

Aligning and Integrating ERM and Business Process



Federal ERM Summit

September 9, 2013

11:00-12:00

Agenda

Defining Risk and ERM

The ERM Value Proposition

An Integrated ERM Framework

Aligning ERM with Business Processes

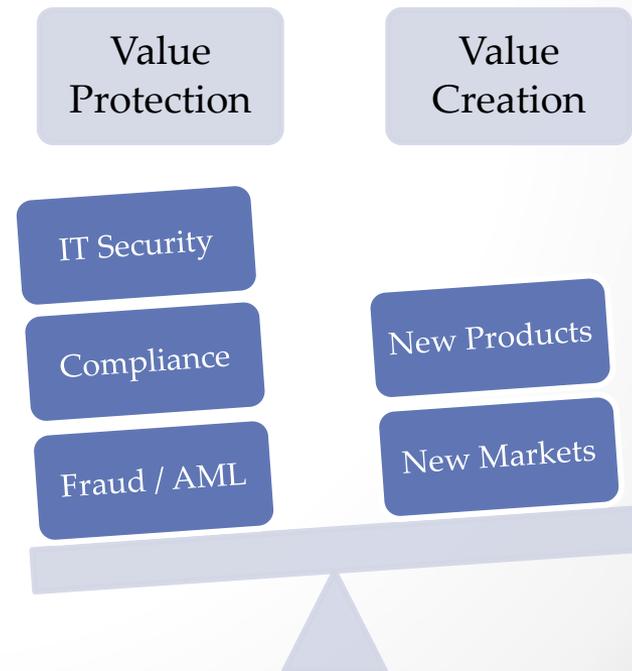
Q&A

Defining Risk, ERM

The correct definition of risk accommodates both the avoidance of losses (value protection) and the enhancement of opportunities (value creation).

Risk is the potential for loss, or the missed opportunity for gain, caused by events that prevent a firm from achieving its strategic objectives.

Simply put, how a firm balances that equation reflects its risk philosophy.

