Enterprise Risk Management

State of Maine September 25, 2013

McGladrey

Assurance • Tax • Consulting

Introductions

- Paul Kiley
  - Director, McGladrey-Risk Advisory Services
  - Boston, MA

McGladrey

Agenda

Topic	Minutes
ERM History & Overview	15 minutes
ERM Frameworks	30 minutes
ERM Detailed Approach	45 minutes
Tools & Techniques	15 minutes

McGladrey

Objectives

By the end of this session, you should:

- Understand key concepts related to ERM
- Gain exposure to implementation approaches
- Be familiar with voting technology and facilitated sessions
- See how ERM works in the real world

McGladrey

Poll

- Resolver Ballot is the tool we use for live facilitated sessions.
- We will use it more later, but let's do a quick vote now…

McGladrey

ERM History & Overview

Risk

"Never in all history have we harnessed such formidable technology. Every scientific advancement known to man has been incorporated into its design. The operational controls are sound and foolproof!"

E.J. Smith: Captain of the Titanic

McGladrey

6

History of Corporate Risk

- 1930's- Corporate failures lead to SEC
- 1980's-S&L Crisis
- 2001- Enron/WorldCom/Andersen
- 2008-Financial Crisis

Organizations are more concerned than ever about:

- Risk Management
- Governance
- Control
- Assurance (and Consulting)

McGladrey

Evolution of ERM

Historically
- Risks managed in silos

1990s
- First "Chief Risk Officer"
- First use of ERM terminology
- Risk-related regulatory requirements (e.g., Turnbull)

2000s
- September 11
- Corporate scandals / beginning of efforts to improve corporate governance (e.g., Sarbanes-Oxley)
- Recession and financial services industry failure
- Government bailouts resulting in public scrutiny and higher compliance requirements

McGladrey

Recent Guidance Timeline

- *2004-COSO ERM Framework Released*
- *2007- S&P "flirted" with applying ERM program as a factor in bond ratings for non-financial companies. "Clarified" in 2010*
- *2009- NACD Blue Ribbon Commission*
- *2009- SEC Proxy disclosures directly mention oversight for risk management*
- *2009- ISO 31000*

McGladrey

Introduction to Business Risk

- What is a business risk?
  - The threat that an event or action/inaction will adversely affect an organization's ability to ***achieve its business objectives*** and execute its strategies effectively
  - *OR*
  - Something bad will happen
  - Something good won't happen

McGladrey

ERM Definitions

Institute of Internal Auditors

"…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."

COSO ERM Integrated Framework (2004)

"…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."

ISO 31000 (2009)

"A systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk."

McGladrey

4

What ERM Is and Isn't

ERM IS…

- ✓ A disciplined approach to what previously had no process
- ✓ A way to get more out of an organization's risk management practices
- ✓ Tied to Corporate goals and objectives
- ✓ A link between risk management and business decision-making
- ✓ Applicable to most organizations

McGladrey

What ERM Is and Isn't

ERM ISN'T…

- ✓ Scientific
- ✓ Mutually exclusive from risk management
- ✓ The same as an IA risk assessment
- ✓ An extension of Internal Audit or Compliance
- ✓ A regulatory requirement for most organizations…yet
- ✓ A guarantee of eliminating surprises

McGladrey

Why ERM Is Important

Underlying principles:

- Every entity, whether for-profit or not, exists to realize value for its stakeholders.
- Value is created, preserved, or eroded by management decisions in all activities, from setting strategy to operating the enterprise day-to-day.

McGladrey

Traditional Risk Management vs. ERM

Traditional Risk Management	ERM
Tactical, compliance focused	Strategic, performance focused
Silo-based processes	Consistent risk management approach across the enterprise
Business line or risk type view	Holistic view of key risks
Looks at risks individually	Considers risk interactions
Business decisions not closely linked to risks	Business decisions based on a clear understanding of risks
Driven by Risk Management and Internal Audit	Driven by the board and owned by the business
Supported by rules	Supported by a "risk culture"

McGladrey

15

ERM Jump Start

- Many companies are interested in developing an ERM program, but have trouble defining what this means in their organization.
  - Various factors affect the way ERM is executed at companies, including their ***size, management culture, prior/current risk assessment activities, mandate and buy-in from executives and the Board***, etc.

- ERM has been described as a **"journey" rather than a "destination".**
- The key is to begin that journey, without trying to get it perfect on the first iteration
- Remember the 3 definitions, there is not really a "right" or "wrong" way to do ERM. It is not like SOX

McGladrey

16

ERM Value

"A rattlesnake may bite us every now and again, but we knew it was there and how much it might hurt…"

Rick Buy, Executive Vice President and Chief Risk Officer…

Enron, 2000

McGladrey

Key Benefits of an ERM Program

1. To ensure that business decisions are fully informed of potential risks
   - Awareness of the key risks facing the firm is heightened at the business line, executive and board level

McGladrey

Key Benefits of an ERM Program

2. To reduce operational and financial surprises
   - Risk identification, assessment and monitoring processes are forward-looking and consider worst case risks before they result in losses

McGladrey

Key Benefits of an ERM Program

3. To ensure that capital resources are adequate for the firm's overall risk profile
   - All risk types are considered (not just credit risk)
   - Actual risks are compared to a risk appetite that is aligned with risk-taking capacity

McGladrey

Key Benefits of an ERM Program

4. To optimize risk/reward relationships across the firm
   - Risks of all types are measured consistently across the firm, allowing the firm to target profitable segments and manage risk/reward imbalances

McGladrey

Key Benefits of an ERM Program

5. To recognize and manage firm-wide risks
   - Holistic view includes risk interactions and risk concentrations not evident at the business unit level (such as Ford palladium story)

McGladrey

Key Benefits of an ERM Program

6. To gain efficiencies
   - Risk monitoring and response processes are prioritized and focused on the highest risks to the firm

McGladrey

Why ERM Is Important?

ERM supports value creation by enabling management to:

- Gain a common understanding of the risks they are facing
- Deal effectively with potential future events that create uncertainty.
- Respond in a manner that reduces the likelihood of downside outcomes and increases the upside.

McGladrey

Risk Measurement Continuum

Key Factors Impacting Selection of Risk Measurement Methodologies

- **Severity or Volatility of Risk.**
- **Desired Frequency of Reporting.**
- **Desired Level of Precision.**
- **Cost of Implementation.**

Degree of Sophistication	Risk Measurement/ Analytical Techniques
HIGH	• Probability Distributions-Based Modeling (At Risk Frameworks, Stress Testing) • Performance Measurement (Cost, Quality, Time) • Dynamic Simulation Modeling (Scenario Analysis)
MODERATE	• Risk Scoring Techniques • Systematic Exposure Analysis • Qualitative Risk Indicator Analysis
LOW	• Group Facilitated Self-Assessment • Individual Self-Assessment

McGladrey

ERM "Common Sense"

Having an approach to attend to key risks

Making conscious decisions about which risks to take

Knowing your risk tolerance

Having a "Plan B"… and a "Plan C"

Avoiding outsized risks

Being resilient

ERM is a language to communicate all of the above

McGladrey

ERM "Nonsense"

Eliminating all risks

Cramming together disparate policies

Solely compliance/disclosure requirements

Replacement for internal controls

A shiny new software program

Naming a CRO and calling it a day

These mindsets can actually hinder effectiveness

McGladrey

27

ERM Implementation

- Key in understanding ERM:
  - "Risk … is good. The point of risk management is not to eliminate it. That would eliminate reward. The point is to manage it – that is, to choose where to place bets, and where to avoid betting altogether." Thomas Stewart, Fortune Magazine

McGladrey

28

ERM Framework

Enterprise Risk Management — Integrated Frameworks

In order to implement ERM, it makes sense to use a model or framework

ERM frameworks define essential components, suggest a common language, and provide clear direction and guidance for enterprise risk management.

The most widely used frameworks are COSO and ISO-31000

McGladrey

ERM Frameworks ISO 31000

International Recognition

ISO 31000:2009 provides:

"… generic guidelines for the design, implementation and maintenance of risk management processes throughout an organization. This approach to formalizing risk management practices will facilitate broader adoption by companies who require an enterprise risk management standard that accommodates multiple 'silo-centric' management systems."

The scope of this approach to risk management is to enable all strategic, management and operational tasks of an organization throughout projects, functions, and processes to be aligned to a common set of risk management objectives.

McGladrey

COSO

Enterprise Risk Management — Integrated Framework (2004)

McGladrey

Enterprise Risk Management — Integrated Framework

This COSO ERM framework defines essential components, suggests a common language, and provides clear direction and guidance for enterprise risk management.

Not changing with the 2013 updated internal control framework.

McGladrey

Elements of a successful ERM process

- ***Core Team Preparedness*** – Establishing a core team, with representation from business units and key support functions, including strategic planning, is an important first step. This team becomes intimately familiar with the framework's components, concepts, and principles. This familiarity provides a common understanding and language, and a foundational basis needed to design and implement an enterprise risk management process that effectively addresses the entity's unique needs.

- ***Executive Sponsorship*** – While the timing and form of executive sponsorship vary by organization, it is important that executive sponsorship be initiated early and solidified as implementation progresses. Executive leadership articulates the benefits of enterprise risk management, and establishes and communicates the business case for the related investment of resources. CEO support, and usually at least initial direct and visible involvement, drives success.

From COSO ERM Framework

McGladrey

34

Elements of a successful ERM process

- ***Implementation Plan Development*** – An initial plan is created for the next steps, setting out key project phases, including defined work streams, milestones, resources, and timing. Responsibilities are identified, and a project management system put in place. The plan serves as a means to consistently communicate and coordinate with team leadership, and as a basis for communicating and confirming expectations of various units and personnel, and discussing entity-wide changes anticipated from adopting enterprise risk management.

- ***Current State Assessment*** – This includes an assessment of how enterprise risk management components, concepts, and principles currently are being applied across the entity. This usually involves ascertaining whatever risk management philosophy has evolved within the organization and determining whether there is uniform understanding of the entity's risk appetite. The core team also identifies formal and informal policies, processes, practices, and techniques currently in place, as well as existing capabilities in the organization for applying the framework's principles and concepts.

From COSO ERM Framework

McGladrey

35

Elements of a successful ERM process

- ***Enterprise Risk Management Vision*** – The core team develops a vision that sets out how enterprise risk management will be used going forward and how it will be integrated within the organization to achieve its objectives – including how the organization focuses its enterprise risk management efforts on aligning risk appetite and strategy, enhancing risk response decisions, identifying and managing cross-enterprise risks, seizing opportunities, and improving deployment of capital.

- ***Capability Development*** – The current state assessment and the enterprise risk management vision provide insights needed to determine the people, technology, and process capabilities already in place and functioning, as well as new capabilities that need to be developed. This includes defining roles and responsibilities, and modifications to the organizational model, policies, processes, methodologies, tools, techniques, information flows, and technologies.

From COSO ERM Framework

McGladrey

Elements of a successful ERM process

- ***Implementation Plan*** – The initial plan is updated and enhanced, adding depth and breadth to cover further assessment, design, and deployment. Additional responsibilities are defined, and the project management system refined as needed. The plan typically embraces general project management disciplines that are a part of any implementation process.

- ***Change Management Development and Deployment*** – Actions are developed as needed to implement and sustain the enterprise risk management vision and desired capabilities – including deployment plans, training sessions, reward reinforcement mechanisms, and monitoring the remainder of the implementation process.

- ***Monitoring*** – Management will continually review and strengthen risk management capabilities as part of its ongoing management process.

From COSO ERM Framework

McGladrey

Components of Enterprise Risk Management

Enterprise risk management consists of eight interrelated components. These are derived from the way management runs an enterprise and are integrated with the management process. These components are:

- ***Internal Environment*** – The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
- ***Objective Setting*** – Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.

.

McGladrey

Components of Enterprise Risk Management

Event Identification – Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective-setting processes.

Risk Assessment – Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.

Risk Response – Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the entity's risk tolerances and risk appetite.

.

McGladrey

39

Components of Enterprise Risk Management (continued)

• ***Control Activities*** – Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.

• ***Information and Communication*** – Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity.

• ***Monitoring*** – The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

Enterprise risk management is not strictly a serial process, where one component affects only the next. It is a multidirectional, iterative process in which almost any component can and does influence another.

McGladrey

40

The ERM Framework

- Entity objectives can be viewed in the
- context of four categories:
  - Strategic
  - Operations
  - Reporting
  - Compliance

McGladrey

The ERM Framework

ERM considers activities at all levels of the organization:

- Enterprise-level
- Division or subsidiary
- Business unit processes

McGladrey

The ERM Framework

Enterprise risk management requires an entity to take a *portfolio view* of risk.

McGladrey

The ERM Framework

- Management considers how individual risks interrelate.
- Management develops a portfolio view from two perspectives:
  - Business unit level
  - Entity level

McGladrey

The ERM Framework

The eight components
of the framework
are interrelated as you
move through the Cube…

McGladrey

Internal Environment

- Establishes a philosophy regarding risk management. It recognizes that unexpected as well as expected events may occur.
- Establishes the entity's risk culture.
- Considers all other aspects of how the organization's actions may affect its risk culture.

McGladrey

Objective Setting

- Is applied when management considers risk strategy in the setting of objectives.
- Forms the risk appetite of the entity — a high-level view of how much risk management and the board are willing to accept.
- Risk tolerance, the acceptable level of variation around objectives, is aligned with risk appetite.

McGladrey

Event Identification

- Differentiates risks and opportunities.
- Events that may have a negative impact represent risks.
- Events that may have a positive impact represent natural offsets (opportunities), which management channels back to strategy setting.

McGladrey

Event Identification

- Involves identifying those incidents, occurring internally or externally, that could affect strategy and achievement of objectives.
- Addresses how internal and external factors combine and interact to influence the risk profile.

McGladrey

Risk Assessment

- Allows an entity to understand the extent to which potential events might impact objectives.
- Assesses risks from two perspectives:
  - Likelihood
  - Impact
- Is used to assess risks and is normally also used to measure the related objectives.

McGladrey

Risk Assessment

- Employs a combination of both qualitative and quantitative risk assessment methodologies.
- Relates time horizons to objective horizons.
- Assesses risk on both an inherent and a residual basis.

McGladrey

Risk Response

- Identifies and evaluates possible responses to risk.
- Evaluates options in relation to entity's risk appetite, cost vs. benefit of potential risk responses, and degree to which a response will reduce impact and/or likelihood.
- Selects and executes response based on evaluation of the portfolio of risks and responses.

McGladrey

Control Activities

- Policies and procedures that help ensure that the risk responses, as well as other entity directives, are carried out.
- Occur throughout the organization, at all levels and in all functions.
- Include application and general information technology controls.

McGladrey

Information & Communication

- Management identifies, captures, and communicates pertinent information in a form and timeframe that enables people to carry out their responsibilities.
- Communication occurs in a broader sense, flowing down, across, and up the organization.

McGladrey

Monitoring

Effectiveness of the other ERM components is monitored through:

- Ongoing monitoring activities.
- Separate evaluations.
- A combination of the two.

McGladrey

Internal Control

A strong system of internal control is essential to effective enterprise risk management.

McGladrey

Relationship to *Internal Control — Integrated Framework*

- Expands and elaborates on elements of internal control as set out in COSO's "control framework."
- Includes objective setting as a separate component. Objectives are a "prerequisite" for internal control.
- Expands the control framework's "Financial Reporting" and "Risk Assessment."

McGladrey

COSO Risk Model

External Factors

Economic	*Natural Environment*	*Political*	*Social*	*Technological*
• Capital availability • Credit issuance, default • Concentration • Liquidity • Financial markets • Unemployment • Competition • Mergers/acquisitions	• Emissions and waste • Energy • Natural disaster • Sustainable development	• Governmental changes • Legislation • Public policy • Regulation	• Demographics • Consumer behavior • Corporate citizenship • Privacy • Terrorism	• Interruptions • Electronic commerce • External data • Emerging technology

Internal Factors

Infrastructure	*Personnel*	*Process*	*Technology*
• Availability of assets • Capability of assets • Access to capital • Complexity	• Employee capability • Fraudulent activity • Health and safety	• Capacity • Design • Execution • Suppliers/ dependencies • Mergers/acquisitions	• Data integrity • Data and system availability • System selection • Development • Deployment • Maintenance

McGladrey

58

Components of an Effective ERM Program

Range of Scalable ERM Practices

Firm size

Small firm ERM practices

- Policies for each risk type
- Decisions based primarily on management judgment
- CFO or other executive responsible for risk oversight
- Less board involvement / reliance on Audit Committee
- Manual aggregation processes
- Tactical risk management training

Large firm ERM practices

- Formally documented ERM framework
- Decisions based on complex, data-driven analysis
- ERM function and CRO
- Active board and Risk Committee involvement
- Highly automated aggregation and reporting processes
- ERM training based on a common risk language

McGladrey

60

Roles and Responsibilities

Three Lines of Defense

1st	Business Lines and Functions	"**Own**" the risks associated with their activities
2nd	Risk Management	Designs & coordinates the implementation of the ERM program
3rd	Internal Audit	Validates the effectiveness of the ERM program, including management's actions to address risks

McGladrey

Internal Audit's Role in ERM

- Boards require objective assurance that risk management processes are working and key risks are being managed effectively.
- Internal (or external) auditors respond to this need by giving assurance on:
  - The appropriateness of the company's ERM framework
  - The accuracy of risk and control assessments
  - The effectiveness of risk management processes
  - The appropriateness of management's actions to address risks
  - The accuracy of risk reports

McGladrey

62

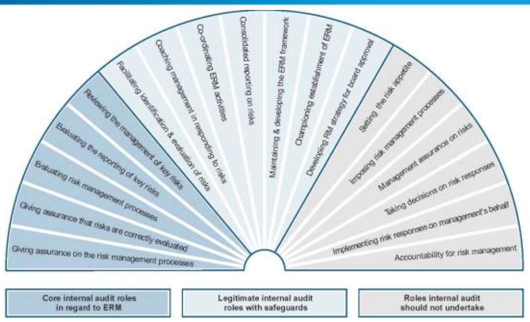
Internal Audit's Role in ERM

- In smaller firms, Internal Audit may play a larger role in developing and overseeing the ERM framework, with appropriate safeguards to protect their independence.
  - Audit should not be involved in actually managing risk, as this is the responsibility of the management team.
  - Audit's responsibilities should be documented and approved by the Audit Committee.
  - Audit cannot give objective assurance on any part of the ERM framework for which it is responsible.
  - Audit should not undertake any ERM responsibilities in which the function does not have adequate expertise.

McGladrey

63

IIA Depiction of Internal Audit Roles…



McGladrey

Internal Auditors

- Play an important role in monitoring ERM, but generally should NOT have primary responsibility for its implementation or maintenance.
- Assist management and the board or audit committee in the process by:
  - Monitoring - Evaluating
  - Examining - Reporting
  - Recommending improvements

McGladrey

Internal auditors can add value by:

- Reviewing critical control systems and risk management processes.
- Performing an effectiveness review of management's risk assessments and the internal controls.
- Providing advice in the design and improvement of control systems and risk mitigation strategies.

McGladrey

Internal auditors can add value by:

- Implementing a risk-based approach to planning and executing the internal audit process.
- Ensuring that internal auditing's resources are directed at those areas most important to the organization.
- Challenging the basis of management's risk assessments and evaluating the adequacy and effectiveness of risk treatment strategies.

McGladrey

Internal auditors can add value by:

- Facilitating ERM workshops.
- Defining risk tolerances where none have been identified, based on internal auditing's experience, judgment, and consultation with management.

McGladrey

Assessing Needs

- Discussions with management should start with questions to develop an understanding of the organization's objectives
- This information can be used to determine ways that Internal Audit can help, such as through:
  - A review of their overall approach to ERM and recommendations on ways to improve
  - Guidance in developing specific ERM program components (e.g., Risk Appetite or ERM Policy)
  - Hands-on assistance in building ERM components, such as an enterprise-wide risk assessment

McGladrey

ERM Key Components

Keys to success:

- Providing a methodology vs. a completed assessment to ensure the process is sustainable
- Starting with a clear view of the desired outputs of the assessment (such as heat maps)
- Conducting facilitated risk assessment sessions with business managers
- Developing and adhering to common definitions
- Including risks inherent in business activities – even if they haven't yet been experienced by the organization

McGladrey

ERM Program Components

- A strong risk culture
- Effective risk governance
- Risk appetite
- Enterprise-wide risk management processes
  - Risk identification and assessment
  - Risk measurement
  - Risk responses
  - Risk monitoring and reporting
- Integration of risk management and strategy
- Independent validation

McGladrey

ERM Implementation

Risk Education

- Conceptual understanding by the Board and Executive Management
  - Why implement ERM?
    1. What is the purpose?
    2. What is the vision?

- Anticipated results
  - Value derived from a calculated risk taken or avoided due to preparedness

- How much does the company already know about risk management?
  - Tailor the approach based on existing knowledge

McGladrey

72

ERM Program Components

Business strategy is central to ERM

McGladrey

Risk Culture

Ways that Organizations can establish a strong risk culture:

- **"Tone at the top"** that communicates the importance of risk management
- **Code of Conduct**
- Risk management factors included in **incentive and performance evaluation** plans
- Clearly defined **roles and responsibilities** that are consistent with three lines of defense

McGladrey

Risk Governance

McGladrey

Risk Appetite

- An effective ERM program relies on the establishment and communication of the company's risk appetite
  - Helps employees to understand the specific risks that the company is willing and not willing to take.
  - Provides a means for ensuring that actual risk-taking is consistent with the company's risk-taking capacity.

McGladrey

76

Risk Appetite

- There are many ways to define risk appetite:
  - Statements, such as "a zero tolerance for compliance risk" or "target debt rating of AAA"
  - Specific products, markets and/or customer segments that are outside of the company's risk tolerance
  - Metrics that define risk thresholds, such as financial measures (e.g., ROE target) or limits (e.g., % of total risk exposure)

Are you able to articulate your company's appetite or tolerance for risk?

McGladrey

77

How to begin…

ERM Implementation Approach

COSO Key Implementation Factors

1. Organizational design of business
2. Establishing an ERM organization
3. Performing risk assessments
4. Determining overall risk appetite
5. Identifying risk responses
6. Communication of risk results
7. Monitoring
8. Oversight & periodic review by management

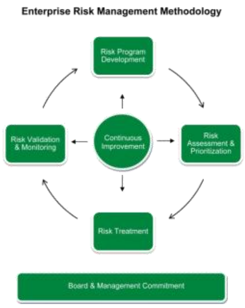
McGladrey

ERM Framework

Framework overview

The ERM process is broken into four phases including:

- Risk program development
- Risk assessment & prioritization
- Risk treatment
- Risk validation & monitoring



McGladrey

ERM Framework

Phase 1 – Risk Program Development

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, which is the level of risk a company is prepared to accept before action is required
- Development of a common risk language
- Determination of risk materiality
- Confirmation of the project scope
- Customization of tools and templates to your ERM program

McGladrey

Risk Culture

Development of a risk culture is critical to effective ERM

Ways to establish a risk culture that is supportive of risk management:

- "Tone at the top"
  - Reference the importance of risk management in the company's objectives
  - Incorporate risk management into ongoing executive management communications
  - Exhibit the desired risk management behaviors
- Code of Conduct or Ethics
- Risk management factors included in incentive and performance evaluation plans
- Clearly defined roles and responsibilities that are consistent with three lines of defense

McGladrey

83

Key Questions:

- Do you have Board and C-Level buy in?
- Does the organization take other aspects of accountability and measurement seriously?
- Will the culture allow sustainable risk management?
- What level do you want to start at for the first iteration? (Enterprise, business unit, etc.)

McGladrey

ERM Framework

Phase 2 – Risk Identification & Prioritization Cont.

- Identify the risks in the organization through various methods, including interviews, surveys and workshops
- 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, operational, strategy and compliance implications to the Client in the event the risk occurs
  - **Likelihood** – the probability the risk may occur within business operations
  - **Other Criteria-** Control Effectiveness, Velocity

McGladrey

Risk Identification

- Risk identification processes should begin with appropriate planning:
  - Mapping of the company's business lines and processes
  - Determination of the risk types to be included in the process (e.g., operational, legal, reputational)
  - Identification of resources responsible for the process in each area
- Risks can be identified through various methods, such as interviews, surveys and/or facilitated workshops
  - Different levels of the organization may have different perspectives on risks
  - Include emerging risks
  - Be wary of risks that are really the absence of controls

McGladrey

86

Open Risk Identification Questionnaire

- Review Risk Identification Process

McGladrey

ERM Framework

Phase 2 – Continued

- Coordinate a facilitated session with the ERM core team (or executives) 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 in results / spread in prioritization results to gain insight on reasons for variation

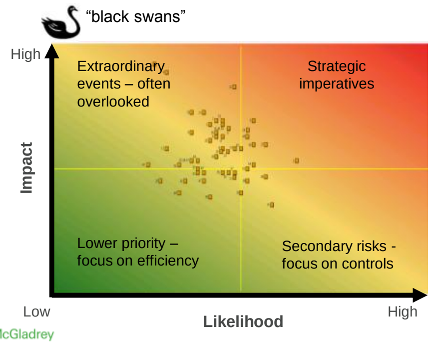
McGladrey

Facilitated Sessions

- Facilitated sessions are one of the most important tools in the ERM arsenal
- Get senior executives offsite for AT LEAST ½ a day
- They wont want to do it, but later they will say it added the most value of the whole effort

McGladrey

Sample Risk Assessment Voting Output



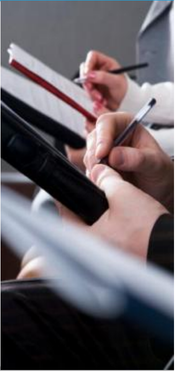
McGladrey

ERM Framework

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 we will:

- 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 risk gaps
  - Evaluate design and known effectiveness of mitigating strategies
  - Risk management strategy
    1. Avoid
    2. Retain
    3. Reduce
    4. Transfer
  - Gap remediation strategy



McGladrey

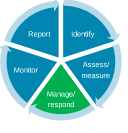
Risk Management / Responses

- Risk responses should be based on assessment of loss frequency and impact
  - Management actions should be specific to reducing likelihood or impact, depending on which one was assessed as high

The most common risk responses include:

- Avoid (get out)
- Accept/retain (monitor)
- Reduce (institute controls)
- Transfer or share (partner with someone)

- Action plans with assigned owners should be developed and monitored by a risk committee



McGladrey

92

ERM Framework

Phase 4 – Risk Validation & Monitoring

In Phase IV, we will work with you to 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

McGladrey

ERM Framework

Phase 4 – Risk Validation & Monitoring Continued

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.

McGladrey

Risk Monitoring and Reporting

Risk monitoring should:

- Be focused on the highest risks
- Include forward-looking key risk indicators (KRIs)

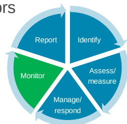
Risk reports should:

- Be effectively summarized
- Include analysis and recommendations
- Compare risks to thresholds/limits

McGladrey

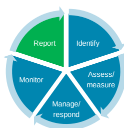
Risk Monitoring

- Risk monitoring should follow from risk assessments
  - Higher risks should be monitored more frequently and in more depth
- Key risk indicators (KRIs) are critical to early identification of risks and, as a result, fewer surprises
  - KRIs should be forward-looking
  - Key Performance Indicators (KPIs), are primarily backward-looking



Risk Reporting

- Reporting should also follow from risk assessments, with higher risks reported in more depth
- Emphasis of risk reporting should be on highlighting *key risks* and recommendations for and status of *management action*
- Volumes of detail should be avoided, particularly for board reporting
- Reports should include early indicators and emerging risks
- Best practices include the development of ERM dashboards that provide a holistic view of risk and thoughtful analysis



Management Oversight & Periodic Review

- Accountability for risks
- Ownership
- Updates
  - Changes in business objectives
  - Changes in systems
  - Changes in processes

Integrating ERM into decision-making

- To be effective and sustainable, risk management must be integrated into day-to-day business line activities and corporate decisions
  - Risk Managers must be involved at the onset of strategy setting processes
  - Risks associated with new products should be considered and communicated to the board
  - Analysis of emerging risks and stress tests should influence business decisions
  - Risk information should be shared across the company to avoid the same event recurring

McGladrey

99

Our ERM perspective

Our ERM perspective includes:

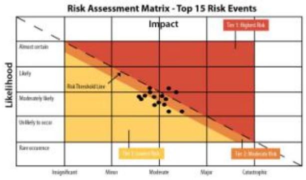
- Establishing a formal, disciplined framework and governance strategy for effective risk management
- Formalizing the process to identify all key risks within the organization
- Developing quantitative and qualitative factors to measure potential risk impact and likelihood
- Quantifying risks, examining risk treatment, and determining risk gaps through effective gap analysis
- Establishing effective and manageable risk monitoring processes and continuous improvement activities
- Significantly reducing the cost of risk management

Our ERM perspective allows you to enlist our **proactive risk management techniques** to create a risk management plan that is strategic to your organization.

McGladrey

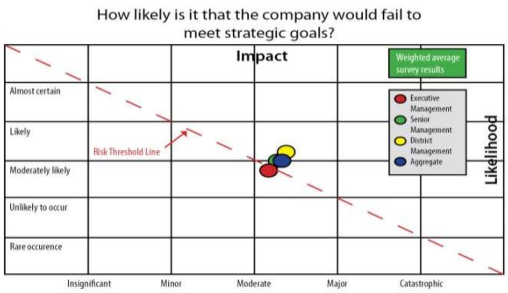
Tools and Outputs

ERM examples



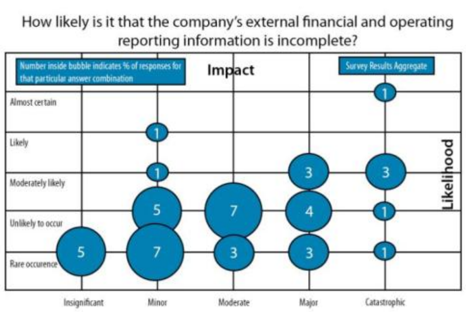
McGladrey

ERM examples



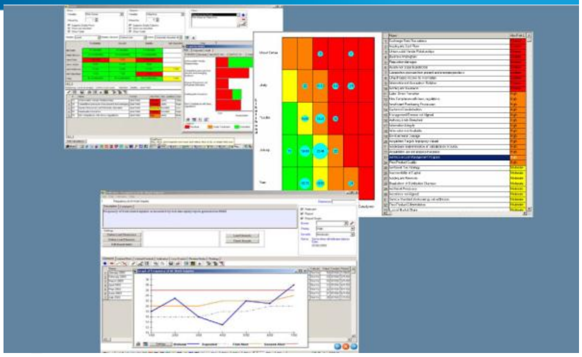
McGladrey

ERM examples

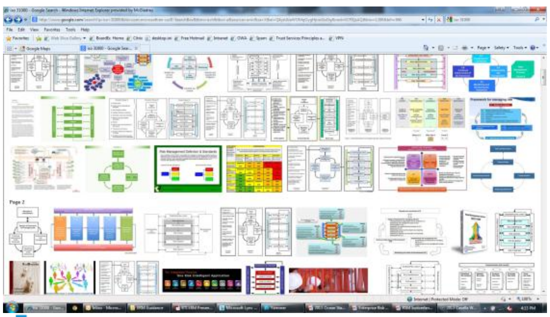


McGladrey

Examples of Tools

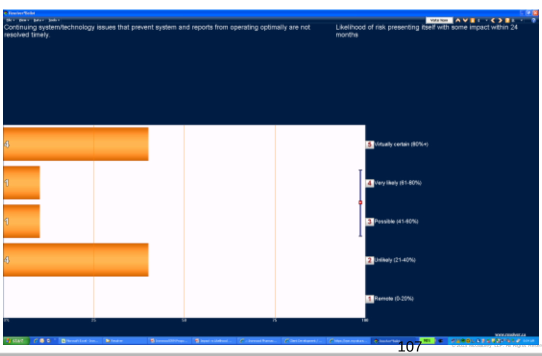


Graphics

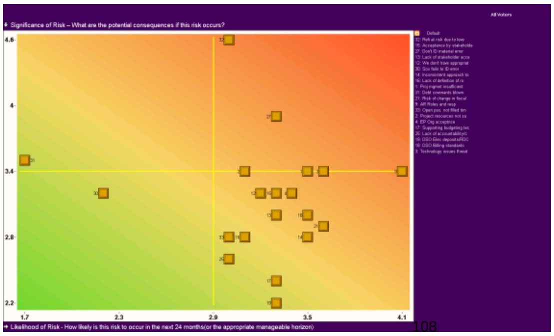


McGladrey

Tools- BPS Resolver Voting Software



Tools- BPS Resolver Voting Software



108

Sample Risk Inventory

Company Name
Division
Function
Sub Function (if applicable)
Fiscal Year

Risk Number	Risk Description	Strategic Goal/ Objective	Business Unit	System used	Likelihood	Impact	F/S Account	Key Measure	Effectiveness	Residual Risk Likelihood	Residual Risk Impact	Residual Risk Total Ratings
1	Not meeting sales targets	Maximizing sales	Operations	Oracle	3	3	Revenue	Strategic	1	1	1	2
2	Not meeting marketing goals	Improve product visibility	Marketing	Oracle	2	2	Cash	Strategic	2	2	2	4
3			Human Resources		5	4	Accounts Receivab	Strategic	5	5	5	10
4			Accounting		4	5	Prepaids	Continuing Operations	4	4	4	8
5			Executives		2	2	Cash	Strategic	1	1	1	2
6			Advertising		4	4	Inventory		5	1	1	2
7			Payroll		3	5	Intangible Assets	Financial	1	1	1	2
8			Events		3	3	Cash	Strategic	4	1	1	2
9			Executive		1	3	Cash	Compliance	3	1	1	2
10			Plant Production		5	5	Expenses	Strategic	3	1	1	2
11			Manufacturing		5	3	Revenue	Compliance	1	1	1	2
12			Department		5	4	Equity	Strategic	4	1	1	2
13			Customer Service		3	3	Cash	Continuing Operations	4	1	1	2
14			Inventory		3	4	Intangible Assets	Continuing Operations	1	1	1	2
15			Relationships		4	5	Cash	Compliance	3	1	5	6

McGladrey

109

Sample Dashboard Report

Company ABC
Enterprise Risk Assessment
FY10

DASHBOARD VIEW OF "TOP" RESIDUAL RISKS

No.	Inherent Rank	Residual Rank	Risk Description	Strategic Goal/ Objective	Impact	Likelihood	Inherent Risk (Impact * Likelihood)	Control Effectiveness	Control Effectiveness (Squared)	Residual Risk (Inherent risk * control effectiveness)	Changes/ Notes	Owner	Risk Response/ Action Plan (Should Be Measurable)	Due Date	X/XX Status
Finance															
8	1	1	The risk that we are not utilizing ERP software to automate processes and maximize efficiency and effectiveness	Cut cost of finance and optimize control environment	3.4	4.1	13.94	3.5	12.25	48.79		Jane Doe	Jane Doe will perform an analysis of ERP capabilities and a gap analysis of those currently used. She will then prepare an action plan to implement automated controls.	xx/xx/2010	Open
11	11	16	The risk that we have not complied with all relevant tax laws.	Compliance with laws and regs.	3.4	3.1	10.54	3	9	31.62		John Doe	John Doe will develop a compliance matrix in conjunction with the Company's tax consultants which will be reviewed quarterly to ensure all relevant Tax laws are being complied with.	xx/xx/2010	Complete
Strategic															
7	3	2	The risk that we we are not prepared to bring a drug to market when we reach that phase including development of marketing and supply chain	Successfully market a commercial drug	5	2	10.00	2	4	20.00		Suzy Q.	Low residual risk. No response required other than ongoing monitoring of control effectiveness by Suzy Q.	xx/xx/2010	Deferred

McGladrey

110

McGladrey LLP

One South Wacker Drive, Suite 800
Chicago, IL 60606
312.634.3400

www.mcgladrey.com

McGladrey

Assurance • Tax • Consulting