Enterprise Risk Management - A Practical Approach
Maryland Financial Bank Advisory Board

April 14, 2011

RSM McGladrey, Inc.

Introductions

John Brackett, CPA, CFSA, MBA
Risk Advisory Managing Director
Charlotte, NC

Matt McKercher
Director
Baltimore, MD

McGladrey

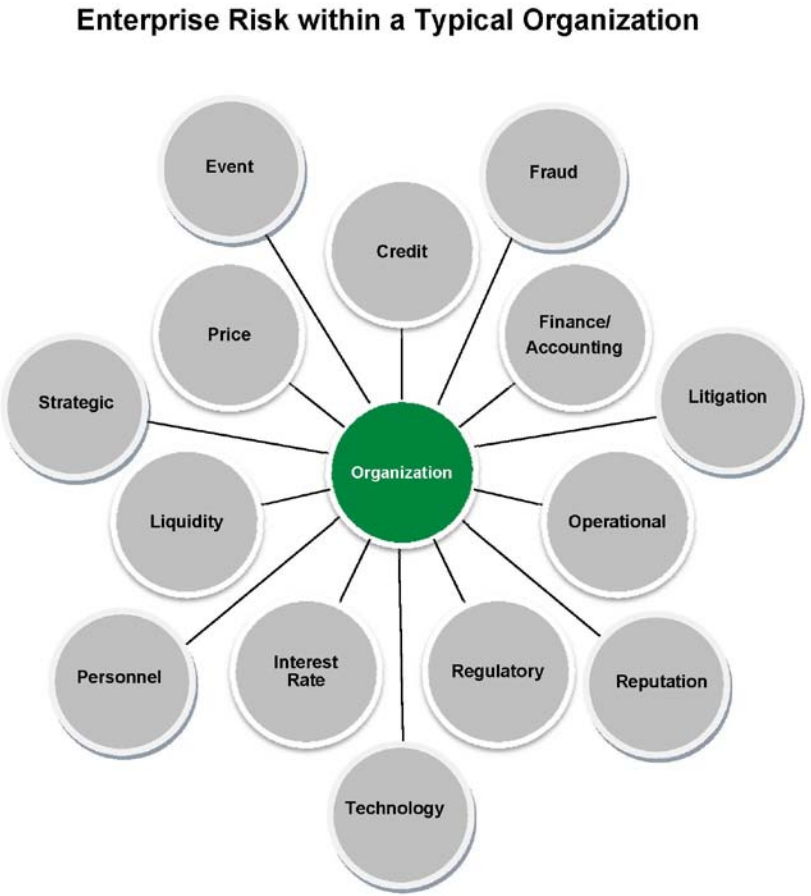
ERM Awareness

- *Do you continue to search for another solution for managing risks within your organization?*
- *Are compliance costs continuing to escalate but the value received from such efforts is remaining stagnant?*
- *Are you frustrated by the duplication of effort to manage risks and maintain a corporate governance framework?*
- *Have you reached the conclusion that disciplined risk management is no longer an option but could, in fact, be a differentiator and competitive advantage?*

McGladrey

ERM Awareness

Risk factors associated with accounting, regulatory compliance, information technology, strategy, operations and other aspects of your business can be difficult to manage because these functions are rarely integrated and have their own unique management challenges.



McGladrey

ERM Awareness

It is critical to understand the complexity of managing business risks and the resulting increase in exposure by not effectively identifying and monitoring such risks. Risks, if not managed and appropriately mitigated, could have a serious impact on your company's profitability and reputation.

- Identification
- Prioritization
- Evaluation
- Monitoring

McGladrey

What is ERM? - Definition

McGladrey

What is ERM? - Definition

- From the Institute of Internal Auditors Position Paper (January 2009): The Role of Internal Auditing in Enterprise-wide Risk Management:

  "Enterprise-wide risk management (ERM) is a structured, consistent and continuous process across the whole organization for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives"

What is ERM? - Objectives

- To create, protect and enhance shareholder value by better ensuring the sustainability of an organization and enabling it to meet its objectives
- Provide a management-supported common risk management framework and language across the enterprise
- Create and maintain a consistent process to identify, assess and mitigate material risks
- Clearly defined roles and responsibilities across the organization for managing risk

What is ERM? - Responsibility

- The Board of Directors has overall responsibility for ensuring that risks are managed
- The Board will delegate operation of the risk management framework to the management team
- Each management team will set up roles and responsibilities for managing risk in a way that differs by organization
- Everyone in the company ultimately plays a role in ensuring successful enterprise-wide risk management. Primary responsibility for risk identification and management will always reside with management

ERM Perspective

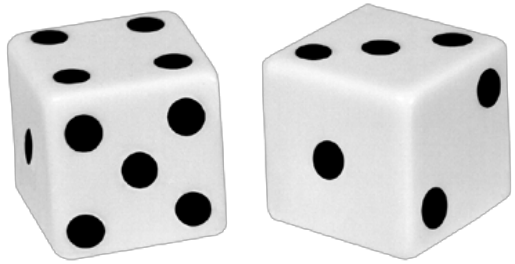
Effective ERM enlists proactive techniques to create a risk management plan that is strategic to your organization including:

- Establishing a formal, disciplined framework and governance strategy for effective risk management
- Formalizing the process to identify all key risks within the organization
- Developing quantitative and qualitative factors to measure potential risk attributes including impact, likelihood, pervasiveness, trending direction
- Quantifying risks, examining risk treatment, and determining risk gaps through effective gap analysis
- Establishing effective and manageable risk monitoring processes and continuous improvement activities
- Minimizing disruptions or hurdles that have an impact on your company's ability to achieve its objectives
- Significantly reducing the cost of risk management

Why is ERM important?
Why have an ERM strategy?