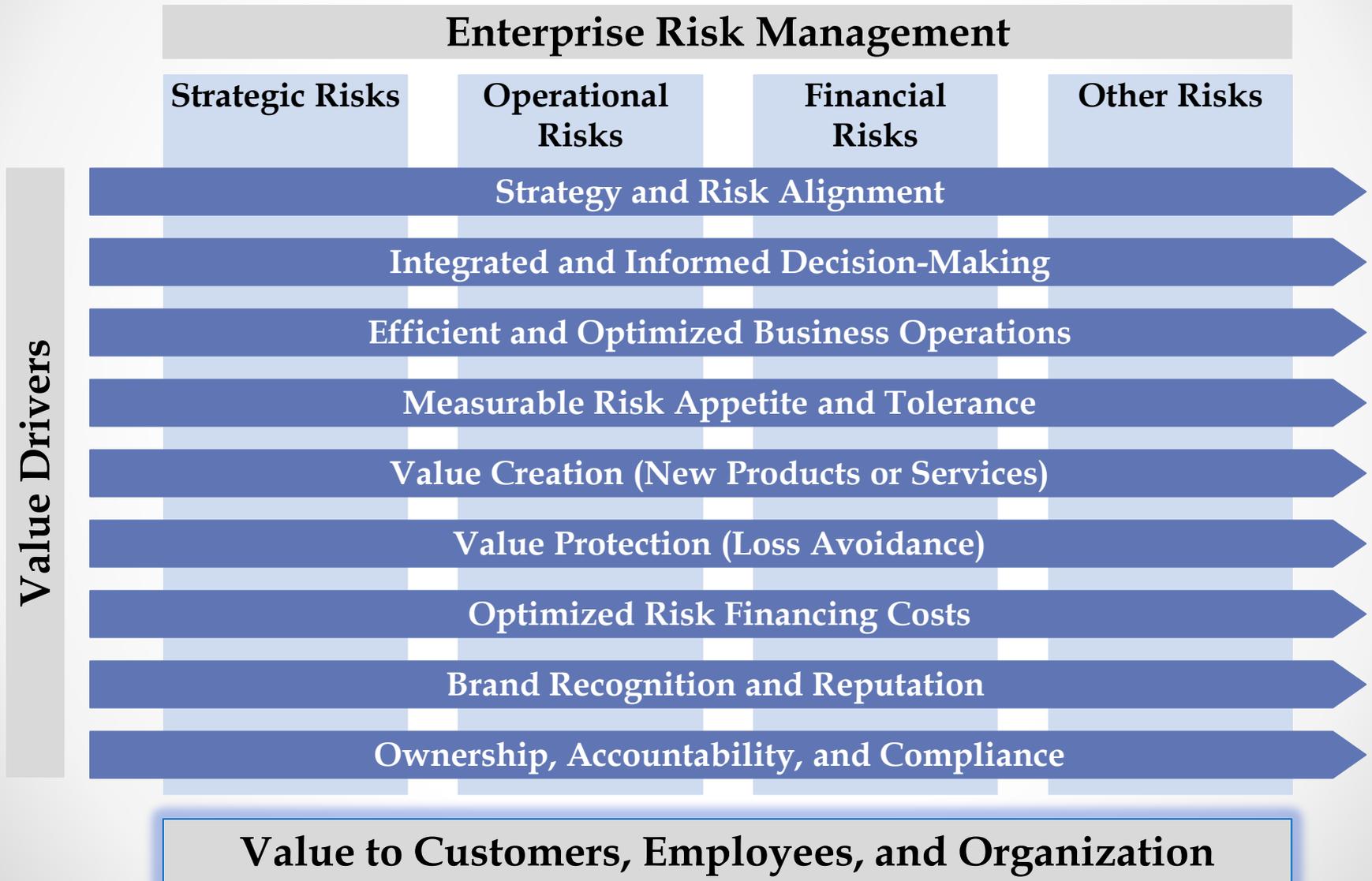


Defining Risk, ERM

ERM is a management tool that, when properly aligned to key business strategies and integrated with key business processes, enables an organization to:

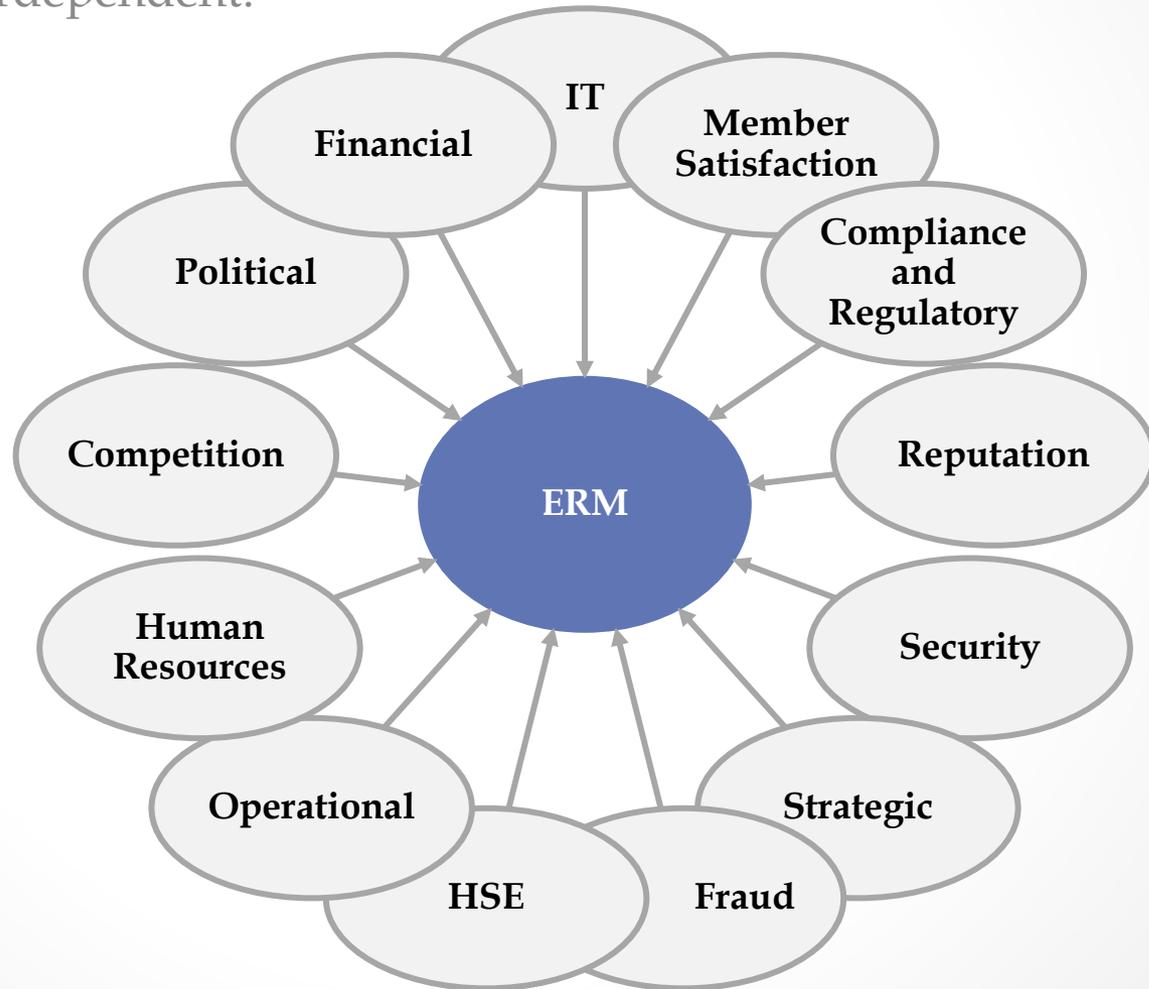
- ❑ Align key objectives with the management of risks that threaten them
- ❑ Systematically identify, measure, assess, prioritize, respond to, report on, and monitor risks across the entire portfolio
- ❑ Address the 'full spectrum' of risks
- ❑ Focus only on key risks
- ❑ Develop risk practices that encompass the entire business, creating connections between silos
- ❑ Consider single events and complex risk interactions / interdependencies
- ❑ Aggregate risks into a corporate-wide risk profile
- ❑ Infuse risk practices into the corporate culture, so that decisions evolve from a risk-informed process linked to risk appetite

