Enterprise risk management: A pragmatic, four-phase implementation plan

Prepared by:

John Brackett, Managing Director, Risk Advisory Services, RSM McGladrey, Inc.
704.442.3820, john.brackett@mcgladrey.com

Risk management has become increasingly important to stakeholders of organizations who are concerned about overall business risks. No organization can succeed without taking on some level of business risk, and recent events have proven the importance of adequate risk management programs. Quite simply, effective risk management is synonymous with sustainable success. Enterprise risk management (ERM) allows companies to design and construct a best-in-class corporate governance program that drives risk awareness throughout the organization.

The inherent complexity and risk profile of business operations and the capital and financial markets in which they operate, increase the importance of effective risk practices and how they are applied. The recent crisis in the financial markets and systemic effects of business failures, affecting not only financial intermediaries across the entire spectrum but now the real economy, provides clear evidence of the critical importance of effective risk management.

Regulatory authorities and governmental bodies responded to the financial crisis with renewed scrutiny of the standards and robustness of risk management practices and frameworks and the effectiveness of the regulatory and supervisory frameworks. Not in recent history have we seen regulators and governmental bodies spend so much time inquiring about and reviewing corporate governance policies and ERM strategy. ERM is no longer an option but a necessity for developing a sustainable business plan.

Scaling the ERM program to fit

Not all organizations are the same. That fact rules out a “one-size-fits-all” solution to risk management, as does a host of other factors, including:

- Complex financial markets
- Abundance of unique products and services
- Diverse technologies
- Varying appetites for risk
- Relative simplicity or complexity of business processes

Achieving effective risk management—which is dependent upon a customized and consistent framework—requires an appropriate response to these risks.

The quality of management practices

Risk management should be approached by matching organizational requirements to best practices and compliance and regulatory requirements. This entails knowledge, experience and a deep understanding of the interrelationships between risk, governance, strategy, product, process, regulation, capital, internal controls, management monitoring and disclosure.

What shape ERM takes in your organization depends on the risks your organization is exposed to, their interrelationships, the organization's susceptibility to those risks and its capacity to absorb losses. ERM classifies the range of risks that might affect your organization. Traditional financial risks like credit, liquidity and balance sheet management are accounted for, as well as operational, regulatory and strategic risks that might endanger your organization's ability to meet its obligations.

Effective ERM should provide management with the information necessary to optimize earnings, and ultimately, the organization's value, while remaining within a well-defined and acceptable risk tolerance. It should include a new and clearer language to communicate information about management's intention and capabilities.

Furthermore, it should improve business performance, establish a competitive advantage and optimize the cost of managing risk. Accomplishing this requires a positive culture that strongly influences and affirms corporate judgment in executives, managers and employees.

Getting started: Risk management culture and governance

Understanding the importance of risk and risk management in executing everyday business decisions depends on the organization's culture and the supporting governance structure. The culture should reflect an environment that not only allows, but necessitates, sound judgment in managing risks and behaviors, the integration of risk management in daily decision-making, and the establishment of risk boundaries, tolerances and habitual monitoring and reporting of control activities.

Culture drives transparency of communication and processes inside and outside the organization. The level of understanding regarding risk tolerances and consistency of understanding related to the impact of risk management on daily activities is critical to establishing an optimal risk management strategy.

The culture should foster the organization's strategic decision-making processes incorporate the assessment and measurement of risk, risk management and risk return. Best practices suggest effective risk management is driven by a strategy underpinned by three factors:

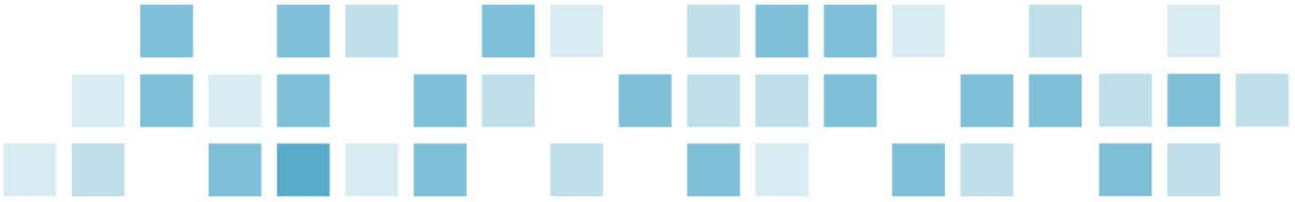
- An integrated framework of responsibilities and functions
- Driven from the board level down to operational levels
- Covering all aspects of risk

