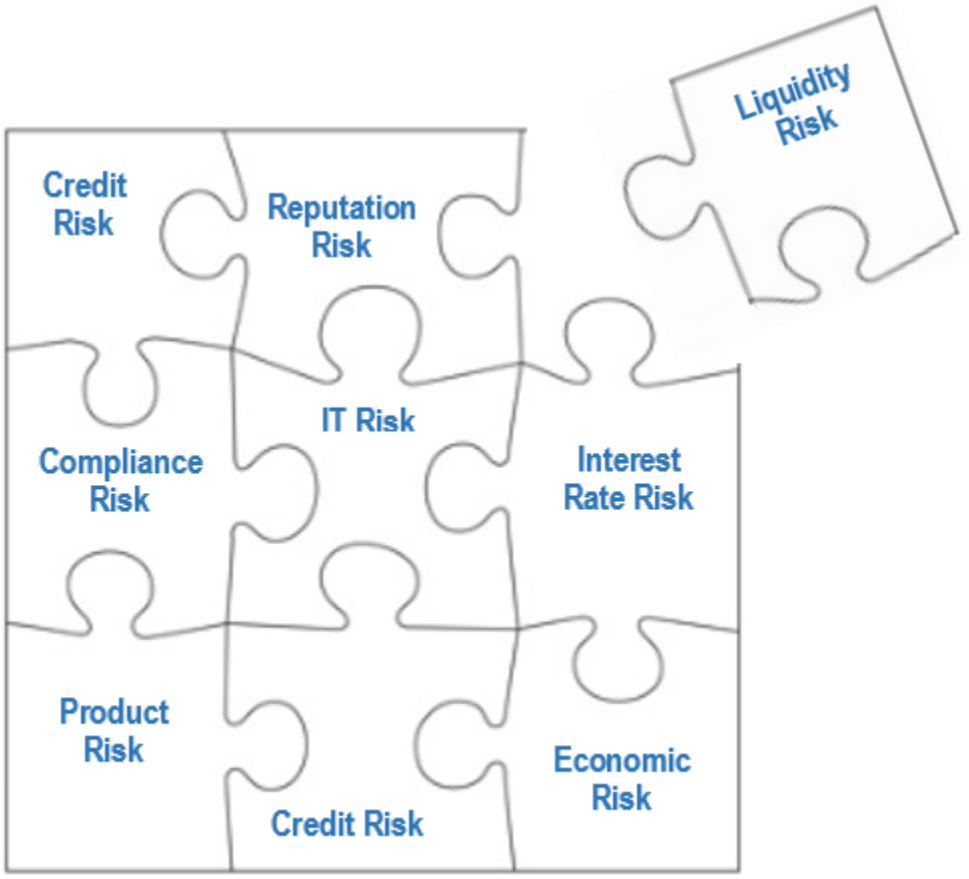
Enterprise Risk Management: A Staged Approach

A Second Pillar Consulting White Paper

Table of Contents

1 Introduction

Developing and implementing an Enterprise Risk Management Program can be like putting together a jigsaw puzzle. Leave out one piece of the puzzle and your picture of risk is incomplete.



1.1 What is Enterprise Risk Management

Enterprise Risk Management (ERM) is the process of putting together the risk puzzle – with all the pieces in place to give you a whole, connected view of risk. According to the Committee of Sponsoring Organizations (COSO), is ERM is "a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."[1] Simply put, ERM is a business strategy that identifies and manages risk as an interrelated portfolio.

Every organization, customer, product, business environment, and transaction has risk that can affect shareholder value.

[1] http://www.coso.org/documents/coso_erm_executivesummary.pdf

1.2 What makes for a good ERM Program?

Though risk cannot be eliminated, it can be defined. This knowledge allows risk to be managed at an acceptable level, which can grow stakeholder value.

All ERM Programs are not created equal. Under best practices, an ERM Program relies on sound risk assessment, risk mitigation, and risk monitoring practices. Because organizations constantly change, it is also important to develop an ERM Program that evolves over time to continually fit the needs of the organization. Ideally, an effective ERM Program cycles with business patterns, as well as changes in the business environment to enable organizations to respond to risks as they arise or change. An effective ERM Program is guided by the principles of COSO and the Risk Management Association (RMA), but specifically tailored to each unique organization.

With these criteria in mind, this white paper discusses:

- Unique ERM Challenges
- A Staged Approach to Implementation
- A Solution for Assistance in Implementation through Second Pillar Consulting

2 Unique ERM Challenges

2.1 Risks Evolve: Risk is ever-present and ever changing.

ERM cannot be approached as a one-time snapshot of risk. An organization, its environment, and the nature of risks all evolve. Thus, effective ERM must be customized to an organization over time. Creating and maintaining a **Risk Inventory** and **Risk Hierarchy** that identify and prioritize risks are crucial components of a successful ERM Program. The Risk Inventory and Risk Hierarchy allow organizations to consistently identify and measure risk and adjust business practices to reflect changes in risk.

