Internal Audit and eRisk Identification and Assessment

September 19th, 2016
Agenda

- A Look at ERM – Setting the Stage
- Snapshot of COSO ERM 2016
- eRisk Identification and Assessment
- Sample Reports
- Summary
- Q&A
Enterprise risk management (ERM) is a complex and nebulous subject for which a vast amount of information is available. Given the tenuous landscape in which ERM resides, various perspectives, views, and opinions have been developed. Perfect uniformity does not exist.

- ERM definitions vary
- There is no standard ERM template
- There is no industry-standard road map for ERM implementation
- Various models/frameworks exist but need to be customized to apply to each organization
- Terminology, concepts, ERM program components, and levels of formality vary
- The extent to which technology, applications, and platforms are used differs
Evolution of ERM – An Overview

Key Business Themes

1980's
- Lean Manufacturing
- TQM
- Six Sigma
- MRP II
- Emerging Multi-National View

1990's
- Transferrable Risk Management
- Basel I
- Emerging ERM Methodologies
- Silo-Adhoc Organizational RM

2000's
- ERP
- CRM
- Client Server Migration
- Multi-National Expansion
- ERP Solution Refined
- Internet Business Growth
- Corp Globalization

2008
- Real Estate Bubble Burst
- Financial Institution Failures
- Global Economic Recession
- Economic Recovery
- ERM Relevance
- Global Community

2010's
- ERM as a Discipline
- Holistic Risk Management

State of ERM Practices

2008
- ERM Failures
Why Now – ERM Drivers Today

Constant Change in Global Business Environment

Increasing Public Scrutiny

Increasing Stakeholder Expectations

Increasing Compliance Requirements

Company Viability More Vulnerable

Customers
- Performance
- Transparency
- Security and Trust

Investors
- Performance
- Transparency
- Active Shareowners

Economies
- Capital
- Cost Containment
- Globalization
- Growth

Regulators
- New Legislation and Rules
- Heightened Expectations
- Scrutiny
- Transparency

Media and Public
- Accountability
- Transparency
- Security and Trust

Employees
- Development
- Security and Trust

Company Viability More Vulnerable

©2016 Crowe Horwath LLP
ERM Myths

- “We have always had an ERM Program”
- “It’s too expensive”
- “It’s distracting and disruptive to management”
- “Does not contribute to achieving the goals of the company”
- “We can hire a consultant to build an ERM Program”
- “The goal of ERM is always to reduce risk”
- “Implementation is a one-time event”
Enterprise Risk Management

ERM is a process designed to identify potential events that may affect the entity, manage risk so that it’s within the entity’s risk appetite, and provide the entity reasonable assurance about the achievement of its objectives.
Enterprise Risk Management (cont’d.)

ERM Basic Tenets … Got ERM?

- Leadership has a repeatable, comprehensive understanding of how to establish acceptable levels of risk the organization is willing to undertake.
- Leadership has a repeatable, comprehensive understanding of how to identify, assess, prioritize, and manage risk within its risk appetite.
- Roles and responsibilities are assigned for ERM governance.
- High-value and relevant information for management decision-making is generated to create and protect value.
- Monitoring and reporting processes are enhanced with risk information.
- ERM is linked to the organization’s strategy, culture, and values.
ERM to Sustainable Risk Management

Sustainable Risk Management Framework

Nearly every organization today recognizes that the threats to their objectives emerge from many sources and the impacts frequently span across departmental boundaries. Yet enterprise risk management programs, designed to address these risks, often lose relevance in a very short time and fall to the bottom of management’s agenda.

Learn more
COSO ERM Enhancements

- Strategy, Performance and ERM
- Governance
- Globalization and Business Complexity
- Reporting and Transparency
- Evolution of Technologies and Data Analytics
ERM’s Contribution to Board Oversight

Boost the board's confidence that the organization is attuned to risks, and managing them well

- Policies and processes are consistent with strategy and risk appetite,
- Culture of risk aware decision-making is embedded throughout the organization.
Framework Evolution

- Connects ERM with Stakeholder Expectations
- Positions risk in the context of performance
- Enables organizations to become more anticipatory

Clearing up Misconceptions

- More than internal controls
- Not a checklist
- Suitable for organizations of any size
Update to the Definition