The ERM Value Proposition



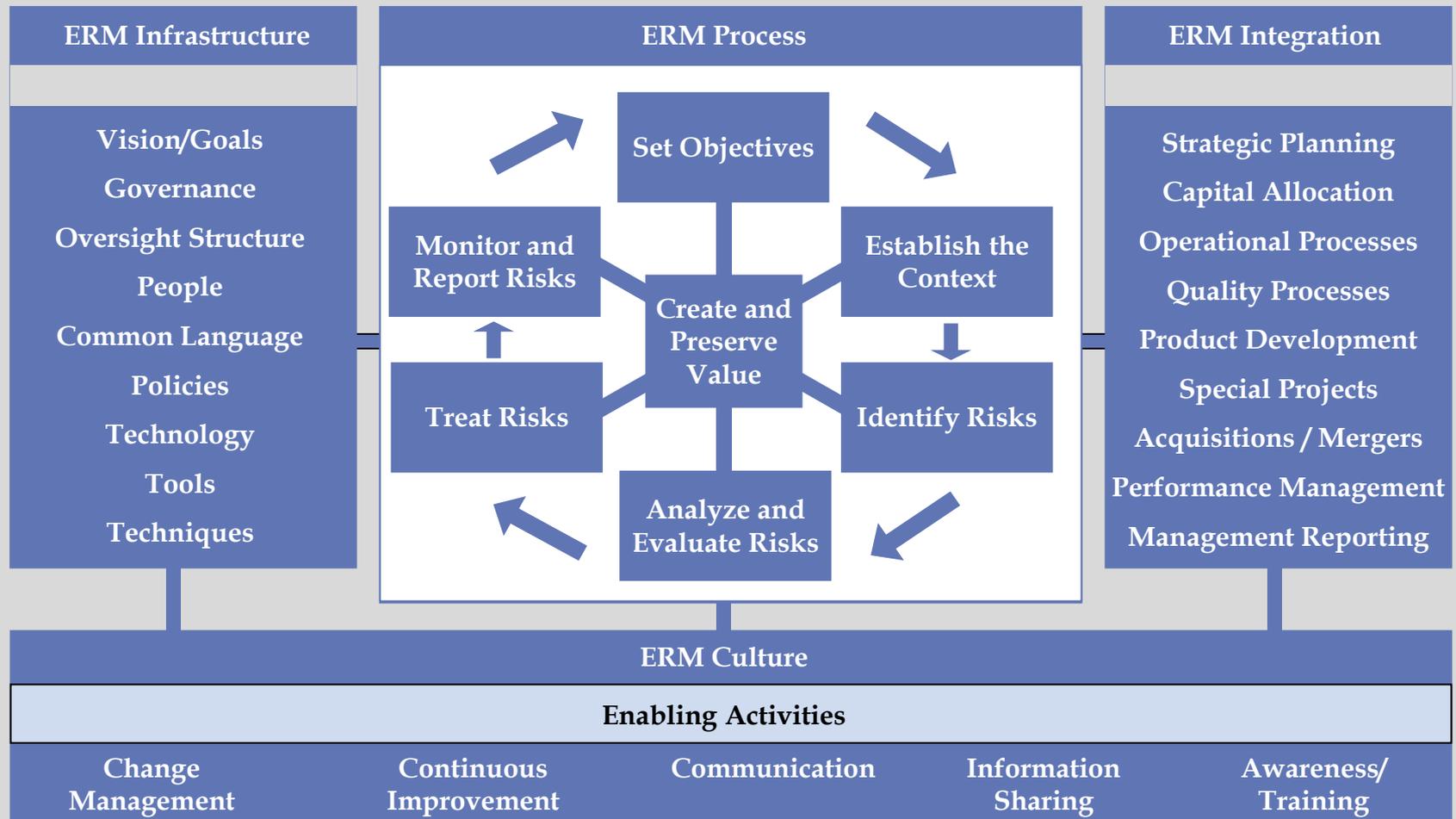
A Comprehensive Approach

Just like processes within an organization are integrated with one another, risks are also linked and interdependent.