Markets move continuously, competitors innovate, technology progresses, and risks change. Organizations need a consistent approach for tracking and prioritizing risks to be able to respond quickly to changes. Using a Risk Inventory to log all known and potential risks provides a framework to analyze the impact of changes. Using a Risk Hierarchy provides management with essential information about which risks pose the most significant threats.

2.2 Risk Ownership: Every department has a piece of the risk puzzle.

Each department within an organization define, measure, understand, and manage risk differently. As a result, each department has a unique **Risk Perspective**. A single Risk Perspective, however, is only one piece of the puzzle and represents only one view of risk and cannot identify risks for the entity as a whole. Each Risk Perspective must fit together with the others to get a complete view of risk across an organization.

Trying to identify, measure, and monitor risk is further complicated because tools, systems, perceptions, and risk cultures vary across organizations. Thus, developing an effective ERM Program requires working through a centralized Risk Management Working Group (RMWG) to gather and fit together each piece of the risk puzzle.

The Credit Department imposes its view of credit risk through underwriting policies and manages risk by lowering credit loss. The Compliance Department imposes its view of risk through Know Your Customer policies and manages credit risk by customer selection. Each perspective is valid and each perspective can complement the other.

2.3 Time and Resources: Developing an ERM Program can be costly.

Developing and implementing a successful ERM Program requires detailed understanding of an organization's products, lines of business, competitive and regulatory environments, and data. Negotiating different Risk Perspectives, modeling the data to reflect the risks, and working with management to identify information requirements can be costly and time consuming. A completed ERM Program that takes too long or costs too much also poses a risk to organizations.

Developing and implementing an ERM Program requires a plan with a specific set of milestones and a schedule.

2.4 A Unique Solution – A Staged Implementation

A **Staged Approach** provides a proven methodology to achieve an ERM Program that uses an organization's data to measure, monitor, and report risk at different management levels. Using ERM experts, data modeling, and management reporting can provide solutions at a reasonable cost within a reasonable timeframe. A staged approach for implementation provides the plan, tasks, milestones, dependencies that can minimize the time and resources needed to implement an ERM Program.

3 A Staged Approach to ERM Implementation

The six ERM Program Stages, shown below, are the key to developing and implementing a successful ERM Program. Based on industry best practices and practical experience, a staged approach implements a process that is repeatable and can be aligned with business patterns and changes in the business environment. The initial analysis performed during the Enterprise Assessment Stage lays the foundation for a successful ERM solution. Subsequent stages build on information learned about the organization and its inherent risks, as well as the mitigating risk principles and practices implemented by the organization's management.

Although many of these stages are easily recognized and accepted as best practices, it is important to understand that *how* each of these stages is performed contributes significantly to the success or failure of an ERM Program. Tailoring each stage to the specific organization is crucial because risk is organization specific. The gaps that exist from best practices are unique to each organization. Customized ERM solutions, grounded in industry-standard ERM principles and incorporating guidance from the COSO and the RMA, provide the most successful ERM.

Start with the end in mind.
Understand the desired state, identify gaps, and build bridges to piece the puzzle together.

Below is an overview of the

E

Stage 1: Analyze the Organization

- Achieve a full understanding of the organization
- Identify organization's structure and management
- Identify stakeholders
- Review reports, data, and strategic business documents
- Conduct strategic interviews across the organization
- Develop Risk Assessment Goals, Strategy, and Plan

R

Stages 2, 3, and 4: Identify and Measure Risks

- Interview senior managers, business line managers, and staff to identify how risk is interpreted
- Develop custom Risk Survey for the organization based on interviews
- Analyze Risk Survey responses and conduct follow-up interviews
- Develop Risk Hierarchy aligned with organization's structure
- Facilitate priority ranking of risks to develop a Risk Inventory
- Identify Key Risk Drivers for each risk
- Perform Gap Analysis
- Develop Risk Appetite for the organization

M

Stages 5 and 6: Monitor and Determine How Risk Impacts Decisions

- Analyze policies, standarads, and operating procedures
- Determine metrics (Key Risk Indicators) that measure each risk
- Design monitoring program, cycle, and reports
- Determine how risk impacts the short- and long-term strategy of the organization

3.1 Stage 1: Enterprise Assessment

Developing an ERM Program begins with the enterprise. The Enterprise Assessment Stage is especially critical for an organization with complex structures consisting of multiple entities and management layers. The Enterprise Assessment Stage consists of an in-depth study of the organization to understand the business environment, financial status, culture, goals, and products and services.

The assessment includes reviewing to review any previous research, surveys, studies, or reports completed on risk. In addition, reviews of all financial statements, audit reports, strategic and other management plans, management committee meeting minutes, organization charts, and existing policies and standards are reviewed. The information gathered generates a set of questions and discussion topics that are presented during meetings with key stakeholders.

Approaches that begin by identifying risks without completing a full study of the organization cannot capture a view of risk from a holistic perspective.