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

In practice, the benefits include

- Increasing the range of opportunities
- Identifying and managing entity-wide risks
- Reducing surprises and losses
- Reducing performance variability
- Improving resource deployment
- Examines role of culture
- Enhances alignment with performance
- Links into decision making
Five Components - Twenty-three Principals

1. Exercises Board Risk Oversight
2. Establishes Governance and Operating Model
3. Defines Desired Organizational Behaviors
4. Demonstrates Commitment to Integrity and Ethics
5. Enforces Accountability
6. Attracts, Develops, and Retains Talented Individuals
7. Considers Risk and Business Context
8. Defines Risk Appetite
9. Evaluates Alternative Strategies
10. Considers Risk while Establishing Business Objectives
11. Defines Acceptable Variation in Performance
12. Identifies Risk in Execution
13. Assesses Severity of Risk
14. Prioritizes Risks
15. Identifies and Selects Risk Responses
16. Assesses Risk in Execution
17. Develops Portfolio View
18. Uses Relevant Information
19. Leverages Information Systems
20. Communicates Risk Information
21. Reports on Risk, Culture, and Performance
22. Monitors Substantial Change
23. Monitors Enterprise Risk Management
Let’s Get To IT!! - eRisk Identification and Assessment

Objective is twofold: To understand individual perspectives on critical risks and concerns that face the company; develop an organic risk inventory based on leadership’s view and perspective.

Brings the key participants into a facilitated consensus session to assess all risks in the inventory. Risks are assessed based on impact, likelihood, and control effectiveness.

Analysis and quantification of the results of the consensus session. Report content designed to meet the needs and expectations of senior leadership and BOD.
Executive Level - *eRisk* Identification and Assessment

- **Risk Views**
  - Set expectations: provide overview of the project, objective, confidentiality, timeline, and deliverable
  - Discussion to glean top-of-mind risks and concerns
  - Most executives are eager to discuss risks, challenges, emerging trends, strategic direction
  - Sample questions to get discussion off the ground
    - Describe the company’s major competitors, and are new ones emerging?
    - What were the key changes to the operating environment and their impact?
    - What are the challenges relating to growth and profitability?
    - What are the key challenges moving forward?
    - What risks worry you across the organization?
  - Set risk evaluation criteria
    - Establish “impact,” “likelihood,” and “control effectiveness” criteria
    - Set expectations for the consensus session
### Executive Level - *eRisk* Identification and Assessment

**Risk Summit**
- Three hour facilitation session with senior leadership team
- Confirm risk measures – impact, likelihood, control effectiveness
- Conduct a walkthrough of a hypothetical risk scenario and assessment process
- Conduct assessment of all risks and rate impact, likelihood, control effectiveness

<table>
<thead>
<tr>
<th>Ref</th>
<th>Risk Scenario</th>
<th>Consequence</th>
<th>Likelihood</th>
<th>Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>The organization is adversely affected by a breakdown of audit/monitoring/measuring systems (e.g., failure to identify non-compliance, shrinkage, failed business initiatives).</td>
<td>4</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

**Summit Outcome**
- Assessment based on leadership consensus
- Individual executive view of critical risks and controls are not siloed
- Opportunity to uncover unknown risks
- Senior leadership team begins to adopt a singular and comprehensive view of the organization’s risk landscape
- Awareness of the true value or risk management
Executive Level - eRisk Identification and Assessment

- Risk Reveal
  - Develop summary of results report
  - Meet with senior leadership team
  - Review process, key findings, discuss recommendations
  - Establish next steps
Sample Reports

Sample Report Table of Contents

1. Introduction
   1.1 Engagement Overview
   1.1.1 Scope and Objective
   1.1.2 Project Scope and Approach
2. Summary of results
   2.1 Risk assessment
   2.1.1 Scenario sheets
   2.1.2 Top 20 risks ranked
   2.1.3 Risks identified with weak management effectiveness
   2.2 Assessment of existing risk management arrangements and practice
3. Action Plan for Improvement
   3.1 Attention to Extreme and High risks
   3.2 Short Term Action Plan
   3.3 Long Term Action Plan
4. Risk Assessment Report
   4.1 Appendix A
   Methodology
   Risk matrix explained
   The risk matrix
   Client participation

