Creating a Robust Enterprise Risk Management Infrastructure
September 16, 2019

Moderator:
Matthew Hensley, VP, Enterprise Risk Management, Arch MI

Panelists:
Gregory A. Keith, SVP & CRO, Office of Enterprise Risk, Ginnie Mae
Gwen Muse-Evans, President & CEO, GME Enterprises
Michael Wood, SVP, Credit Risk Executive, Bank of America
ERM Fundamentals
Enterprise Risk Management
Key Concepts, Risk Types, Lines of Defense, Foundations

Michael Wood
SVP, Credit Risk Executive
Bank of America
Key Concepts of Risk Management

Risk is inherent in all businesses and organizations. Managing risk well is the responsibility of all employees within an organization. Effective risk management enables you to serve your customers and deliver for your shareholders. If you do not manage risk well it can result in financial loss, regulatory sanctions and penalties, and damage your reputation, each of which may negatively impact your ability to execute the business strategies. It is very important that all employees embrace their responsibility to manage risk well.

One way to accomplish this is to establish a Risk Framework. The risk framework establishes roles and responsibilities for the management of risk by front line units, independent risk management, other control functions and Corporate Audit. Once the Risk Framework is established it applies to all employees. It will explain the Company’s approach to risk management and each employee’s responsibility for managing risk. It is crucial that all employees take ownership for managing risk and are accountable for identifying, escalating and discussing risks that face the Company.

The following are common components of a risk management approach:

• Culture of managing risk well
• Risk appetite and limits
• Risk management processes
• Risk data management and reporting
• Risk governance
Fundamental Risk Types

The following list establishes key risk types and definitions:

- **Credit risk** – Risk of loss arising from the inability or failure of a borrower or counterparty to meet its obligations.
- **Strategic risk** – Risk resulting from incorrect assumptions about external or internal factors, bad business plans; not effective execution of business strategy; or failure to adjust/adapt in a timely manner to regulatory changes, macroeconomic (or microeconomic) environments in the geographic locations you operate.
- **Market risk** – Changes in market conditions that adversely impact the value of assets or liabilities or negatively impact earnings.
- **Liquidity risk** – An organization’s inability to meet expected or unexpected cash flow and collateral needs while continuing to support the business based on current economic conditions.
- **Operational risk** – A loss resulting from inadequate or failed internal processes, people and systems or external events.
- **Compliance risk** – Risk of legal or regulatory sanctions, material financial loss or damage to the reputation of the Company arising from the failure of the Company to comply with current requirements of applicable laws, rules and regulations, and your internal policies and procedures.
- **Reputational risk** – A risk that comes from negative perceptions of the Company’s conduct or business practices that adversely impacts its profitability or operations.
Three Lines of Defense

Front line units – these business units own and are responsible for managing risk in the day to day business activities. Independent risk management – oversees all risk activities within the front line units and across the organization. Their purpose is to provide independent risk assessment on current business activities to determine if they are appropriate or not based on established risk appetite.

Corporate Audit – provides independent oversight via validation testing of key processes and controls performed by front line units.

One of the keys to a successful and effective risk management framework is identifying and establishing the three lines of defense. It is crucial for the Front Line Unit (the first line of defense) to demonstrate ownership and build effective processes and controls to be able to identify, measure, monitor and control the inherent risk to the business. Equally important is the partnership with the second line (Independent risk management) and third line (Corporate Audit) to enhance and maintain an effective risk framework.
Additional foundations of Risk Management

Building on your risk framework it is important to have established Compliance and Operational Risk programs. These programs (or departments) work together to drive a comprehensive approach for the proactive identification of risk, management, mitigation and escalation of operational risk that may arise within your company.