Developing and implementing an ERM Program requires relentless outreach that facilitates communication across the organization. During the Enterprise Assessment Stage, it is essential to work closely with senior management and key stakeholders to:

- Elicit data, opinions, and knowledge from across the organization
- Exchange information about the organization and ERM concepts and practices within senior management
- Develop relationships of trust that support open communication

In-person interviews with key stakeholders are crucial to obtain critical information about the organizational system and its environment from historical, current, and prospective standpoints. Once a clear understanding of an organization and its objective(s) is obtained, a Project Plan for developing and implementing an ERM Program can be created. An ERM Program Development Schedule is essential to ensure that a plan identifies the milestones and deliverables so status and progress can be easily assessed.

Once the ERM Program is developed, risk managers must reassess the organization periodically to identify changes in structure, business environment, and strategies.

3.2 Stage 2: Define Primary Risk Indicators and Dashboard Reporting Needs

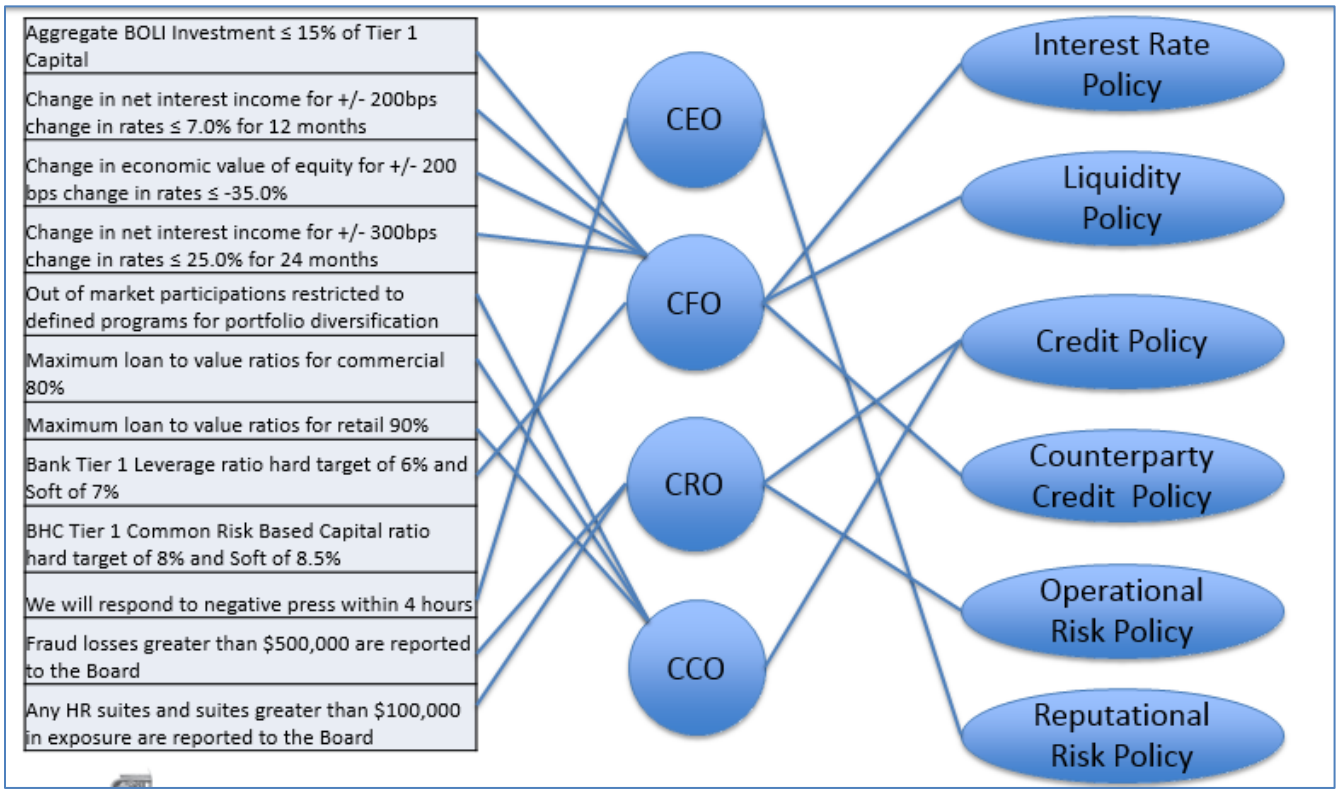
3.2.1 Step 1 – Conduct Interviews, Workshops, and Identify Top Risks

The departments within any organization define and understand risk differently; as a result, each department has a unique Risk Perspective. These different Risk Perspectives complicate the identification, measurement, and monetarization of risk, but working with management throughout the organization to better understand these Risks Perspectives ensures that the final ERM Program draws from all perspectives.

An effective way to begin to consolidate Risk Perspectives is to hold a one-day facilitated ERM Workshop for key stakeholders. The goal of this workshop is to compile the organization's strengths and weaknesses in ERM, as well as a list of Top Risks and corresponding management personnel to be held responsible for each. Facilitating discussion during the workshop also builds consensus among the key stakeholders.