ERM enhances an organization's ability to do the following:

- Reconcile strategic objectives and organizational risk tolerance (appetite)
- Increase likelihood of achieving objectives
- Support educated strategic, operational and financial decisions
- Anticipate and respond timely to emerging risks
- Identify and share cross-business risks
- Maximize profitability through risk analysis
- Minimize operational expenses and losses
- Reduce surprises or losses
- Strategically train and allocate resources
- Create a proactive regulatory environment



McGladrey

ERM Methodologies

The most common internationally accepted frameworks or standards:

- ISO 31000:2009 (Published November 13, 2009)
  - Superseded ASNZ 4360:2004, previously one of the most commonly accepted international frameworks

- Committee of Sponsoring Organizations of the Treadway Commission - COSO
  - ERM – Integrated framework (’04)

ISO 31000:2009 vs. AS/NZ 4360:2004

According to the International Standardization Organization (ISO – www.iso.org):

"ISO 31000 provides principles, framework and a process for managing any form of risk in a transparent, systematic and credible manner within any scope or context."

- Kevin W. Knight, Chair of the ISO working group that developed the standard explains:

"*All organizations, no matter how big or small, face internal and external factors that create uncertainty on whether they will be able to achieve their objectives. The effect of this uncertainty is 'risk' and it is inherent in all activities.*

ISO 31000 is a practical document that seeks to assist organizations in developing their own approach to the management of risk. But this is not a standard that organizations can seek certification to. By implementing ISO 31000, organizations can compare their risk management practices with an internationally recognized benchmark, providing sound principles for effective management."

ISO 31000:2009 vs. AS/NZ 4360:2004

7 Step Risk Management Process Implicit in both ISO 31000:2009 and AS/NZ 4360:2004

Committee of Sponsoring Organizations of the Treadway Commission (COSO)

- *ERM – Integrated Framework issued in 2004*
- National commission was sponsored by five professional associations
  - American Accounting Association (AAA)
  - American Institute of Certified Public Accountants (AICPA)
  - Financial Executives Institute (FEI)
  - Institute of Internal Auditors (IIA)
  - Institute of Management Accountants (IMA)
- Commission also contained representatives from industry, public accounting and academia

ERM Integrated Framework – COSO Model

Internal Environment
Risk management culture
Risk tolerance
Ethics and core values

Objective Setting
Organization objectives align with strategy and risk tolerance

Event Identification
Identification of internal and external opportunities and threats

Risk Assessment
Risks are identified and measured (impact & probability)

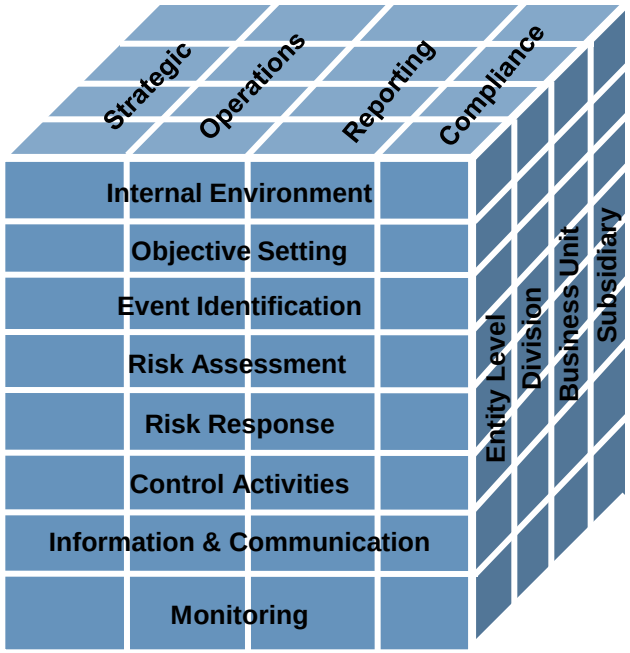
Risk Response
A risk management strategy is selected (evade, reassign, accept, exploit)

Control Activities
Policies and procedures
Standard operating procedures

Information & Communication
Communication throughout the company
Timeliness and accuracy of data

Monitoring
Continuous monitoring
Remediation as necessary

The COSO Model

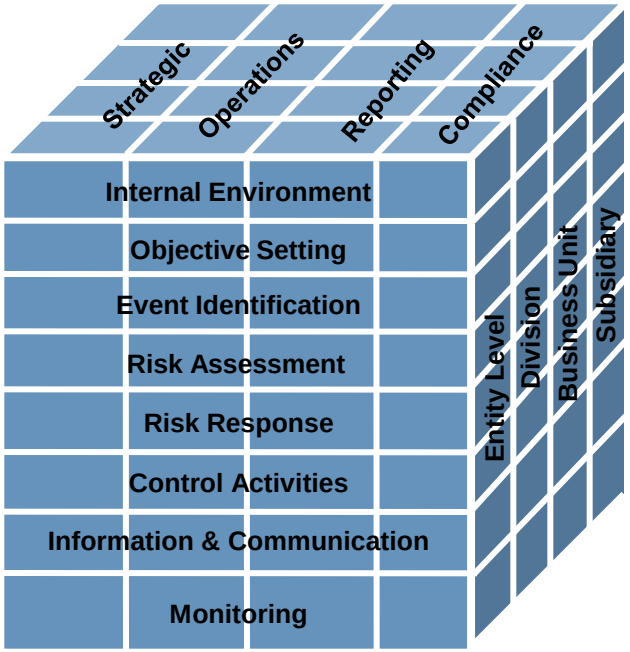


McGladrey

ERM Integrated Framework – Which One?

AS/NZ Model

The COSO Model

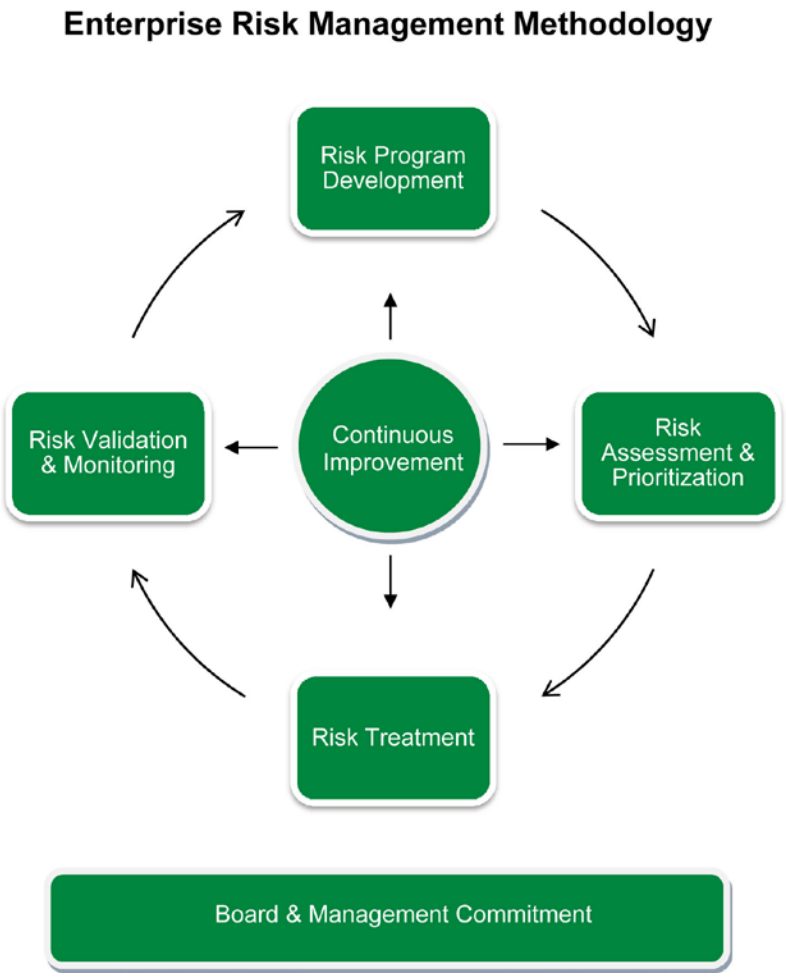


McGladrey

Applied ERM Methodology

Methodology overview

- ERM program is divided into four phases:
  - Risk Program Development
  - Risk Assessment & Prioritization
  - Risk Treatment
  - Risk Validation & Monitoring



McGladrey

Applied ERM Methodology

Phase 1 – Risk Program Development

- In this phase, we design and develop the foundation of the ERM program. This first phase includes:
  - Identification of the ERM sponsor or champion and the core team
  - An assessment of the company's tone-at-the-top, materiality assessment and risk appetite
  - Development of a common risk language
  - Confirmation of the project scope
  - Customization of tools and templates to the ERM program

Applied ERM Methodology

Phase 2 – Risk Assessment & Prioritization

- In Phase II, you identify and formally document a portfolio of risks within your organization. In this phase you will:
  - Complete a limited number of interviews with select members of management to identify and discuss enterprise risks
  - Identify and capture a sufficient risk population relevant to the functional areas to allow significant risks to be identified
  - Risks will be captured and categorized by the following ERM Integrated COSO elements
    - Strategy
    - Operations
    - Reporting
    - Compliance
  - Further categorize risk by sub-classification or process

Applied ERM Methodology

Phase 2 – Risk Assessment & Prioritization (cont.)