Below are some key examples of programs or metrics when determining your Operation Risk appetite:

- Establish Key Performance Indicators (KPI's)
- Establish Key Risk Indicators (KRI’s)
- Development of Risk and Control Self-Assessment (RCSA)
- Establishing Quality Assurance (QA) and Quality Control (QC) program standards
- Implementing Operational Risk Coverage Plans
- Establishing routine Operational Risk Reporting and Escalation protocols

No matter the size or type of organization the key to creating a successful risk management infrastructure is establishing departments, programs and protocols to meet the needs of your customers, investors, shareholders and regulators. Remember if a culture manages risk well it protects the Company and its reputation and will enable you to deliver on your purpose or strategy.
Enterprise Risk Management
Risk Culture, Selected ERM Tools and Risk Appetite

Gregory A. Keith
SVP & CRO
Office of Enterprise Risk
Ginnie Mae
Discussion Points

• Risk Culture
  • Sources of Culture Failures
  • Healthy Risk Culture Features

• Create Risk Culture “Muscle Memory”
  • Risk Profile
  • Risk Control Self Assessments (“RCSA”)
  • Operational Incident Root Cause Analysis

• Advanced Risk Culture – Risk Appetite
To develop a “winning” risk culture, we must understand the root causes of cultural failures

Profile of Risk Culture Failures

“Who is going to tell the CEO (owner) that things are not all rosy?”
Servicing Executive

“We can originate our way out of this problem”
CEO

“I don’t know how our portfolio will perform when things get bad”
CFO

“The market always turns around, no need to make changes to our strategy”
Head of Production

“What product makes me the most money and how do I get all of my borrowers into the product?”
Loan Officer

Source: McKinsey & Company
To get here is a marathon, pick a few (some of my favorites highlighted) that resonate with your organization and get started!

Speak truth to power

Start building the Ark before the rains turn into a flood

If you can’t see the Tsunami coming, your response will always be too late

Without a culture of rule following, all the controls in the world won’t stop bad things from happening

Profile of a Strong Risk Culture

Source: McKinsey & Company
# Selected Tools to Reinforce a Risk Culture

<table>
<thead>
<tr>
<th>Goals</th>
<th>Risk Profile</th>
<th>Risk Control Self Assessments (&quot;RCSA&quot;)</th>
<th>Operational Incident Root Cause Analysis</th>
</tr>
</thead>
</table>
| Assignment of ownership of risks and decisions on whether to avoid, accept, transfer or mitigate the risk. | • Consensus on risks facing the organization. Foundational to developing a risk appetite.                                             | • A proactive and systematic program to assess business risks and internal controls  
• Empower business divisions to become responsible for managing (or even accepting) their risks  
• Increase awareness and transparency of relevant exposures in business processes | • Raise your hand, if you had an incident (or near miss) so that root cause can be identified (e.g. training, procedures, systems controls, etc.) and mitigation strategies can be developed |
| Expected Outcomes                                                    | • Front line responsibility for 1st line of defense risk management and control embedded in the business unit with clear ownership of action plans |                                                                                                                                                                                                                                       | • Cultural change characterized by staff that understand that no one cares who is to blame, but rather how do we fix it?  
• Populates initial mitigation project plan, informs budget requests and serves as a reality check on effectiveness of controls |
Risk Appetite Definition & Benefits

The types and amount of risk, on a broad level, an organization is willing to accept in pursuit of value. Risk appetite may be articulated in the context of: strategy and business objectives that align with the mission, vision, and core values; business objective categories; and/or performance targets.

Benefits

- **Boundaries** delineating the amount of risk an organization is willing to accept when making key decisions to achieve its mission and run the business
- Acknowledge divergent views and encourage debate on **tradeoffs** when pursuing desired outcomes – establishing an agreed upon balance between value **protection** and value **creation**
- Establish **consistency** in the amount of risk an organization accepts in routine operational decisions, resulting in **confidence** that the right amount of risk is being taken
- **Measure** whether risks are being managed to the acceptable level
- Reinforce a more risk-aware **culture** by empowering employees at all levels to deliberately consider risk and act independently within established boundaries
Risk Appetite Methodology

The organization’s strategic plan is the anchor around how enterprise risk appetite and its components are defined.

The following methodology describes how an organization can engage each division to convert what were often implicit expressions of risk appetite into explicit risk appetite statements and tolerance levels.

- **Identify potential metrics aligned with each strategic (alternatively from the organization’s risk taxonomy) objective** that would guide the enterprise risk appetite statements’ focus and establish parameters for the risk tolerance levels.

- **Conduct interviews (initial questions validate RCSA themes)** with senior leadership and line managers to validate potential metrics; identify additional areas of focus; determine tolerance levels for each applicable metric.

- **Facilitate an enterprise risk appetite working session** to further educate stakeholders and discuss risk tolerance levels in a group setting.