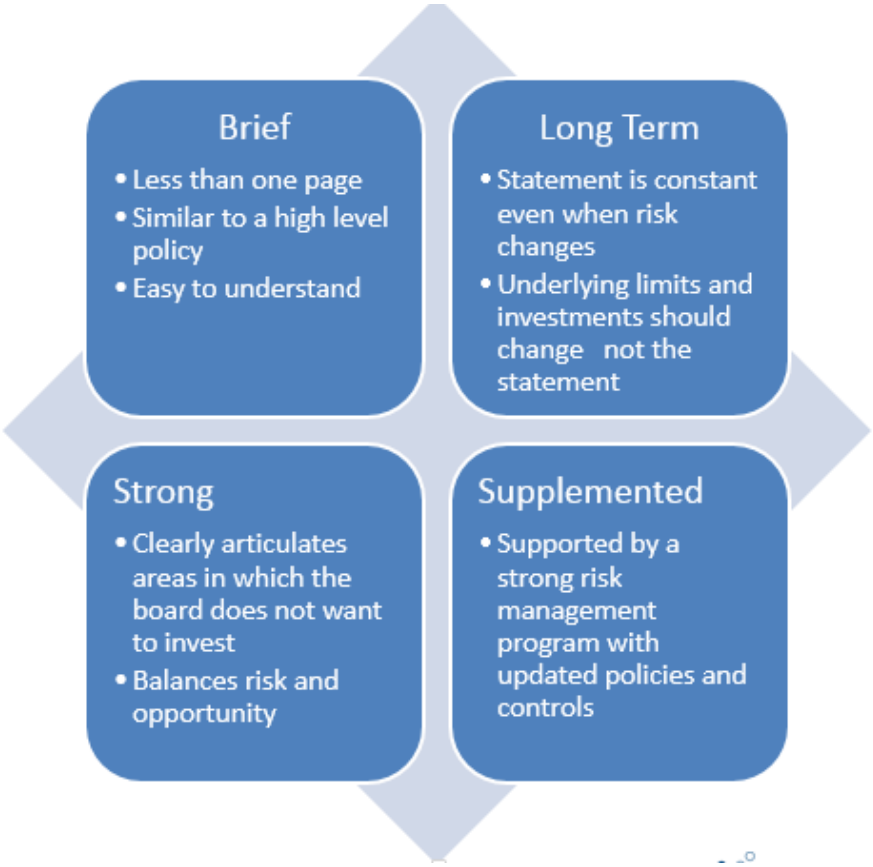
Following the workshop, in-person interviews serve to clarify Risk Perspectives and define primary Risk Categories, Key Risk Indicators (KRIs) and their dashboard reporting requirements. The table below shows results of an ERM Workshop and interviews from a sample organization.

Example of Top Risk Categories Developed from Interviews and Workshops



3.2.2 Step 2 – Develop a Risk Appetite Statement

A Risk Appetite Statement captures the organization's tolerance for risk-taking and provides a "line in the sand" for monitoring that ensures the ERM Program will operate within the desired risk. A best practice Risk Appetite Statement is characterized by the following traits:



3.2.3 Step 3 – Aggregate Risks into a Risk Hierarchy

A good ERM Program doesn't just identify the risks in each department or entity, but also determines how they are related to each other to achieve an organization-wide risk perspective

Structuring the Top Risks, identified in Step 1, along a hierarchical framework is effective in reflecting the organizational structure of risk. A hierarchy allows an accurate depiction of how risks flow among business lines and entities. It can be a useful tool in identifying the risk dependencies that can be risk drivers and in depicting risk ownership across an organization.

A Risk Hierarchy enables risk to be structured from more general to more detailed. This method cannot use a generic or standard set of risks and then force them into canned categories; rather, it is necessary to develop the risk hierarchy specifically for the organization at issue, utilizing information obtained in Step 1 (i.e., review of documentation, workshops, and interviews with key stakeholders).

3.2.4 Step 4 – Create Risk Inventory of Prioritized Risks with Risk Indicators

The Risk Hierarchy is converted to a Risk Inventory that ranks each risk according to two rating scales, reflecting likelihood and severity. Determining the impact of risks is always challenging and ultimately relies on:

- Quantitative data and metrics that show relative size, volume, relationships (ratios), or projections (stress testing), standards, and limitations; and
- Qualitative information and consensus provided by the organization's management and staff.