- Review the identified risks with the ERM sponsor or champion to establish and determine the risk population for prioritization
- Rank and prioritize the identified risks according to:
  - Impact – the financial implications in the event the risk occurs
  - Likelihood – the probability the risk may occur within business operations
- Coordinate a facilitated session with the ERM core team to evaluate the prioritization results and discuss:
  - Agreement with the risk prioritization
  - Questions or concerns relative to the risk prioritization
  - High and moderate risks to evaluate impact and likelihood factors for clarification and understanding of overall risk exposure
  - Risks with significant deviation/spread in prioritization results to gain insight on variation

Applied ERM Methodology

Phase 3 – Risk Treatment

- Phase III will allow you to identify and assess how each key risk is mitigated and identify existing control gaps. In this phase you:
  - Identify risk treatment for high and moderate risks
  - Coordinate a discussion with the ERM core team to evaluate risk treatments and discuss:
    - Agreement with mitigation analysis
    - Identified control gaps
    - Evaluate design and known effectiveness of mitigating strategies
    - Risk management strategy
      1. Avoid
      2. Retain
      3. Reduce
      4. Transfer
    - Gap remediation strategy

McGladrey

Applied ERM Methodology

Phase 4 – Risk Validation & Monitoring

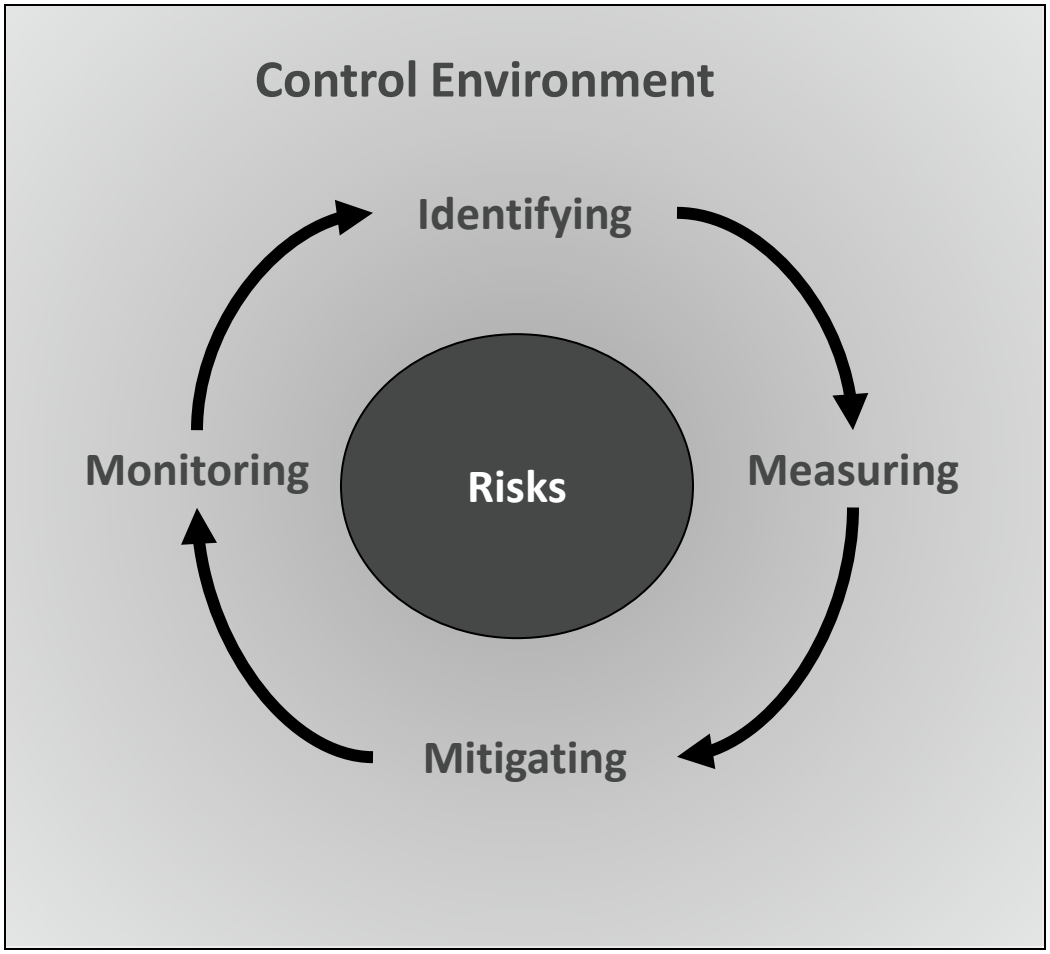
- In Phase IV, you establish a validation strategy for each key risk. Validation can be completed by utilizing many options including
  - Control self-assessments
  - Internal audit
  - Third-party assistance

The key is to effectively design a validation plan to ensure the mitigating strategies are designed and working as intended.

Additionally, an ongoing monitoring and reporting strategy should be customized so key risks are routinely monitored and reported.