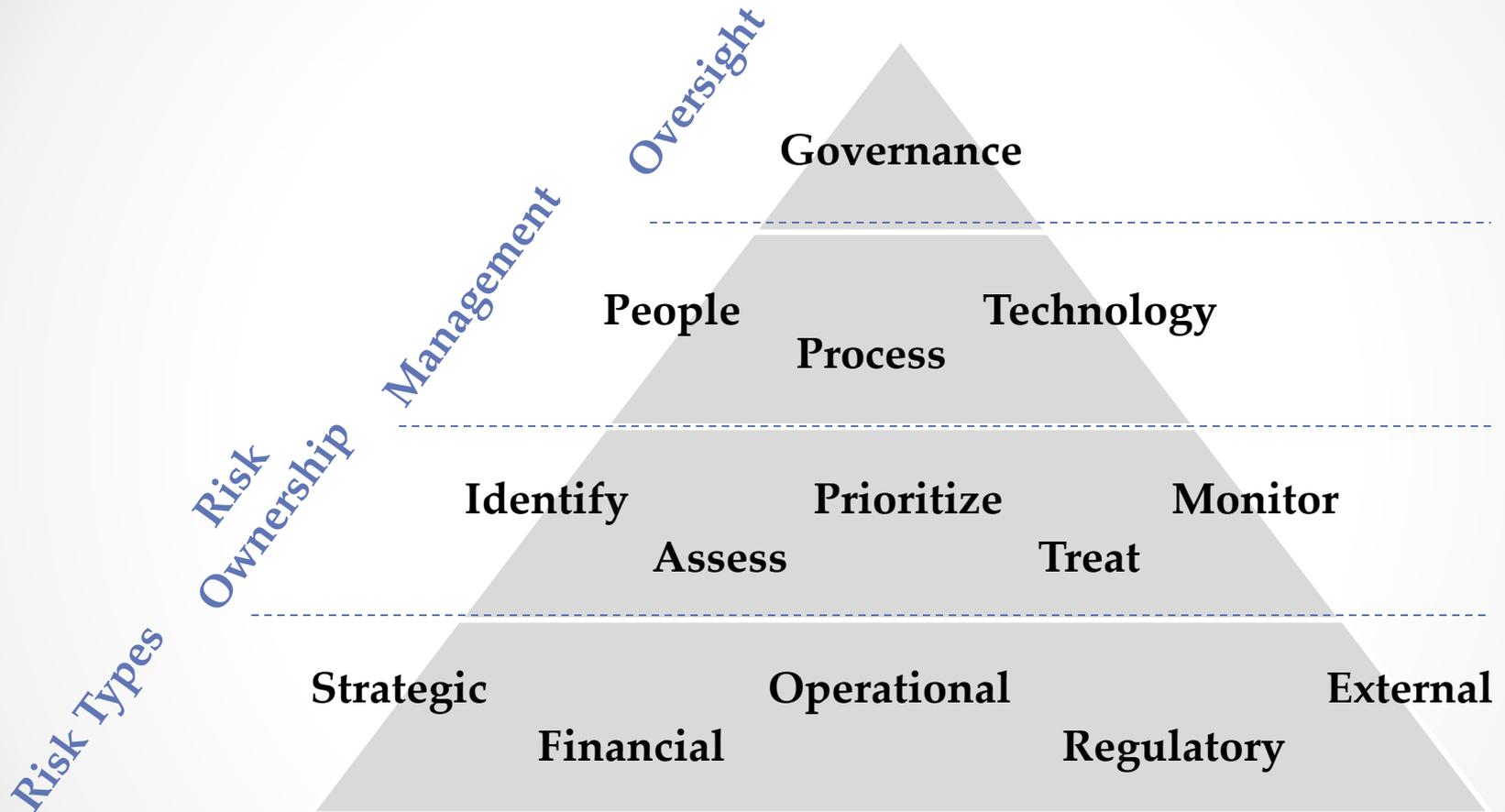


An Integrated Framework

Enterprise Risk Management



An Integrated Framework, Adopted



Integrating ERM with Business Process

Five key areas of focus to ensure success:

1. Tone at the top and leadership buy-in
2. Organizational awareness, education, and change
3. ERM strategy aligned with corporate strategy
4. Active role in key business activities
5. ERM process reinforcement

1. Tone at the Top

The number one killer of well intentioned ERM programs.

- ❑ The board and c-level executives must be genuinely engaged from day one and reinforce all ERM activities and messages
- ❑ The CRO – or equivalent – must have sufficient authority to work hand-in-hand with other executives in risk-taking roles... and to stand up to them when necessary
- ❑ The CRO should have a ‘seat at the table’ for all key strategy meetings and business decisions
- ❑ The CRO should have a direct line to the board, and should be a regular at board meetings, even if a risk committee isn’t in place or isn’t reporting

2. Organizational Awareness, Education, Change

A robust ERM program involves substantial 'set up time' and should not be rushed...

- ❑ Board, executive management, senior management, and staff kick-off meetings
- ❑ Flyers, brochures, intranet sites
- ❑ Risk surveys
- ❑ Training at all levels

Five Enterprise Risk Management (ERM) Focus Areas illustrate the ERM framework of PenFed over its enterprise-wide. The Focus Areas provide a summary of the information used to prepare and effectively implement ERM across the business.

Introduction

Organizations that are most effective and efficient in managing risks to both existing assets and to future growth will, in the long run, outperform those that are not. Strong risk businesses raise money by managing risks well.

Risk is the potential for loss, or the diminished opportunity for gain, caused by events that can adversely affect the achievement of PenFed's objectives.

The aim of Enterprise Risk Management (ERM) is to effectively deal with uncertainty. Uncertainty is associated with events (e.g. an action, new projects, change in market trends) that could result in positive consequences (e.g. increase of revenue) or negative consequences (e.g. loss or reversal). These negative consequences are 'risks' that PenFed needs to be aware of and prepare for in advance. However, risks are often intertwined and interdependent, making them difficult to identify and manage. Implementing effective ERM processes helps PenFed better manage its risks and therefore increase the probability of prosperity.