Example of Top Risk Categories Mapped to KRIs and Owners and Policies

Rank	Risk	Key Risk Indicators
1	Credit Risk	Aged Payments, Defaults, Customer Segmentation
2	Regulatory Risk	New regulations, Review Findings, MRAs, MRIAs
3	Strategic / Business Risk	New Products, Marketing Results vs. Plan, Product Segmentation
4	Interest Rate Risk	Default Rate, Economic Outlook
5	Concentration Risk	Customer Base Characteristics
6	Reputational Risk	Customer Complaints, Employee Feedback, News
7	Compliance Risk	Audit Reports, Regulatory Reviews
8	Operational Risk	Employee Retention, Technology Solutions vs. Plan
9	Earnings Risk	Revenue, EPS, Product Profitability
10	Technology Risk	Technology Budget, Technology Failures, System Availability %

Armed with the Top Risks facing the organization, KRIs, and information from interviews, the impact of various risks can now be quantified. Three risk metrics must be identified for each Top Risk:

- **Severity** – identifies the current level of risk
- **Trend** – identifies the direction of risk
- **Likelihood** – indicates the probability of risk

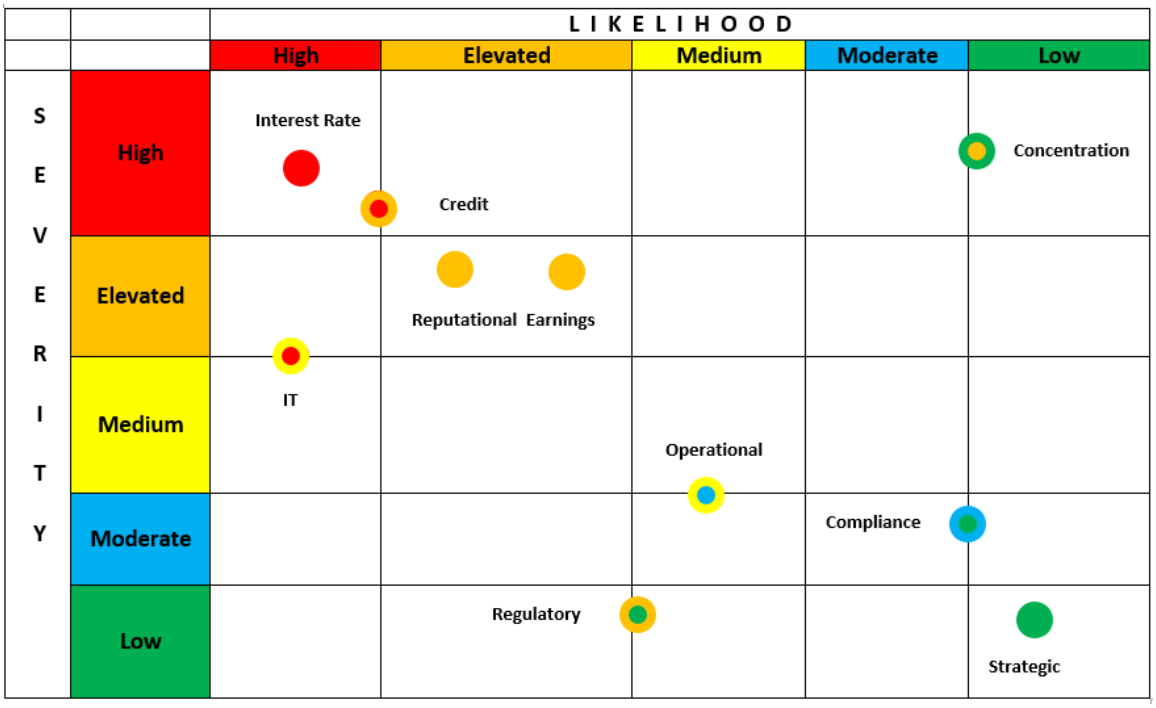
While it's acceptable and common to segregate severity and likelihood into three categories (High, Medium, Low), segregating severity and likelihood into five categories achieves greater separation in determining the risk's prioritization. The sample Risk Inventory below shows how effective such a graphic representation of priorities and trends can be.

Example of Top Risk Categories Trends and Probabilities

	High	Elevated	Medium	Moderate	Low	
Rank	Risk		Owner	Severity	Trend	Likelihood
1	Credit Risk		Credit			
2	Regulatory Risk		Compliance			
3	Strategic / Business Risk		Board			
4	Interest Rate Risk		ALLL			
5	Concentration Risk		CEO			
6	Reputational Risk		CEO			
7	Compliance Risk		Compliance			
8	Operational Risk		COO			
9	Earnings Risk		CEO			
10	Technology Risk		IT			

The Risk Inventory can also be represented on a grid or Heat Map that shows the severity and likelihood of risk in a different way. Below is an example of a Heat Map-style Risk Inventory that shows prioritized risks along with trends. The inside of each circle represents the current severity and the outside of each circle represents the likelihood.