What is ERM? – Back to the Definition

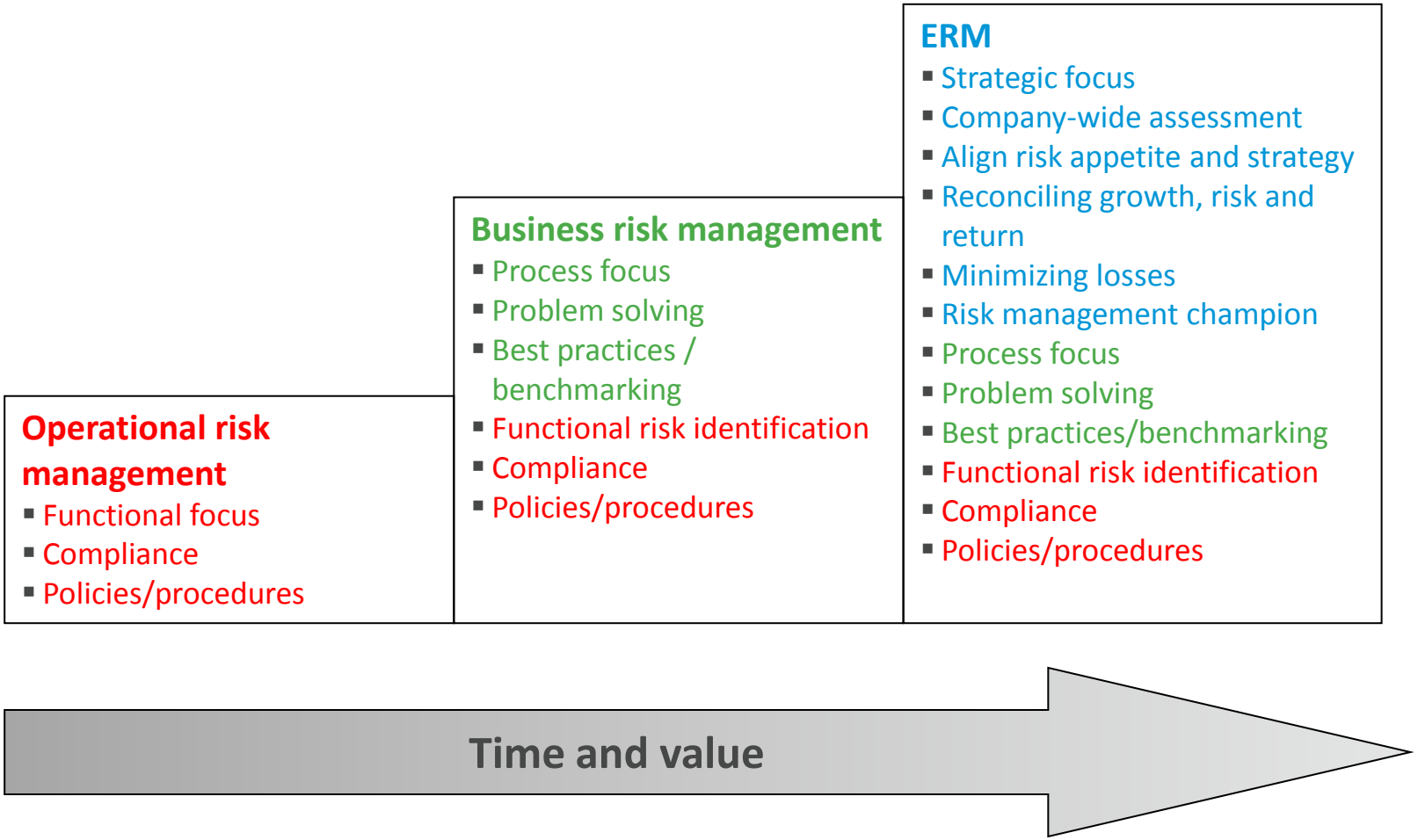
A company-wide control environment that identifies, measures, mitigates and monitors risks.



McGladrey

The Evolution of ERM

The risk management continuum



McGladrey

Practical ERM Implementation – Keys to Success

McGladrey

Practical ERM Implementation – Keys to Success

- Strong support by executive management is critical
- Identify specific (not vague) risks and potential impact
- Accountability (for risk and mitigation) – clear communication throughout executive management is imperative
- Clear understanding of the organization's risk appetite, as defined by the Board
- Focus on top risks
- Link risks to goals and strategy; tailor the initiative to the organization's specific business processes, objectives & strategies
- Understand that ERM is a framework and not an instruction manual or project-task for management to complete in a short time period and check off the list (it may never be "complete")

Limitations of ERM

- Assumptions often include past performance or future projections – both may be incorrect
- ERM should be appropriately scoped for each company and expectations should be documented
- Business process and controls can breakdown or be overridden
- The governance process is dependent on coordination and collaboration of the core team, which is dependent on individual participation
- Ongoing maintenance is dependent on commitment and contribution from all employees (everyone is responsible for risk management)
- ERM should be a tool not a rule

The Future of ERM

- Risk management today
  - Fragmented and inconsistent risk identification and analysis
  - Reports are generated but not reviewed or updated for business changes
  - Quantitative analysis is historical and is not used to quantify opportunities or manage the business
  - Risk management is Internal Audit's responsibility

- Risk management tomorrow
  - Risk identification and analysis efforts are coordinated and centralized (risk champion)
  - Risk management reporting is included at all levels and used for managing the business
  - Quantitative analysis is used in decision making, managing the business and success quantification
  - Risk management is my responsibility