1. Establish the Context

Overview

This step involves understanding PenFed's internal and external environment. For instance, the economic climate, our competitors, and how laws and regulations constitute part of the external environment. Likewise, understanding our internal operations and the dynamics of PenFed as part of the internal environment. The VP ERM will provide the context against which risks will be evaluated for consistent assessment.

One of the distinguishing features of ERM is the linking of strategic decision-making and risk management. Under ERM, all strategic decisions are made in the context of the risks and opportunities represented, and capital is allocated accordingly. PenFed's strategy and supporting business objectives drive the entire ERM process from setting the risk appetite and tolerance levels to risk assessment and treatment decisions. In this way, PenFed knows what the greatest risks are to achieving its objectives, how much risk it is willing to accept through business activities, and the anticipated return on capital it can expect to realize.

Objectives

- To establish the scope of the risk management process
- To understand and consider PenFed's strategic objectives, the

The ERM team accomplishes enterprise risk through:

- Industry and market research
- Individual meetings with executive and senior management
- Workshops and focus groups with risk owners

Objectives

- To identify a comprehensive list of key risks and events that might impact the achievement of PenFed's strategic directives, including missed opportunities and organizational waste
- To differentiate between risks, root causes, and consequences
- To assign owners to each risk for ongoing assessment and reporting

3. Analyze Risks and 4. Evaluate Risks

Overview

This step involves consideration of the scope of risk, the magnitude of their positive and negative consequences, and the likelihood that those consequences may occur. Once the analysis is concluded, ranking and prioritizing of the risks allows management to decide which risks require treatment. Ranking criteria are based into consideration when analyzing risks.

Risks are identified during the Identify phase and subjected to a semi-quantitative evaluation of the likelihood and impact using predefined risk levels to then removed and retained based on the risk. Those risks falling below a defined threshold may be treated and managed within the business but will not be executive level.

Enterprise Risk Management - What is All the Buzz About?

What is Risk?

Risk is "the potential for loss—or diminished opportunity for gain—caused by events that can adversely affect the achievement of PenFed's objectives."

What is ERM and How Does it Help PenFed Manage Risk?

By Implementing ERM...

PenFed will be better positioned to anticipate and react to opportunities, and be better prepared for devastating losses or business disruption.

- A systematic process to identify, measure, prioritize its exposure to risks across the portfolio
- Risk practices that encompass the entire business, creating connections between departments
- Risk strategies that address the full spectrum of risks (not just financial)
- Consideration for both single events, and complex risk interactions & interdependencies
- Risk practices are infused into our culture, so that decisions evolve from a risk-informed process

When Do We Do It?

Several ERM activities occur on a schedule. For example, ERM objectives are defined during the semi-annual planning process, risk identification and assessment are conducted quarterly, and reporting monthly. However, many activities occur on an as-needed basis. For example, new risks can emerge at any time and may require analysis, risk treatment plans are developed once a risk is identified, and ERM communications flow regularly.

ERM is a living, ongoing process that is dynamic in nature and should be part of how we work everyday!

Who is Involved?

Everyone! In order to be successful, everyone must play a role in ERM.

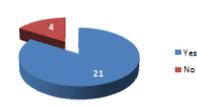
Why Do We Do It?

ERM can create value for PenFed, our Members, and our other stakeholders in many ways:



2a. General Risk Management Activities

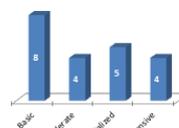
4. Does your department perform any risk management activities on a regular basis?



Some examples listed include:

- Disaster Recovery planning and testing
- Security questionnaires
- Due diligence studies
- Contingency and back-up planning
- Risk analysis for new partners/vendors
- Policies and procedures
- Interest rate and credit risk assessments

5. How comprehensive are the risk activities performed?

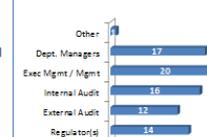


For those who answered 'Yes'