Example of Top Risk Categories Heat Map



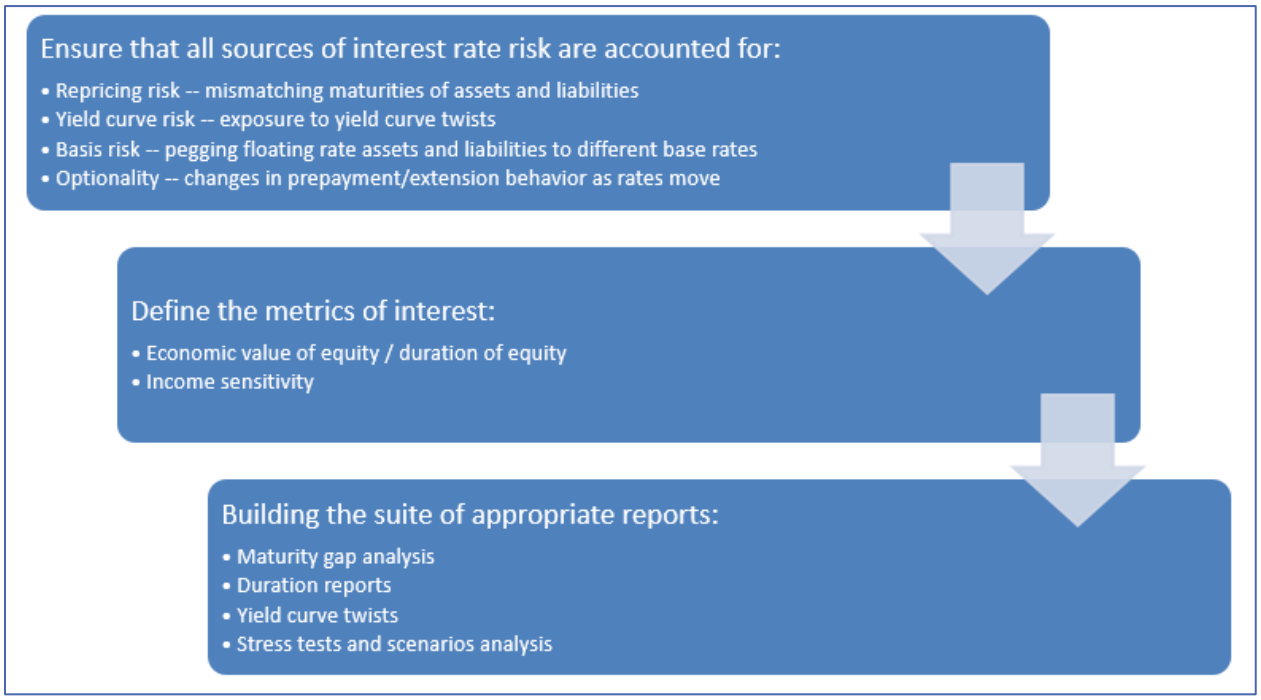
3.3 Stage 3: Gap Analysis

The purpose of the Gap Analysis Stage is to compare an organization's current data and ERM processes to the best practices. The Gap Analysis Report records industry standards or best practices and identifies actions that can be taken to address identified gaps.

To create the Gap Analysis Report, a Data Requirements Matrix is developed, based on the Risk Inventory created in step 3 (documenting each risk and key risk indicators). The Data Requirements Matrix identifies the data each risk owner requires to perform ongoing monitoring of each risk. By working with the organization's staff to identify the source data elements for each key risk indicator, it is then possible to identify any gaps in the source data available. This ensures a comprehensive list of data sources, data characteristics, format, and sensitivity level for each data element.

The graphic below shows the type of information included in a Gap Analysis Report to help management and staff understand the industry standards or best practices.

Example of Gap Analysis: Best Practices in Interest Rate Risk Management



The Gap Analysis Report should be presented to senior management and key stakeholders as soon as possible. It can be very helpful to do so via a full-day Gap Analysis Workshop, which clarifies best practices in ERM and helps create a common risk language for all in the organization moving forward.

3.4 Stage 4: Develop Prototype Risk Monitoring and Reporting

Risk monitoring and reporting are key to sustaining an ERM Program, and they often receive significant focus from managers who realize they need to consider risk when making decisions. In many instances, however, those managers are often left with incomplete or confusing information. Management must be able to quickly identify any segment of the organization struggling with risk. Doing so requires developing a prototype reporting system with metrics and dashboards that are

specifically tailored to the organization. The graphic below summarizes the importance of monitoring and reporting in an ERM Program.

ERM Reporting Benefits

Developing a risk monitoring and reporting function presents several unique challenges. First, the number and variety of organizational entities must be considered to determine the level of granularity needed for reporting. For example, risk monitoring and reporting can be performed on each line or business or as a group within each entity. Second, it is critical that risk monitoring and reporting is available for the entire organizational structure. Database experts are needed to work with the organization's IT department to determine the level of aggregation possible in reporting. The specific steps of risk monitoring and reporting development are outlined below.