The Future of ERM

- Next steps for your organization
  - Identify the company's approach to managing risk
  - Inventory current risk management tools/methodologies within the organization
  - Identify the ERM champion
  - Start at the top – what is the tone at the top
  - Identify and measure operational risks (source not symptom)
  - Develop and implement a risk management strategy (roles and responsibilities)
  - Assess results, redefine the process and continuously improve
  - Drive risk management to every level within the organization

ERM – Internal Audit's Role

- Provide objective assurance to the Board of Directors on the organization's effectiveness of risk management
- This can include a number of activities but should NOT include:
  - Setting the risk appetite
  - Imposing risk management processes
  - Deciding upon or implementing risk responses
  - Owning responsibility for risk management

APPENDIX

Appendix – Sample Risk Assessment Documents: Risk Assessment Questionnaire

Name	
Department	
Instructions	Please answer the questions below. There are no right or wrong answers and candid information is very much appreciated. When evaluating risks, please identify risks **without** considering existing controls or mitigating strategies. Your input is critical to this process and we appreciate your time spent on the questionnaire. Space is available at the end of each section for additional comments. Comments are strongly encouraged; they help clarify responses and provide constructive focus. Individual responses will remain anonymous. We expect this questionnaire to take approximately 20 to 30 minutes to complete. Please return the questionnaire to Joe Smith at: joesmith@hotmail.com. If you have any questions, contact Jane Smith at 303.555.3820 or Joe Smith at 303.555.1514. Please complete and email the survey by May 13th.

#	Question
1	What is your understanding of the company's strategic objectives?

2	What is your understanding of your department's strategic objectives?

McGladrey

Appendix – Sample Risk Assessment Documents: Risk Assessment Questionnaire

3	Risk Identification (Please identify as many risks as you think appropriate or relevant for each section below.)	
3.1	Environmental Risks	
	Risks that arise when factors in the environment may significantly change the fundamentals that drive a company's overall objectives and strategies.	
	Examples may include: Competitor, Customer Desires, Innovation, Political Changes, Regulatory, Industry, Legal, Financial Markets, or Catastrophic Loss	
	1	
	Comments	

3.2	Process Risks	
	Risks that arise when business processes are not clearly defined, communicated or aligned with business strategy; perform ineffectively; do not meet customer needs; or expose financial or intellectual assets to loss or misuse.	
	Examples may include: Operations - Knowledge Capital, Product Development, Efficiency, Capacity, Sourcing, Channel Effectiveness, Partnering, Compliance, Business Interruption, or Trademark/Brand Erosion Leadership - Management Monitoring, Authority Limit, Performance Incentives, or Communication Financial - Price, Liquidity, or Credit Fraud - Management,, Employee, Illegal Acts, or Unauthorized Use	
	1	
	2	
	Comments	

McGladrey

Appendix – Sample Risk Assessment Documents: Risk Assessment Questionnaire

3.3	Decision Management
	Risks that arise when information used to support business decisions is not reliable, pertinent, or accurate.
	Examples may include: Operational - Product Pricing, Contract Commitments, or Plant Metrics Business Reporting - Budget, Forecasting, Accounting, Taxation, Treasury, Benefit Management, or Financial Reporting Strategic - Organizational Structure, Resource Allocation, or Portfolio Analysis

	1	
	Comments	

4	Are there any other areas within the company that could prevent you from meeting corporate or departmental objectives?

5	How does the company's IT environment / infrastructure prevent or enable the achievement of departmental goals?

6	What risks does the company or your department face relative to HR/people (e.g., skill sets, cross-training, succession planning, recruitment, retention, etc.)?

Appendix - Sample Documents: Risk Analysis - Risk Measurement

Risk Tolerance:

The following criteria was used to assess, rank, and measure each risk identified by management. The scale was also used as a guideline and reference point for discussions. Original risk ranking was completed for inherent state (without consideration of current mitigating strategies or controls) and for current state (considering mitigating strategies or controls). The following information presented in this analysis is based on the current state assessment.

Likelihood of Occurrence Descriptions

- **1 – Rare Occurrence** – Event may only occur in exceptional circumstances
- **2 – Unlikely to Occur** – Event could occur at some time
- **3 – Moderately Likely** – Event should occur at some time
- **4 – Likely** – Event will probably occur in most circumstances
- **5 – Almost Certain** – Event is expected to occur in most circumstances