Sample Deliverable - Sources of Risk

- Over 50% of risks
- General Management
- Technology and IT
- Asset Management
- Largest Source
- General Management

Sample Deliverable - Summary of Risk

<table>
<thead>
<tr>
<th>Key Risk Outcomes</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of risks identified in the risk</td>
<td>8</td>
</tr>
<tr>
<td>Number of risks identified as being</td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>30</td>
</tr>
<tr>
<td>Medium</td>
<td>50</td>
</tr>
<tr>
<td>Low</td>
<td>2</td>
</tr>
<tr>
<td>Total</td>
<td>5</td>
</tr>
</tbody>
</table>

Number of risks identified as having weak or marginal risk controls: 5

Make areas of extreme and high risks: General Management Technology and IT Asset Management

Sample Deliverable - Risk Matrix Heat Map
Sample Deliverable - Summary of Risk

### Key Risk Outcomes

<table>
<thead>
<tr>
<th>Risk Category</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of risks identified in the risk</td>
<td>61</td>
</tr>
<tr>
<td>Number of risks identified as being:</td>
<td></td>
</tr>
<tr>
<td>Extreme risk</td>
<td>8</td>
</tr>
<tr>
<td>High Risk</td>
<td>32</td>
</tr>
<tr>
<td>Moderate Risk</td>
<td>20</td>
</tr>
<tr>
<td>Low Risk</td>
<td>1</td>
</tr>
</tbody>
</table>

Number of risks identified as having weak or marginal risk controls: 5

Main areas of extreme and high risks:
- General Management
- Technology and IT
- Asset Management
Sample Deliverable - Sources of Risk

- Over 50% of risks
  - General Management
  - Technology and IT
  - Asset Management
- Largest Source
  - General Management
# Sample Deliverable - Top 10 Risks

<table>
<thead>
<tr>
<th>Risk Ref</th>
<th>Risk Description</th>
<th>Risk Severity</th>
<th>Controls</th>
<th>Consequence</th>
<th>Likelihood</th>
<th>Control Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.02</td>
<td>The Company suffers from a changing competitive landscape.</td>
<td>Extreme</td>
<td>4 - Strong</td>
<td>5 - Catastrophic</td>
<td>5 - Almost Certain</td>
<td>The Company currently has several resources focused on maintaining the business environment (e.g., compliance, economy shifts, financial markets, competitor product development efforts).</td>
</tr>
<tr>
<td>4.1</td>
<td>Possibility that multiple key executives may become injured while traveling in the same vehicle together (e.g., charter/commercial flights, car/bus/taxi travel between locations).</td>
<td>Extreme</td>
<td>3 - Moderate</td>
<td>5 - Catastrophic</td>
<td>4 - Likely</td>
<td>The Company has developed and implemented a formal travel policy that restricts executives from traveling together. Corporate security monitors travel itinerary to identify aggregation risks.</td>
</tr>
<tr>
<td>9.01</td>
<td>Possibility that viruses or corrupt files may compromise the availability or integrity of the Company's software or data supply (causing business interruption, cost to rebuild systems and data, and third-party liability).</td>
<td>Extreme</td>
<td>4 - Strong</td>
<td>4 - Major</td>
<td>4 - Likely</td>
<td>Formal security policy has been established and implemented. User training is conducted during new employee orientation as well as on an annual basis. Virus protection software has been implemented and updated on a regular basis. Security administration staff monitors and manages security vulnerabilities.</td>
</tr>
<tr>
<td>2.16</td>
<td>The Company fails to monitor and comply with changing expert controls. (e.g., export licenses, licenses to work in restricted countries, etc.)</td>
<td>Extreme</td>
<td>2 - Marginal</td>
<td>4 - Major</td>
<td>5 - Almost Certain</td>
<td>The Company has several resources monitoring export laws, regulations, and requirements. A formal policy and/or procedure has not been established. Frequent reporting to senior leadership and the board has not been established.</td>
</tr>
<tr>
<td>3.01</td>
<td>The Company fails to manage projects and costs effectively due to lack of project management framework and requirements (e.g., slow in detecting problems overseas)</td>
<td>Extreme</td>
<td>2 - Marginal</td>
<td>4 - Major</td>
<td>5 - Almost Certain</td>
<td>The Company currently has informal project management requirements outlined based on project type, goals and objectives, geographic requirements. Experienced project managers are retained that have proven industry and technical expertise.</td>
</tr>
<tr>
<td>1.16</td>
<td>During periods of peak activity and temperatures the data center struggles to maintain adequate heating/cooling to maintain consistent temperatures throughout the facility.</td>
<td>Extreme</td>
<td>3 - Moderate</td>
<td>4 - Major</td>
<td>5 - Almost Certain</td>
<td>Air conditioning and chillers have been implemented and are currently at maximum capacity. A second data center is currently under construction to relieve environmental restrictions.</td>
</tr>
<tr>
<td>2.07</td>
<td>The Company is accused of violating employment discrimination laws such as EEOC (e.g., EEOC claims, not adhering to employment contracts).</td>
<td>Extreme</td>
<td>3 - Moderate</td>
<td>4 - Major</td>
<td>5 - Almost Certain</td>
<td>A formal HR function has been established and policies and procedures are in place.</td>
</tr>
<tr>
<td>6.17</td>
<td>The Company fails to achieve market diversification goals.</td>
<td>Extreme</td>
<td>2 - Marginal</td>
<td>4 - Likely</td>
<td>4 - Likely</td>
<td>Senior Management and the Board of Directors maintain focus on market trends and impact to diversification goals and objectives.</td>
</tr>
<tr>
<td>2.17</td>
<td>The Company suffers from copyright infringement/privacy laws.</td>
<td>Extreme</td>
<td>2 - Marginal</td>
<td>3 - Moderate</td>
<td>5 - Almost Certain</td>
<td>Management meets with general counsel and corporate compliance to discuss potential copyright and privacy threats.</td>
</tr>
<tr>
<td>1.17</td>
<td>The Company becomes acquired.</td>
<td>Extreme</td>
<td>2 - Marginal</td>
<td>5 - Catastrophic</td>
<td>3 - Possible</td>
<td>Management monitors marketplace conditions regularly.</td>
</tr>
</tbody>
</table>
Sample Deliverable Gap Analysis (Top 20 Risks)

**Control Description**

- The Company currently resources focused on monitoring the business environment (e.g., compliance economic shifts, financial markets, product innovations).
- A formal travel policy has been implemented and travel itineraries are monitored.
- A formal security policy has been implemented and users are trained annually. Virus protection software has been implemented and updated frequently.
- Several resources monitor export laws, regulations, and other compliance requirements.
- The Company hires experienced project managers. Informal project management requirements outlined based on key project criteria & requirements.
- Air conditioning and chillers implemented and at maximum capacity.
- A formal HR function has been established and policies / procedures are in place.
- Senior Management and the Board of Directors maintains focus on market trends and impact to diversification goals and objectives.
- Management meets with general counsel and corporate compliance to discuss potential copyright and privacy threats.
- Management monitors marketplace conditions regularly.
- Service links monitored 24 X 7 and formal service level agreements are in place with key vendors.
- Business leadership partners with HR / outside search firms. Work life balance and compensation are strong. Retention is high.
- Global application and technology architecture is reviewed by IS management and business units annually.
- A succession plan is in place and reviewed on an annual basis. Training is also reviewed on a semi annual basis.
- IS has backup equipment, formal maintenance program, and a formal change control process.
- Key system redundancy, backup equipment, formal maintenance program, and a formal change control process.
- Formal security admin policies and procedures established and audited (internal & external) on a regular basis.
- Management has implement system controls to prevent / detect unauthorized access to confidential information. Policies have been established that includes privacy.
- Formal contracts and service level agreements established for key vendors. A formal vendor maintenance process and metrics have been implemented.
- A documented disaster recovery plan implemented. Backups performed daily and stored offsite by Iron Mountain.

**Risk Statement**

- Company suffers from changing competitive landscape
- Key executives traveling together
- The risk that viruses significantly corrupt Company data
- The Company fails to monitor and comply with changing export controls
- The Company fails to manage projects and costs effectively.
- Risks related to inconsistent temperatures at the data center that impede system performance
- The Company is accused of violating employment discrimination laws such as EEOC
- The Company fails to achieve market diversification goals
- The Company suffers from copyright infringements/privacy laws
- The Company becomes acquired
- Risk of extended failure in service links, e.g., connectivity
- The risk that the Company is unable to attract key talent
- Risk related to the increasing complexity of the IT architecture
- Risk related to training, development, and succession planning
- Loss/damage/breakdown of a significant number of micro computer equipment
- Loss/damage/breakdown of primary computer equipment
- Risk that the user access administration process fails
- The Company has a direct or indirect involvement with identity theft (e.g., employees, customers).
- Risk of inadequate vendor support
- Aggregation risks to primary single data center location
Sample Deliverable - Risk Matrix Heat Map

<table>
<thead>
<tr>
<th>Probability</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Major</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 Almost Certain</td>
<td>Financial - 1</td>
<td>Prod Recall - 1</td>
<td>Info Tech - 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 Likely</td>
<td>Regulatory - 1</td>
<td>Financial - 1</td>
<td></td>
<td>Regulatory - 1</td>
<td>Prop Damage - 1</td>
</tr>
<tr>
<td>3 Possible</td>
<td>Regulatory - 1</td>
<td>Financial - 1</td>
<td>Prod Recall - 2</td>
<td>Save Suppliers - 1</td>
<td>Regulatory - 1</td>
</tr>
<tr>
<td>2 Unlikely</td>
<td>Environmental - 1</td>
<td>Prod Damage - 1</td>
<td>Prod Recall - 1</td>
<td>Liability Claim - 1</td>
<td>Set Suppliers - 1</td>
</tr>
<tr>
<td>1 Rare</td>
<td>Financial - 2</td>
<td>Prod Damage - 5</td>
<td>Prod Damage - 2</td>
<td>Liability Claim - 1</td>
<td>People - 4</td>
</tr>
</tbody>
</table>

Legend:
- Extreme Risk
- High Risk
- Moderate Risk
- Low Risk
### Sample Deliverable - Board Perspective on Risk

#### Board of Directors Participation

The executive leadership team requested additional context setting interviews with the members of the Board of Directors (BOD). These interviews were designed to gain an understanding of what risk exposures that are on the top of mind at the BOD level, thus providing executive leadership with a full and comprehensive inventory of risks. The table reflects risks discussed with the BOD and a cross reference to the Riskscape risk inventory and associated top 20 risks.

<table>
<thead>
<tr>
<th>Risk Event</th>
<th>Description</th>
<th>Top 20 Risks</th>
<th>Risk Ref No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Damage to Products, Good or Equipment While in Storage</td>
<td>Food safety is a critical risk to the company. Increase the focus on domestic and international safety as well as product packaging to ensure food safety.</td>
<td>Yes</td>
<td>1.06, 8.01, 8.08</td>
</tr>
<tr>
<td>Competitor Activity &amp; Loss of Market Share</td>
<td>Product innovations to diversify product offerings, i.e., single-brand vs. multi-brand.</td>
<td>Yes</td>
<td>6.02, 6.03</td>
</tr>
<tr>
<td>General Management Risk – i.e., Poor Franchisee Relationships</td>
<td>Executive management / franchisee relationship can negatively impact financial stability, product quality, brand and reputation</td>
<td>No</td>
<td>3.16</td>
</tr>
<tr>
<td>Shareholder Confidence – Board Composition / Management Arrangements</td>
<td>Executive management and board of directors (BOD) relationship are strained that negatively impacts productivity and effectiveness. Roles and responsibilities should be further defined and enforced to minimize the current disruptions and distraction.</td>
<td>Yes</td>
<td>3.03</td>
</tr>
<tr>
<td>Training Development and Succession Planning</td>
<td>Executive management to demonstrate actionable steps completed to address requirement documented in the current succession plan.</td>
<td>No</td>
<td>3.07</td>
</tr>
</tbody>
</table>
Thank you

Bart W. Kimmel
Principal, Risk Consulting
Crowe Horwath LLP
bart.kimmel@crowehorwath.com
Direct  818-325-8478
Mobile  818-917-0585