The risk management framework

While several formal ERM frameworks are available today, the minimum risk management requirements, according to practical best business practices, are as follows:

- Appropriate risk management processes, including policies, procedures and reports highlighting risk positions
- Assignment of risk ownership to clearly define responsibility and the accountability of performance monitoring in managing specific risks
- Clearly specified delegations of authority
- Regular assessment of risk across strategic, compliance, financial and operational processes, including the nature, likelihood and impact of identified risk events
- Appropriate guardrails and control performance monitoring
- Procedures and an individual reward system designed to ensure compliance

The framework, reflecting clear independence between risk-taking and risk-monitoring functions, should incorporate:



- **The board,** which is ultimately responsible for any financial loss or reduction in stakeholder value suffered by the organization
- **Executive management,** which owns and approves risk strategy (in line with defined risk tolerance, overall business strategy and management expertise)
- **The corporate governance committee**, which establishes risk appetite, defines risk management policies and ensures the risk management strategy is implemented through appropriate systems, controls, technologies and people

Directors and executives should establish their roles within the ERM framework as high-level monitors of key risks and ensure their delegates cover their responsibilities and statutory duties. To be successful, they must understand the nature of each risk, the implications of risk events, the methods of control and implications of control failure. They should ask themselves two important questions. How is the risk being controlled? What management information is available to monitor ongoing risk positions and control effectiveness? The answers to these questions should address:

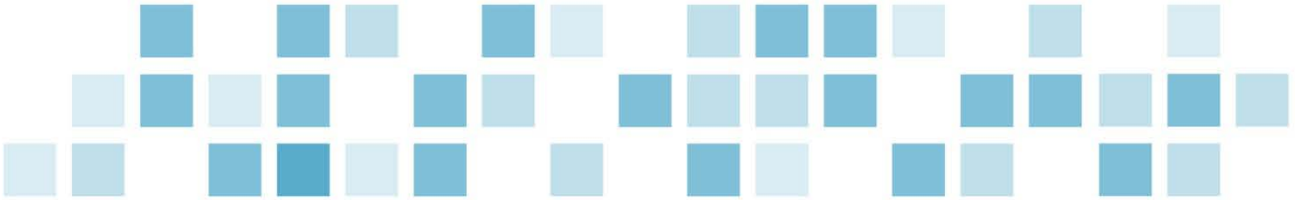
- The organization's level of knowledge and supervision governing known risks
- The extent to which the organization's management risks loss of, or maximizes revenue for, the risk positions assumed

Pragmatic implementation

To the uninitiated, the scope and potential complexity of addressing all the components of ERM can be daunting. Which ERM approach you elect to adopt will depend on many factors, including:

- The ongoing accuracy and comprehensiveness of risk assessments
- Risk measurement tools and expertise
- Markets to which the organization is exposed
- Products and financial instruments employed
- Information technology applications and architecture
- Organizational structure and geographic spread
- The prevailing risk culture
- Risk management strategy and available expertise

In short, your approach depends on the maturity level of your risk management infrastructure and framework.