3.4.1 Step 1 – Review Gaps, Data Requirements, and Key Risk Indicators

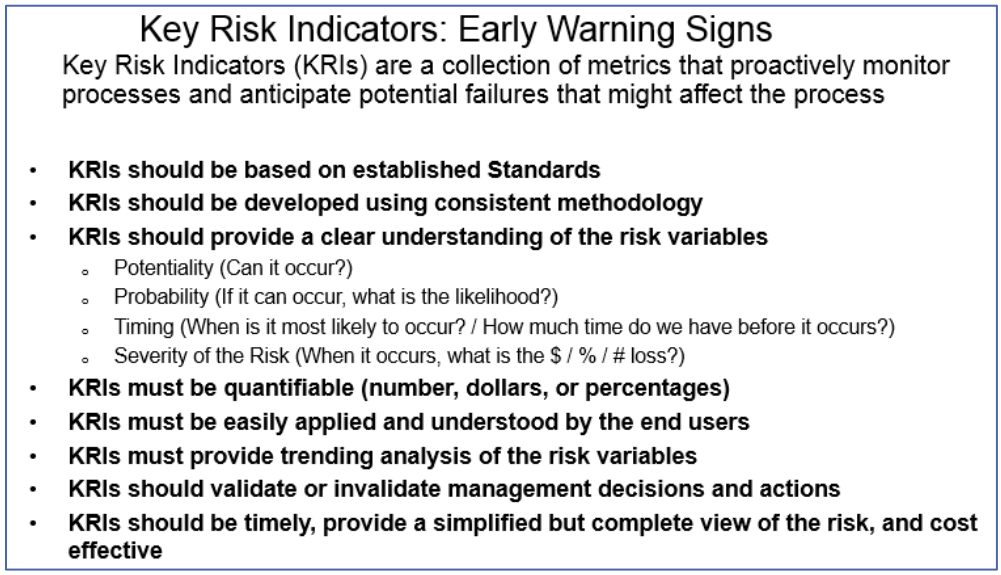
By building on the information gathered and analyzed in earlier Stages, a recommendation of the design of custom reports and dashboards can be made using the following resources:

- Prioritized risks on the Risk Inventory with key risk indicators
- Data Requirements Matrix with key risk indicator data sources
- Impact measurement metrics, data, and qualitative information identified jointly with risk owners used as input for risk prioritization
- Risk dependencies documented on the Risk Hierarchy
- Recommendations related to risk measurement and reporting documented on the Gap Analysis
- Guidance, limitations, and tolerances defined by the Risk Appetite

Using the information developed and analyzed in earlier Stages, a presentation of the Gap Analysis Report and Data Requirements Matrix can be made to the RMWG and other relevant committees (RMC, Funding Corp. representatives, etc.) to:

- Review key risk indicators identified and related source data
- Obtain feedback on identified gaps and data requirements
- Determine additional internal reporting requirements
- Identify external metrics investors and rating agencies require to continue to maintain a targeted rating
- Assess alternative source data identified in the Gap Analysis

The feedback provided by key stakeholders assists in finalizing the data requirements for monitoring and reporting and also helps identify specific KRIs that may be refined to specific limits or tolerances. This approach achieves a strong alignment between the data used to rank risks and the data used to monitor and report risks, which, in turn, provides management with a single view that they can understand and investigate in more detail now that the supporting data or information is known and available. The graphic below lists best practice standards for KRIs.



3.4.2 Step 2 – Design Reports and Dashboard

After all assessments of data requirements, gaps, and KRIs are finalized, it is time to design reports and dashboards that will provide the monitoring results for risk. Reports and dashboards are based on templates so that managers throughout the organization receive a consistent set of data. The report templates should be distributed to stakeholders for review and comment and then finalized. It is important to document the data and information monitored and reported as this serves as a specification for development efforts. Further, a monitoring and reporting cycle that corresponds to management's requirements for the information should be used to record any data limitations identified in the KRIs. Ways of capturing the otherwise limited data in the future also should be considered and recorded.

Example of KRI Limits

Limit	Risk Category	Executive Manager Oversight	LOB/BU	Risk Appetite Statement or Guidelines	Policy ID
Change in net interest income for +/- 200bps change in rates ≤ 7.0% for 12 months	Marketing	CFO	Treasury	Yes	POL 000-0004
Change in economic value of equity for +/- 200 bps change in rates ≤ -35.0%	Marketing	CFO	Treasury	Yes	POL 000-0004
Net Short Term Non-Core Funding Dependence <30%	Liquidity	CFO	Treasury	Yes	POL 000-0001
Short Term Liquid Assets/ Short Term Liabilities >125%	Liquidity	CFO	Treasury	Yes	POL 000-0001
Loan to Deposit Ratio hard target 125%, Soft Target 100%.	Liquidity	CFO	Treasury	Yes	POL 000-0001
We will not invest in assets with a rating lower than B+	Counter Party Credit	CFO	Treasury	Yes	POL 000-0011
Concentrations by industry, cannot exceed 25% of loans.	Credit	CCO	Credit Admin	Yes	POL 000-0017
Insurance reserves will be greater than 110% of exposure	Operational	CRO	Corporate	Yes	POL 000-120

3.4.3 Step 3 – Design Dashboard Interface

The dashboard interface design requires careful analysis and consideration. The graphical presentation of information is critical to allow users to easily identify important information, adjust the view, and maintain consistency with organizational presentation guidelines. A professional graphical interface designer should be utilized in developing the overall design and can present the design to the RMWG and other key stakeholders for feedback before a final design is completed.