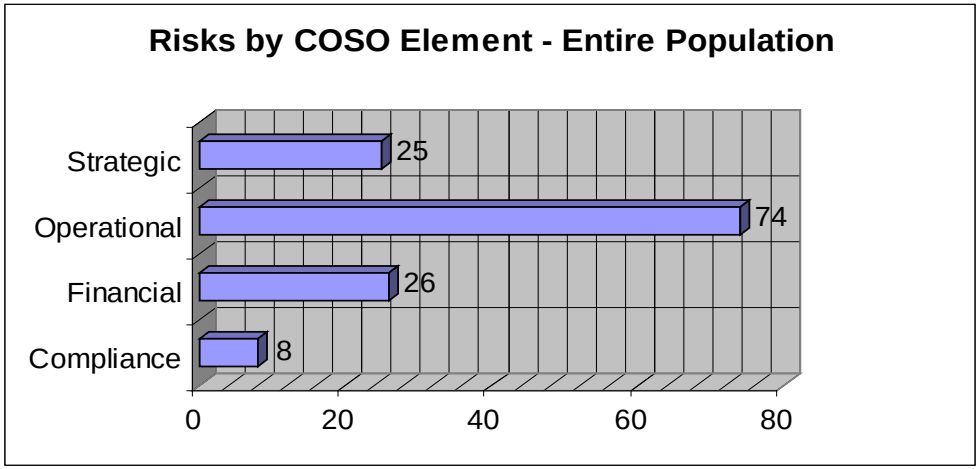
Impact Descriptions

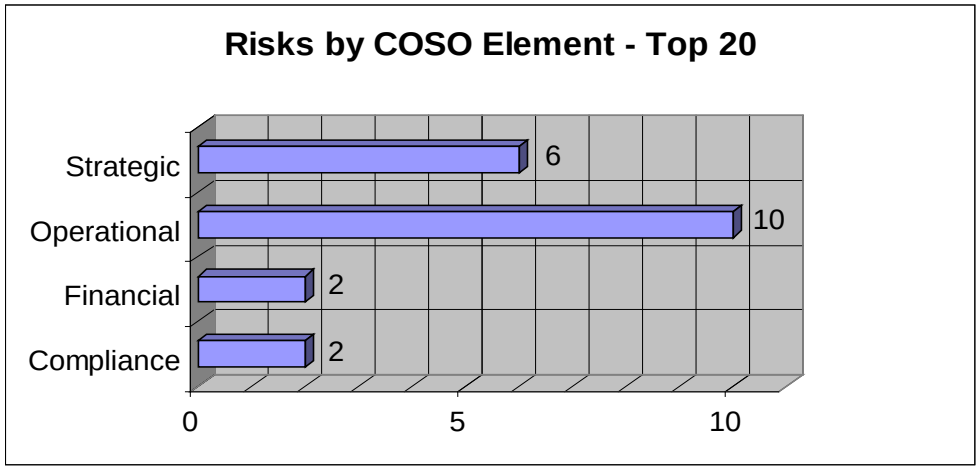
- **1 – Insignificant** – Event will result in a loss of **$0 - $100,000**
- **2 – Minor** – Event will result in a loss of **$100,000 - $500,000**
- **3 – Moderate** – Event will result in a loss of **$500,000 - $1,000,000**
- **4 – Major** – Event will result in a loss of **$1,000,000 - $10,000,000**
- **5 – Catastrophic** – Event will result in a loss of **$10,000,000 +**

Appendix – Sample Documents: Risk Analysis – Entire Population & Top 20

Identified Risks – COSO Categorization:

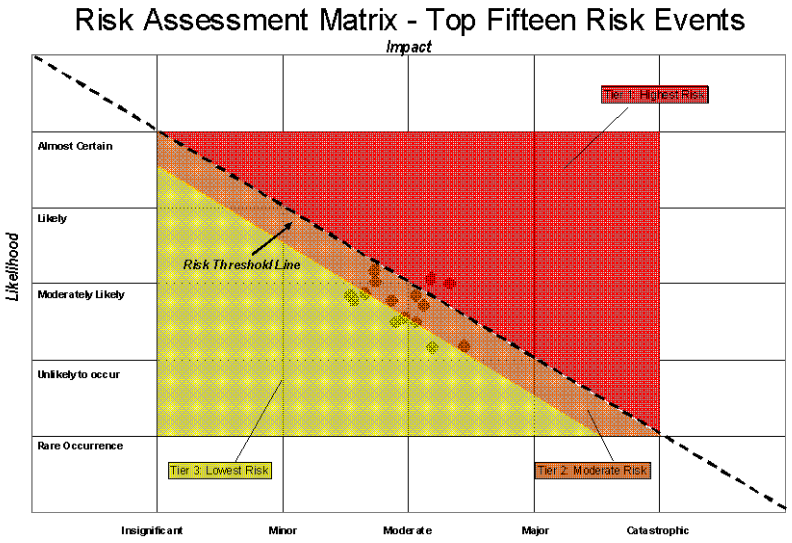
The following graphs portray the risk categories by COSO element for both the entire population and the Top 20 risks.

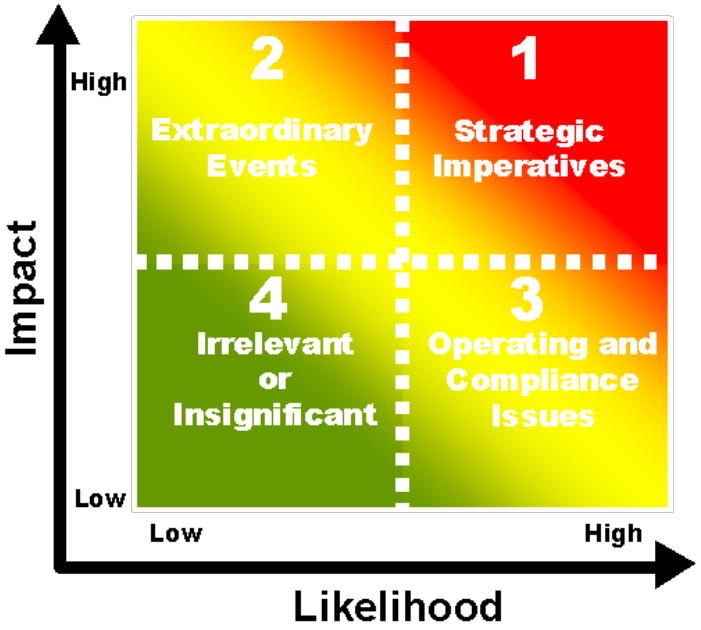




McGladrey

ERM Examples

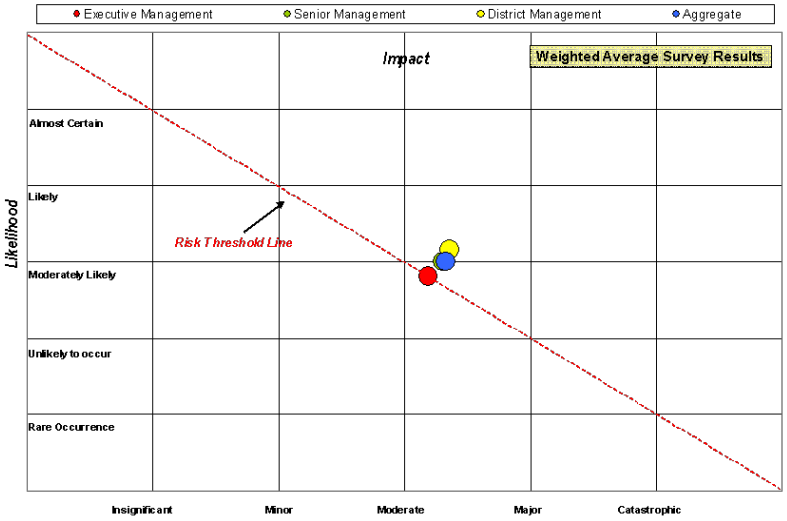




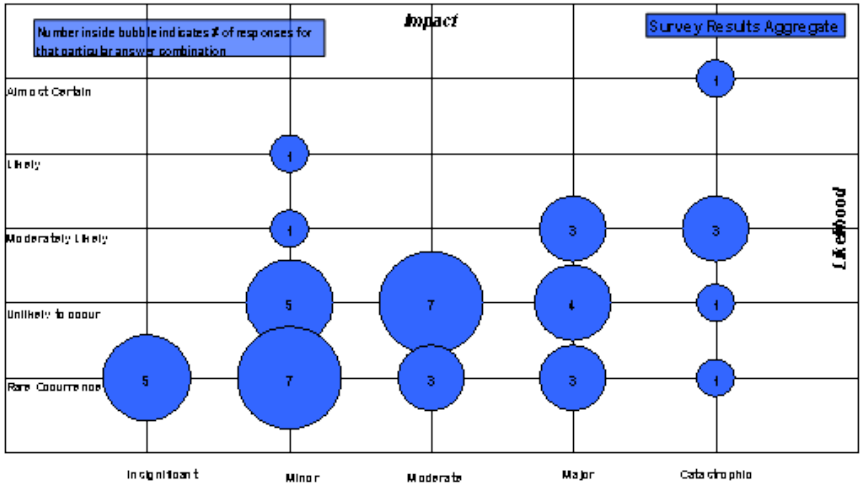
McGladrey

ERM Examples

Question 31: How likely is it that the company would fail to meet strategic goals?



Question 42: How likely is it that the company's external financial and operating reporting information is incomplete?



McGladrey

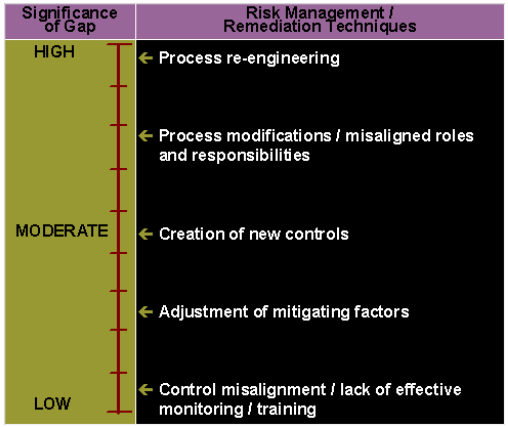
ERM Examples

AVOID	• Divest • Eliminate • Stop
RETAIN	• Accept • Plan • Self insure
REDUCE	• Mitigate • Control
TRANSFER	• Insure • Securitize • Reinsure • Share • Hedge • Outsource • Indemnity

Gap Remediation Strategy

Considerations Impacting Risk Management / Remediation Techniques

- Severity/Volatility of Risk
- Process Complexity
- Availability of Data
- Desired Capability
- Cost Benefit Analysis
- Time to Correct
- Cross-silo Implications



McGladrey

QUESTIONS?

McGladrey