Enterprise Risk within a Typical Organization

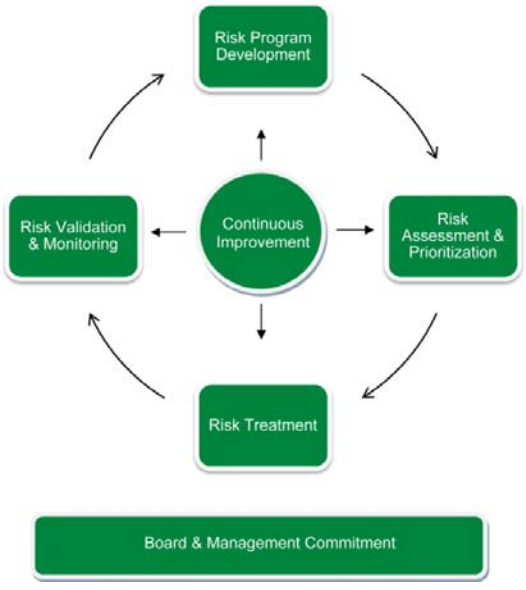
Two critically important factors are the level of support your ERM initiative has from the board and executive management, and whether the initiative has a driven and enthusiastic champion.

As a guide, if you haven't identified your risks and performed a comprehensive risk assessment, that's where you should start. At the same time, culture and governance issues discussed earlier should be explored using surveys and facilitators. For simplicity, you could start with your organizational strategic plan and any existing internal risk assessments (e.g., internal audit, Sarbanes-Oxley 404, financial reporting risk disclosures, fraud assessments) and build on these to address your organization's full range of risks and consider introducing more robust risk measures. Standard risk listings and descriptions are readily available.

A four-phase ERM methodology

A pragmatic, four-phase approach to ERM helps organizations address the core components of risks and establish a risk management framework sized for their specific needs. The ERM strategy should be fluid and effective so significant risks are properly identified, prioritized, treated and monitored. All while the basics of a common risk language, scope and materiality are maintained and communicated to everyone involved in the risk management process. The extent to which an organization completes this process and the timescale associated with the implementation is entirely organization-specific.

Enterprise Risk Management Methodology



Phase one: Risk program development

In this first phase of implementation, priority is given to the design and development of the ERM strategy and program. This phase includes:

- Identification of the ERM sponsor or champion and the core team or ERM committee
- An assessment of the organization's tone at the top, risk appetite and scope evaluation

- Development of a common risk language
- Determination of risk materiality
- Confirmation of the project scope
- Customization of ERM tools and templates

At the end of phase one, you'll have a solid foundation for risk identification and assessment.

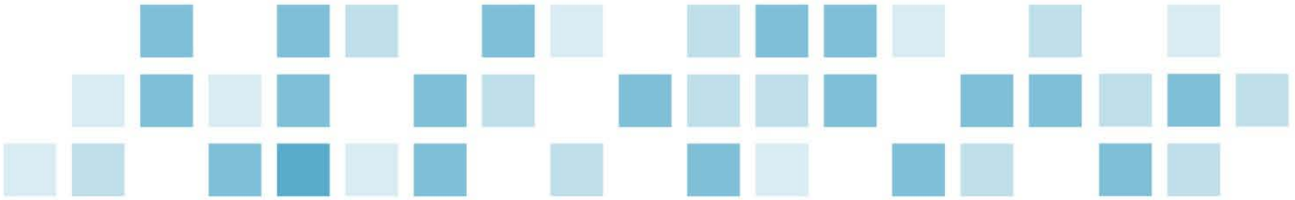
Phase two: Risk assessment and prioritization

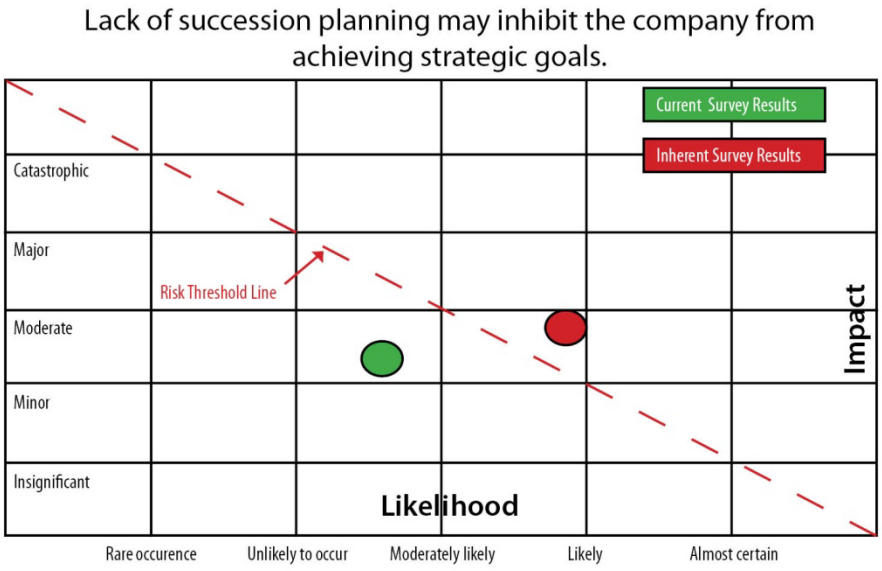
The second phase focuses on identifying and documenting the organization's portfolio of risks. Specific tasks include:

- Completing surveys and interviews with select members of management to identify, discuss and capture enterprise risks
- Evaluating all functional areas and comparing them to risk universes or libraries to facilitate the organization's identification of significant risks
- Categorizing risks within the ERM integrated Committee of Sponsoring Organizations of the Treadway Commission (COSO) elements to allow for clarification, analysis, additional research as necessary and reporting. The ERM Integrated COSO elements include:
    - Strategy
    - Operations
    - Reporting
    - Compliance

    Note: Further categorization by sub-classification (risk themes) or process may be necessary or helpful for analysis and reporting
- Reviewing identified risks with the ERM champion or committee to confirm and establish the risk population for prioritization
- Ranking and prioritizing the identified risks according to:
    - Impact – The financial implications to the organization in the event the risk occurs
    - Likelihood – The probability the risk may occur within the business operations (reference the following chart)

      Note: Further ranking and prioritizing may include risk direction, scale or scope of risk impact, velocity or speed of risk outcomes and interdependencies of individual risks.

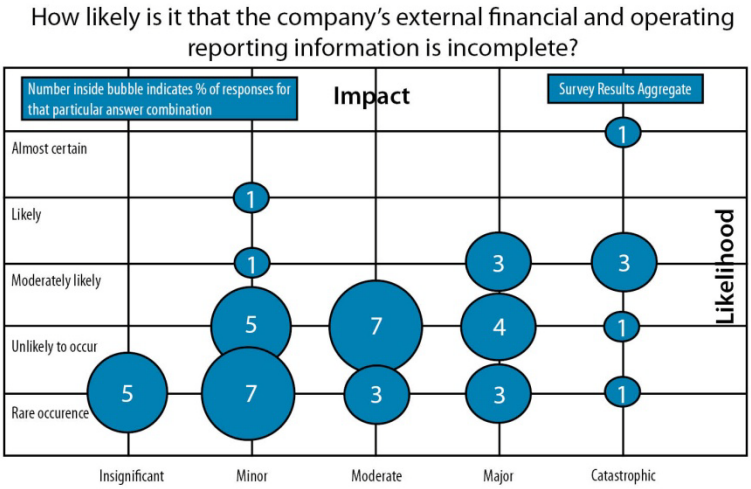




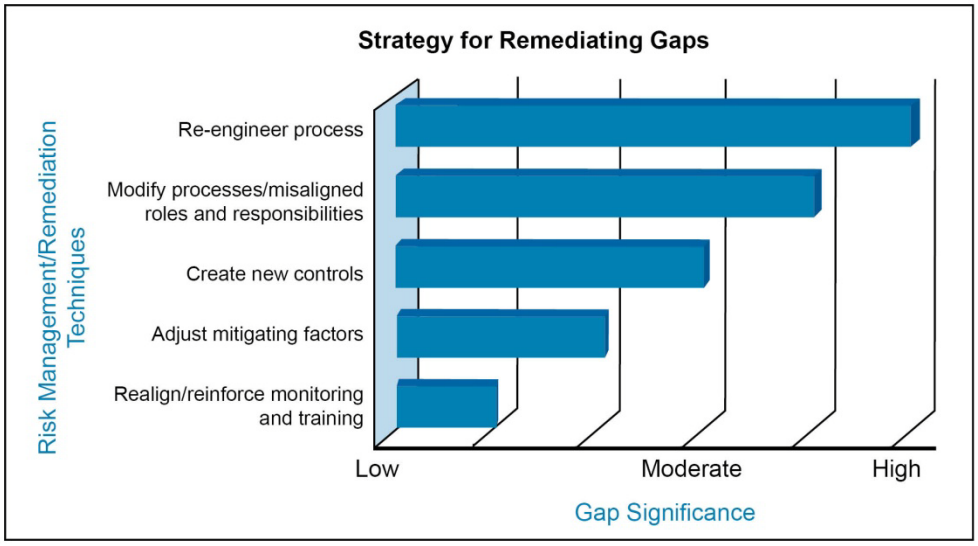
- Coordinating a facilitated session with the ERM committee and select members of management to evaluate the prioritization results and discuss:
  - Agreement with risk prioritization
  - Questions or concerns relative to the risk prioritization
  - High and moderate risks to evaluate impact and likelihood factors for understanding of overall risk exposure
  - Risks with significant deviation/spread in prioritization to gain insight on variation (reference the following chart)

Phase three: Risk treatment

The third phase of ERM implementation focuses on risk treatment strategies. This phase includes discussing and identifying mitigation strategies for the prioritized risks and defining the organization's risk appetite and tolerance. Additionally, control gaps or improvement opportunities should also be discussed and identified. This process is completed by:



- Identifying the risk treatment for high and moderate risks
- Coordinating with the ERM committee and key members of management to discuss and evaluate risk treatment strategies, including:
  - Agreement with specific mitigation plans or control analysis
  - Agreement with identified control gaps or improvement opportunities
  - Evaluation of known design and effectiveness measures for mitigating strategies or controls
- Remediating gaps or improving the implementation strategy, including identifying or creating sub-teams, as appropriate (see the following chart)



Phase four: Risk validation and monitoring

The final phase is designed to establish a validation strategy for each key risk. Validation can be completed using a variety of assessment options, including:

- Control self-assessment
- Internal audit
- Third-party assistance

The key to this phase is the effective design of a validation plan that verifies the mitigating strategies are designed and working as intended. Additionally, an ongoing monitoring and reporting strategy (executive level dashboard) should be customized so key risks are routinely monitored and reported.

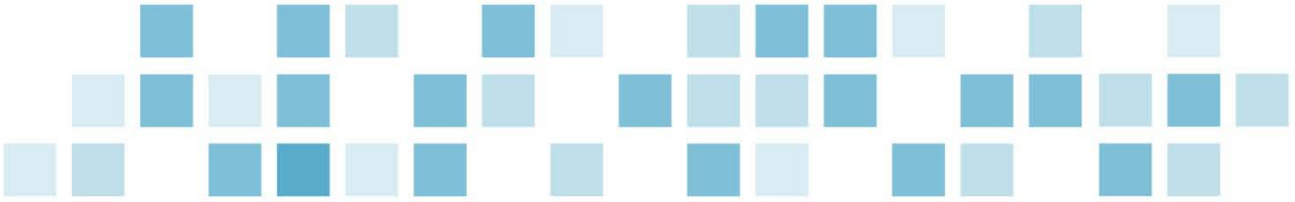
Implementing ERM can yield many benefits

An effective, pragmatic ERM program can drive risk awareness throughout the organization. Best of all, implementation doesn't have to be difficult. Our four-phase approach, described earlier, starts by identifying your risks and performing a comprehensive risk assessment and ends with risk validation and monitoring.

By following that road map, you should reach your destination and, hopefully, reap ERM's many potential benefits:

- Better information to optimize earnings and organizational value
- Clearer communication about management's goals and capabilities
- A competitive advantage through improved business performance
- Optimized risk management costs

While it's true you can't operate a business without risk—you can definitely minimize your risk exposure through an effective, pragmatic ERM program.



800.274.3978
www.mcgladrey.com