Example of Dashboard Interface

3.5 Stage 5: Develop and Implement Risk Management Governance and Controls

Implementation of risk governance and controls is the ultimate and primary goal for an ERM Program. A chain is only as strong as its weakest link; therefore, the overall system is only as strong as the organizational departments. Hence, it is extremely important that strong risk management governance and controls become a part of the risk culture of every association. The key outcome of this stage is to identify the ongoing sponsor/ownership of the ERM Program and clearly define each participant's roles and expectations.

During this stage, it is necessary to educate key decision makers in the role of monitoring and assist them in determining if key targets, triggers, or limits should be set as the risk response in given situations. Tripping key triggers may lead the system to start a methodical process to execute key parts of the contingency plans.

3.6 Stage 6: Establish Implementation Strategy

The final stage in this process is integration of the prototype dashboards and reports into an ongoing IT infrastructure and production system. Working with key stakeholders to determine next steps needed to develop the production model will facilitate contingency planning and strategies to facilitate decision making especially under stress when decisions have to be made quickly.

Making decisions quickly in the face of uncertainty is the largest benefit of a successful ERM program.

4 Utilizing Stages in a Management Approach: Second Pillar Consulting

With over 300 years of combined risk management experience, Second Pillar's team is well equipped to implement and expand ERM strategies. Work at Second Pillar isn't delegated to junior-level analysists. The Principal, senior consultants, and industry experts work together to perform engagement tasks and offer expertise. Second Pillar's Technical Approach, outlined above, complies with industry-best practices for development and implementation of ERM Programs. Throughout this process, Second Pillar's Management Approach aligns with steps taken in the Technical Approach to communicate and confirm with management the information gathered and the solution being built. Providing strategic, concise, and frequent communications keeps management informed and immediately capable of identifying issues. Following is an overview of Second Pillar's approach to assisting organizations with developing, implementing, or expanding an ERM Program.

4.1 Stage 1: Enterprise Assessment Deliverables

- A kickoff meeting to determine the deliverables
- Identify the key stakeholders
- Submit request for materials, including:
  - Risk Assessments
  - System Governance Committee Structures
  - Structure and charter of key risk committees or work groups such as Risk Management
  - Publicly available information such as financial statements and internal reports on operations from the Funding Corp, banks and associations
  - Audit reports
  - Policies, standards, and procedures
  - Strategic and management plans
  - Data and data definitions
  - Strategic Plans
- Develop Status Report template for review and approval
- Draft Project Plan that provides step-by-step plans for meeting the project goals, resources required, milestones, and specific project deliverables

4.2 Stage 2: Define Primary Risk Indicators and Dashboard Reporting Needs Deliverables

- Conduct interviews with key stakeholders and produce summary report
- ERM Workshop for senior management and key stakeholders
  - Top Risks and owners identified during ERM Workshop

    - Develop Risk Hierarchy and Risk Inventory of Prioritized Risks
- Conduct data analysis that identifies key risk indicators for each Risk Inventory item
- Develop Risk Appetite template and assist management with creation of Risk Appetite Statement

4.3 Stage 3: Gap Analysis Deliverables

- Develop Data Requirements Matrix that documents the data requirements for each risk and key risk indicator
- Develop Gap Analysis Report that documents each risk and the risk response
- Create a report detailing identified deficiencies in data required for risk monitoring, risk management, governance, controls, and reporting

4.4 Stage 4: Develop Prototype Risk Monitoring and Reporting

- Present Gap Analysis Report and Data Requirements Matrix to management and key stakeholders
- Provide data, metrics, and qualitative information supporting each key risk indicator
- Draft and Final Risk Monitoring Reports
- Draft and Final Report and Dashboard Templates and Monitoring and Reporting Cycle

4.5 Stage 5: Develop and Implement Risk Management Governance and Controls

- Assist in establishing the roles in owning the risk and the system of risks
- Help identify the “owner” of the system and assist in the change process
- Work with the RMWG to establish the owners of the primary risks
- Assist RMWG in developing the policies that should surround the process
- Risk Management Framework Gap Analysis

4.6 Stage 6: Establish Implementation Strategy

- Assist in the decision to buy or build the system in-house or having a vendor provide the capabilities
- Develop the transition plan
- Assist with change management

5 Conclusion

A successful ERM Program is essential in safeguarding an organization against risk. When working against time and budget constraints, creating and maintaining an ERM Program is difficult, as every department has a different view of risk, which is ever-present and ever-changing.

Through the implementation of a Staged Approach, a complete and extensive assessment of an organization's risk allows for a personalized ERM Program that can be timed to cycle with business patterns or changes in the environment. Many of the steps listed in the Staged Approach are already considered best practice, but tailoring these steps to an organization is crucial because each organization's risk is specific and unique.

Our Management Approach, which aligns with steps considered best practice, assures continual communication and coordination with management and key stakeholders. This provides the fullest understanding of an organization and its risks, and assures that we can provide the highest quality assistance and expertise during planning and implementation of an ERM Program.

For additional information contact Second Pillar Consulting.

Bill Nayda, Ph.D.

(804) 432-1629

bnayda@secondpillar.com

11174 Lake Shore Ct.

Glen Allen, VA 23059