- **Develop the organization of the enterprise risk appetite**, comprised of risk appetite statements aligned with the organization’s strategic and management goals and objectives, and risk tolerance levels.

- **Socialize** the enterprise risk appetite with leadership.
Risk Appetite Decision Making

An organization’s risk appetite is used by leadership and staff to make better, more informed decisions to accelerate performance outcomes and manage the risks that threaten those outcomes.

**Reporting Channels**

- **Enterprise Risk Appetite Statements and Risk Tolerances**
  - Drive Performance Decisions → Executive summary focused on the strategic plan, performance metrics, and adherence to defined tolerance levels
  - Drive Risk Decisions → Executive summary focused on the risk portfolio and the level of mitigation required to stay within desired tolerance levels

- Executive Operating Committee
- Enterprise Risk Committee
Risk Appetite Decision Making

An organization’s enterprise risk appetite success and effectiveness is determined by how leadership uses this information and these boundaries to inform decisions.

### Performance Decisions

- Is the organization achieving its established strategic objectives?
- Should the organization invest in X innovation to bring us within tolerance?
- Should we deprioritize projects/investments in this area due to poor performance?
- Should we shift investments to X project/initiative that is not meeting its stated objectives?
- Should we more aggressively pursue this performance target? At the expense of which other target?
- What compensating action should be taken if we do aggressively pursue this performance target?

### Risk-Informed Decisions

- What is our capacity for risk taking in this area?
- Is this risk within the organization’s tolerance or acceptable range?
- Are we taking on too much risk to achieve a certain performance target?
- Should we invest more (or less) to manage this risk?
- Looking at the current trend, how should we alleviate this Key Risk Indicator?
- Are we comfortable accepting this tradeoff?
- What risks are we creating by accepting this tradeoff?
Panel Q&A
Audience Q&A
Question for the Audience

How many in the audience have formal ERM programs at their organization?
Question for the Audience

How is the ERM program incorporated into the operating rhythm of your company?
Question for the Audience

Have you seen any differences in your organization's approach to risk management over the past few years with the market changes/challenges?
ERM Best Practices
Enterprise Risk Management Best Practices

Gwen Muse-Evans
President & CEO
GME Enterprises
Culture/Tone at the Top

Monitor, Mitigate & Measure

Risk-based Decision-Making

Risk Framework

Biz. Strategy = Risk Management

ERM BEST PRACTICES
ERM Best Practices – Culture/Tone at the Top

• Risk Culture – Created by the organization’s leadership.

• Shapes risk decisions of both management and employees. Managing risk well is the responsibility of all employees within an organization. Do the right thing.

• Mortgage industry is highly competitive. Beware of reverting to sales culture!

• Risk management is an integral part of ALL organizational processes.

- Include ERM in strategic planning and goal-setting processes. ERM can assist with strategically-aligned portfolio view of organizational risks and opportunities.
- Establishing Risk Appetite is a key part of the Business strategy.
- Define Risk Profile - Include cross-functional participation
- Integrating ERM practices can help to accelerate growth and enhance performance.
ERM Best Practices – Develop Risk Framework

- Establish Organization’s Risk Framework.

- Dedicated ERM resources (even if Matrixed organization) with clear Roles and Responsibilities – Beware of focus on sales at the exclusion of risk. Different roles but equally important.

- Three Lines of Defense – Defined roles. **Business owns the risk.**

- Authorities documented in Delegations of Authority and Risk Policies.

- Establish risk limits, thresholds and key performance indicators.
ERM Best Practices – Risk-based Decision-Making

• Risk Appetite is used to guide decision-making

• Standing formal Committee or Senior Leadership Meeting

• Structured approach for analyzing risk and communicating across business lines to make risk decisions and business decisions.

• Timely and systematic review of risk metrics and measures.

• ERM practices contain principles that can be applied from strategic decision-making through to performance.
ERM Best Practices – Monitor, Mitigation and Measure

• Portfolio view of risks – addressing all core risks. Identify, measure and assess risks related to organization objectives and strategies.

• Review of performance and quality results on an ongoing basis.

• Self assessments to identify opportunities for improvement (i.e. RCSA).

• Established processes and delegations of authority to make business decisions that respond quickly to risks and changes.

• Cross-functional collaboration and feedback loops.
Text in your questions for the ERM panel: