Measuring the Effectiveness of Your Enterprise Risk Management (ERM) System

Charlie Wright, CIA
Director, Enterprise Risk Solutions
BKD
Measuring ERM Effectiveness

Overview

– Evolving ERM Frameworks
– Implications for Internal Audit
– Ideas for assessing ERM effectiveness
Measuring ERM Effectiveness

COSO defines “Enterprise Risk Management” …

– 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 risks to be within its risk appetite,
– to provide reasonable assurance regarding the achievement of entity objectives.
Highlights of COSO ERM Update

– Restructures entire focus of the framework
  • “Aligns Risk with Strategy and Performance”
– Updates components and adopts principles
– Emphasizes value, integration and culture
Measuring ERM Effectiveness
Measuring ERM Effectiveness

Five Components

- Governance and Culture
- Risk, Strategy and Objective-Setting
- Execution
- Information, Communication and Reporting
- Monitoring ERM Performance
Measuring ERM Effectiveness

Twenty-three Principles

- Supports the five components
- Adherence suggests comprehension and management of risks
- Principle-based guidance provides practical and flexible language
Revised Definitions

Risk

The possibility that events will occur and affect the achievement of strategy and business objectives.
Measuring ERM Effectiveness

Risk

The possibility that events will occur and affect the achievement of strategy and business objectives

Enterprise Risk Management

The culture, capabilities, and practices,
Measuring ERM Effectiveness

- **Risk**: The possibility that events will occur and affect the achievement of strategy and business objectives.
- **Enterprise Risk Management**: The culture, capabilities, and practices, integrated with strategy and execution.
Measuring ERM Effectiveness

Risk

The possibility that events will occur and affect the achievement of strategy and business objectives

Enterprise Risk Management

The culture, capabilities, and practices, integrated with strategy and execution, that organizations rely on to manage risk
Measuring ERM Effectiveness

Risk

The possibility that events will occur and affect the achievement of strategy and business objectives

Enterprise Risk Management

The culture, capabilities, and practices, integrated with strategy and execution, that organizations rely on to manage risk in creating, preserving, and realizing value
Measuring ERM Effectiveness

Emphasizes value, integration and culture

– Creating, preserving and realizing value
– Risk management - integrated into strategy development and organizational performance
– Culture affects risk decision-making
Measuring ERM Effectiveness

- Does not replace the 2013 *Internal Control – Integrated Framework*
- The two frameworks are distinct and complementary
- Both use components and principles
- Commonalities of internal control to enterprise risk management are not repeated
Measuring ERM Effectiveness

Summary of Framework Changes

– Aligns risk with strategy and performance
– More principles-based and focused on value
– Emphasizes the importance of culture
– Focuses on integration of business processes and decision making
– Differentiates ERM from internal controls
Polling Question #1

What is your perception of the proposed COSO framework?

1) It is a much-needed improvement.
2) A change was needed, but this doesn’t hit the mark.
3) I don’t know yet. Let’s wait and see the final version.
4) I don’t like it.
Measuring ERM Effectiveness

Other ERM Frameworks
Other risk management frameworks

  - AS/NZS 4360 - formally withdrawn on the adoption of ISO 31000
- Open Compliance and Ethics Group “Red Book” 2.0: 2015
- British Standards Institution 31100: 2011
- Federation of European Risk Management Associations: 2002
- Solvency II: 2012 – European Union Insurance Companies
- ISO 31000
- Not designed to provide certification
- Micro or macro level
May 2015 - Announced Revision to ISO 31000

- Draft International Standard (DIS)
  - Closed for comments in May
- Estimated complete late 2017/early 2018
Measuring ERM Effectiveness

Financial Reporting Council
- UK Corporate Governance Code
- Revised October 2014
Measuring ERM Effectiveness

Going concern, risk management and internal control

– Robustly assess principal risks and explain mitigation
– Monitor risk management and internal control systems
  • Annual effectiveness review
– Publicly report risk and viability disclosures
Polling Question #2

What ERM framework does your organization use?

1) COSO
2) ISO 31000
3) OCEG Red Book
4) British Standards Institution 31100: 2011
5) FERMA: 2002
6) Solvency II: 2012
7) A customized version that leverages multiple frameworks
8) We don’t use a framework
9) I don’t know
Measuring ERM Effectiveness

• Role of Internal Audit
• Approaches to ERM Assessment
Measuring ERM Effectiveness

IIA Standard 2120:

The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes
Measuring ERM Effectiveness

IIA Practice Advisory 2010-1 and 2010-2

- Linking the audit plan to risks and exposures
- Must establish risk-based plans
- Must consider organizations risk management framework
Measuring ERM Effectiveness

NIST – Updates Cybersecurity Framework

– Correlation of business results to risk management metrics
– Expanded risk management for Supply Chain
– Access controls
Measuring ERM Effectiveness

Ideal Model

– Organization establishes ERM function
– Internal Audit is required to audit various aspects
Measuring ERM Effectiveness

Practical Model

– Organization relies on Internal Audit to perform or supplement ERM

– Internal Audit needs to establish rules to ensure objectivity
  • Provides insight but makes no decisions
Polling Question #3

What ERM role does Internal Audit play at your organization?

1) IA coordinates with the risk function as necessary
2) IA audits the ERM process
3) IA owns the ERM process
4) We don’t really have a formal ERM process
5) I don’t know
Measuring ERM Effectiveness

Ten Criteria for Effective ERM

Governance Framework Integration Systems
Identification Documentation Assessment Prioritization Emerging Root Cause
Measuring ERM Effectiveness

GOVERNANCE

– Planned approach
– Policies
– Oversight
  • CRO
  • Risk committee
  • Executive participation
– Charter
– Audit Committee review
– Board oversight
– Budget
Measuring ERM Effectiveness

FRAMEWORK

- COSO ERM
- Updated COSO ERM
- ISO 31000
- Customized
  - Routine risk management
  - Articulates ERM approach
- Explains difference between rm and ERM
Measuring ERM Effectiveness

INTEGRATION

– Strategy
– Consideration of interdependencies
– Integrated with risk functions
– Internal Audit
Measuring ERM Effectiveness

SYSTEMS

– GRC Tools
– ERM specific applications
– Internal systems
– Dashboards
Measuring ERM Effectiveness

IDENTIFICATION

- List of risks (Inventory)
- Adequate information
- Does every risk have an owner?
- Reconciled to 10K
- Appetite and tolerance statements
- Inherent vs Residual
Measuring ERM Effectiveness

DOCUMENTATION

– Standardized Templates
  • Common language
  • Risk factors
  • Risk mitigation
DOCUMENTATION

– Standardized Templates
  • Common language
  • Risk factors
  • Risk mitigation

IA can do this!!
## Measuring ERM Effectiveness

### Section 1: Inherent Risk Overview

**Risk Name:** Natural Hazard/Weather

**Risk Sponsor:** Employee Name, Senior VP of Administration

**Risk Coordinator:** Employee Name, VP of EHS
Employee Name, VP of HR

**Risk Definition:** Potential major natural disaster such as a hurricane, earthquake, tornado, flood, wild-fire, drought or winter storm causing a significant business interruption, loss of workforce or damage to physical assets/infrastructure.

**Risk Scope:** The risk scope includes natural type disasters including, but not limited to, hurricanes, earthquakes, tornados, floods and winter storms that can cause a major delay to the Company’s operations, loss of workforce or damage to physical assets/infrastructure. This risk also includes any significant effort necessary to recover from a disaster and return to normal operations. IT business continuity/recovery is excluded from this document.

### Section 2: Contributing Factors

1. Concentration of employees
2. Contingent properties and vendor dependability
3. Significant acquisitions/New facilities

### Section 3: Risk Management Activities

1. Emergency management plans
2. Mass notification tool
3. Third-party vendor program/National weather alerts
4. Humanitarian response process
5. Emergency drill execution
6. Business continuity planning - incident management process and security plans
7. Insurance recovery programs
8. Site-specific geographic response plans
9. Response training/exercises and emergency responder coordination

### Section 4: Opportunities / Issues

No notable opportunities or issues were identified.

### Section 5: Risk Management Plans

N/A
ASSESSMENT/ANALYSIS

• Objective evaluation criteria
• Key risks identified
• Monitored and tracked
• Risk metrics used
• Stratification
  – Board
  – Executives
  – Management
  – Subject Matter Experts
Measuring ERM Effectiveness

PRIORITIZATION

- Risk prioritization process
  - Periodic prioritization of risks
  - Are the right stakeholders involved?
- Scales
- Weighting factors
- Methods of assessment
  - Surveys
  - Interviews
  - Workshops
ERM Prioritization

YEAR OVER YEAR COMPARISON - PRIORITIZED BY CURRENT YEAR

1 – Price Volatility
2 – Strategy
3 – Global Macro
4 – Operations
5 – Human Resources
6 – Information Tech
7 – Operations
8 – Etc.
ERM Prioritization

YEAR OVER YEAR COMPARISON - PRIORITIZED BY CURRENT YEAR

1 – Price Volatility
2 – Strategy
3 – Global Macro
4 – Operations
5 – Human Resources
6 – Information Tech
7 – Operations
8 – Etc.
Measuring ERM Effectiveness

**Financial Impact**
1. < $50 million
2. $50 < $500 million
3. $500 million < $1 billion
4. $1 billion < $5 billion
5. > $5 billion

**Likelihood**
1. Highly Unlikely
2. Somewhat Unlikely
3. Neutral
4. Somewhat Likely
5. Highly Likely

**Preparedness**
1. Very Prepared
2. Prepared
3. Neutral
4. Unprepared
5. Very Unprepared

**Velocity**
1. Greater than one year
2. One Year
3. Weeks to Months
4. Days to Weeks
5. Hours to Days
EMERGING RISK PROCESS

• Method to identify emerging risks
  – Specific brainstorming
  – Integrated into periodic processes

• Resolution of emerging issues

• Events tracked and monitored
Measuring ERM Effectiveness

ROOT CAUSE ANALYSIS

• Gap identification process
  – Compare actual vs needed effectiveness
  – Survey, workshop

• Identify interdependent risks – upstream and downstream
  – Continually ask why

• Aggregate risk impact
Measuring ERM Effectiveness

• Regular discussion with anonymous input lead to impactful changes:
  - Organizational changes to improve facility engineering
  - Initiated corporate focus on data management
Measuring ERM Effectiveness

Key Performance Indicators

VS

Key Risk Indicators
Measuring ERM Effectiveness

• Key Performance Indicators
  – Measurement of performance results
  – Tells you how well something is being done

• Key Risk Indicators
  – Early signal of increasing risk exposures
  – Potential of future adverse impact
Measuring ERM Effectiveness

• Key Performance Indicators
  – Retail – Product Sales

• Key Risk Indicators
  – Number of customer complaints
  – Number of product returns
  – Number of unique visitors
Measuring ERM Effectiveness

- **Key Performance Indicators**
  - Project Management – # of Tasks completed

- **Key Risk Indicators**
  - % of tasks over budget
  - % of tasks on time
  - # of deviations from approved architecture
Measuring ERM Effectiveness

• Key Risk Indicators
  – Identify important metrics
  – Root cause analysis to identify drivers
  – Correlate KRIs to goals and objectives
Polling Question #4

Does your organization use Key Risk Indicators?

1) Yes
2) No
3) I don’t know
Polling Question #5

I would characterize the ERM maturity at my company as:

1) Very mature
2) Moderately mature
3) Not very mature
4) I don’t know
Measuring ERM Effectiveness

• Conclusion
  – ERM is maturing but still varies dramatically
  – Substantial changes in COSO ERM model
  – Internal Audit role varies
    • Required to audit the process
  – Ten measurement criteria may be starting point for audits and assessments
Thank you