6. What are the primary reasons the activities are performed?



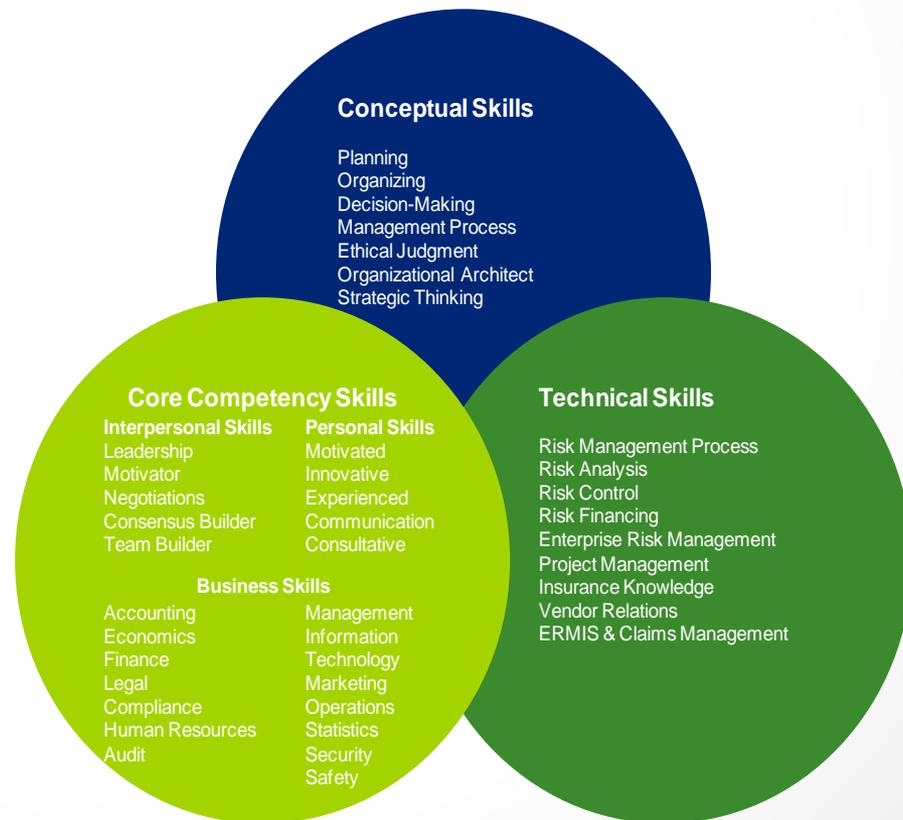
7. Who is driving the process forward?



2. Organizational Awareness, Education, Change

Relationships, relationships, relationships...

The CRO must be more than a technical expert. Soft skills are a **MUST!**



3. ERM Strategy, Business Strategy

The ERM strategy and the overall business strategy must be one and the same...

A case study: Pentagon Federal Credit Union

1. ERM Vision

Optimize the financial and operational performance of PenFed's aggregate portfolio, both through the preservation of existing assets and the creation of future growth opportunities, while continuously adding value to the Members' experience.



3. ERM Strategy, Business Strategy

2. Mission

Corporate Mission

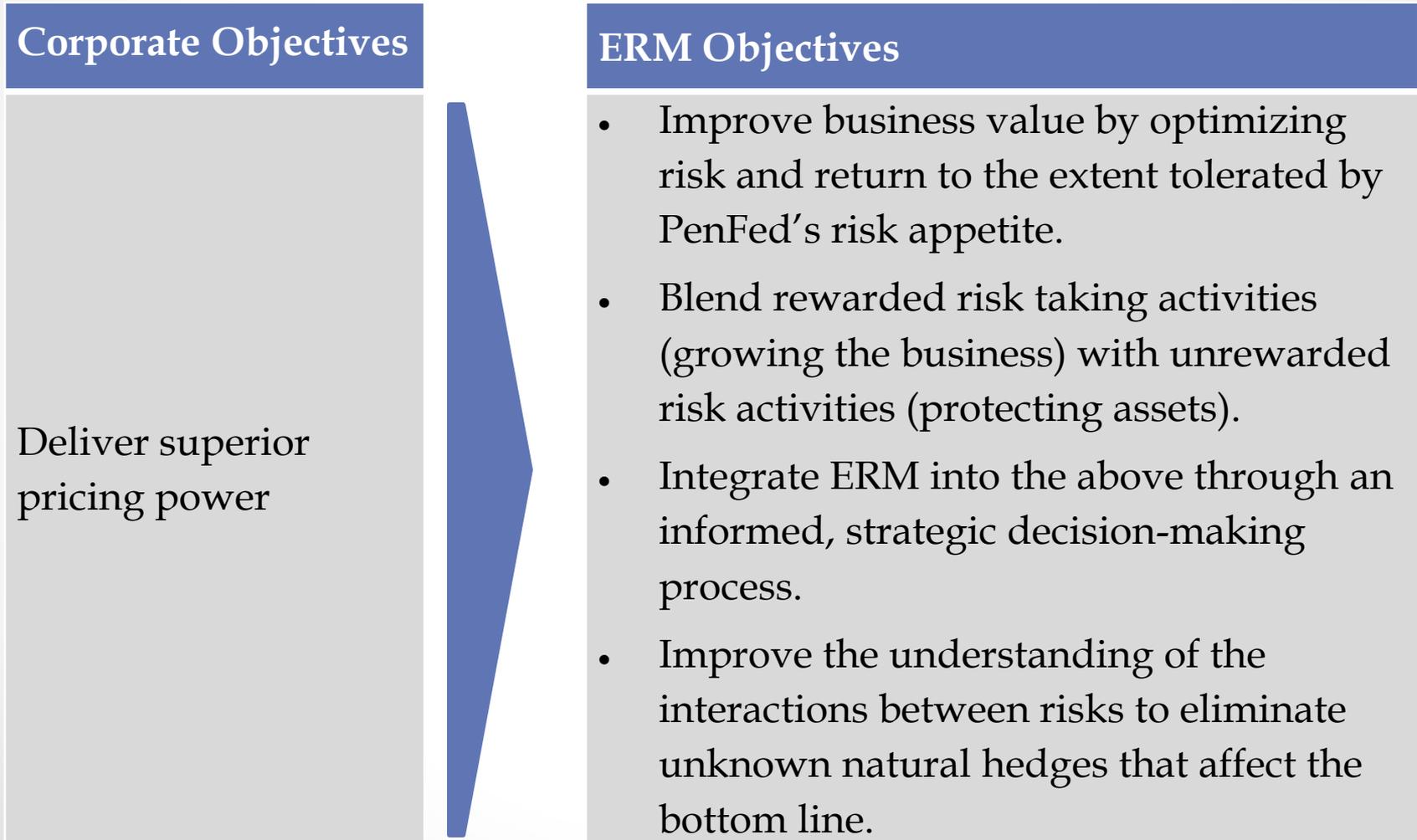
Provide superior financial services, responsive to members' needs, in a cost effective manner

ERM Mission

- Establish a link between risk management and an increase in Member value
- Create a culture of risk awareness that empowers leaders and holds all employees accountable for the protection of assets
- Aggregate and manage the full spectrum of risks and understand their interdependencies
- Provide leaders with the information and analysis required to make informed risk taking and risk mitigating decisions

3. ERM Strategy, Business Strategy

3. Strategic Objectives (one example)



4. Active Role in Key Business Activities

As previously mentioned, the CRO must have a seat at the table when it comes to key business decisions:

- ❑ Strategic planning meetings
- ❑ New product launches
- ❑ Mergers and acquisitions, due diligence
- ❑ Process and technology improvements
- ❑ Implementation of regulatory changes

5. ERM Process Reinforcement

Not a 'one and done'. More than just an 'annual exercise'.

- ❑ Keep policies and procedures current
- ❑ Continuously improve tools and templates
- ❑ Regularly report through audience appropriate dashboards
- ❑ Re-perform risk assessments regularly, and treat risks in a timely manner, according to priority
- ❑ Revisit risk appetite with the board during periods of change and uncertainty
- ❑ Ensure KPIs and KRIs remain relevant and a true reflection of business priorities

5. ERM Process Reinforcement

Understand and communicate the role of Internal Audit... a collaborative effort!

Core Internal Audit roles include:

- Giving assurance on risk management processes.
- Giving assurance that risks are correctly evaluated.
- Reviewing the management of key risks.

Safeguards include:

- Management remains responsible for the risk management activities.
- IA does not manage any of the risks on behalf of management.
- IA provides advice, challenge and support to management's decision making, as opposed to taking risk management decisions themselves.



Questions?

...