IDENTIFYING, UNDERSTANDING AND MANAGING RISKS ACROSS THE ORGANIZATION

Jay Brietz
Shareholder
Email: Jay.Brietz@elliottdavis.com
Phone: 704.808.5247

Melody Reed
Manager
Email: Melody.Reed@elliottdavis.com
Phone: 919.987.2776
Agenda

• Background
• An ERM Framework
• Roles in the Risk Assessment Process
• Key Implementation Factors

This material was used by Elliott Davis Decosimo during an oral presentation; it is not a complete record of the discussion. This presentation is for informational purposes and does not contain or convey specific advice. It should not be used or relied upon in regard to any particular situation or circumstances without first consulting the appropriate advisor. No part of the presentation may be circulated, quoted, or reproduced for distribution without prior written approval from Elliott Davis Decosimo.
We perform risk assessments everyday...

...and we make risk-based decisions
**Importance of the risk assessment**

- Critical part of the risk management process, including determining where internal controls may be needed
- Important planning tool for your organization
- Increased focus of rating agencies
Risk concepts and terms:

- Risk vs. uncertainty
- Definitions of risk
- Myths about risks
What is the difference between risk and uncertainty?
COSO’s definition of risk...

The possibility that an event will occur and adversely affect the achievement of an objective.
Other definitions of risk...

* A probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action.

*BusinessDictionary.com*
The Economic Times describes risks...

Risks are of different types and originate from different situations. We have liquidity risk, sovereign risk, insurance risk, business risk, default risk, etc. Various risks originate due to the uncertainty arising out of various factors that influence an investment or a situation.
Myths about Risk...

- All risks are bad
- Some risks are so bad...we should automatically eliminate them (half-court shot, hole-in-one)
- Playing it safe is always the safest answer
- You cannot develop plans for the unknown
Other risk assessments that often feed into the organization’s ERM Model...

Our focus today
Agenda

• Background
• An ERM Framework
• Roles in the Risk Assessment Process
• Key Implementation Factors
An ERM Framework

Fraud
Credit
Financial
Market
Operational
Regulatory/Compliance

ERM
COSO’s definition of 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 risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.
COSO’s Enterprise Risk Management Integrated Framework

The eight components of the framework are interrelated...
An ERM Framework

- 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.

Source: COSO’s Enterprise Risk Management – Integrated Framework
An ERM Framework

• Is applied when management considers risks 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.

Source: COSO’s Enterprise Risk Management – Integrated Framework
An ERM Framework

• 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.
• 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.

Source: COSO’s Enterprise Risk Management – Integrated Framework
An ERM Framework

- 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.
- 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

Source: COSO’s Enterprise Risk Management – Integrated Framework
## Example Likelihood and Impact Matrix

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Major</th>
<th>Severe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Almost certain</td>
<td>Moderate</td>
<td>High</td>
<td>High</td>
<td>Severe</td>
<td>Severe</td>
</tr>
<tr>
<td>Likely</td>
<td>Moderate</td>
<td>Moderate</td>
<td>High</td>
<td>High</td>
<td>Severe</td>
</tr>
<tr>
<td>Possible</td>
<td>Low</td>
<td>Moderate</td>
<td>Moderate</td>
<td>High</td>
<td>Severe</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Low</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Moderate</td>
<td>High</td>
</tr>
<tr>
<td>Rare</td>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
<td>Moderate</td>
<td>High</td>
</tr>
</tbody>
</table>

*Source: COSO’s Enterprise Risk Management – Integrated Framework*
An ERM Framework

• 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.

Source: COSO’s Enterprise Risk Management – Integrated Framework
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.

Source: COSO’s Enterprise Risk Management – Integrated Framework
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.

Source: COSO’s Enterprise Risk Management – Integrated Framework
Effectiveness of the other ERM components is monitored through:

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

Source: COSO’s Enterprise Risk Management – Integrated Framework
Agenda

• Background
• An ERM Framework
• Roles in the ERM Process
• Key Implementation Factors
Roles in the ERM Process

Three lines of defense

1. Front line unit
2. Risk management, compliance, etc.
3. Internal audit, internal reviews.
Roles in the ERM Process

Three lines of defense - Front line unit

- Boots on the ground managers of risk
- Must have the ability to identify, assess and react to risks on a day-to-day basis
- Own and manage the risks of their area
- Incented to raise the flag
Roles in the ERM Process

Three lines of defense – Risk Management

• Supports and guides the risk owners
• Manages the risk framework
• Monitors risk and compliance with guidance with metrics and other measures
Roles in the ERM Process

Three lines of defense – Internal Audit

• Play an important role in monitoring ERM, but do NOT have primary responsibility for its implementation or maintenance.

• Assist management and the board or audit committee in the process by:
  – Ongoing monitoring
  – Separate evaluations
  – Recommending improvements
Agenda

• Background
• An ERM Framework
• Roles in the ERM Process
• Key Implementation Factors
Key Implementation Factors

- Organizational design of business
- Establishing an ERM organization
- Performing risk assessments
- Determining overall risk appetite
- Identifying risk responses
- Communication of risk results
- Monitoring
- Oversight and periodic review by management
- The last key implementation factor
Key Implementation Factors

Organizational Design of the Business

• Strategies of the business
• Key business objectives
• Related objectives that cascade down the organization from key business objectives
• Assignment of responsibilities to organizational elements and leaders (linkage)
Establishing an ERM Organization

- Determine a risk philosophy
- Survey risk culture
- Consider organizational integrity and ethical values
- Decide roles and responsibilities
Key Implementation Factors

Example Organizational Structure

- Board of Directors
- Audit Committee
  - Risk Management (ERM)
  - Internal Audit
- Enterprise Risk Management Committee
  - Asset/Liability Risk
  - Operational Risk
  - Fraud Risk
  - Reputational Risk
- Compliance
Performing Risk Assessments

• Identify the risk opportunities
• Assess/measure the risks identified
• Prioritize or rank the risks in order to form a risk appetite strategy
Determining Overall Risk Appetite

- Risk appetite is the amount of risk an entity is willing to accept in order to attain appropriate or sought after returns.

- Three components you should know before drafting a risk appetite:
  - Strategic plan and organizational goals
  - Organizational risk profile
  - Risk thresholds – used to monitor exposure compared to risk appetite
Determining Overall Risk Appetite

Key questions in developing your risk appetite:

– What risks will the organization not accept?
  (e.g. environmental or quality compromises)

– What risks will the organization take on (new initiatives)?
  (e.g. new product lines)

– What risks will the organization accept for competing objectives?
  (e.g. gross profit vs. market share?)
Identifying Risk Responses

**Avoidance**
Exiting the activities giving rise to the risk

**Reduction**
Action taken to reduce the risk likelihood or impact or both

**Sharing**
Reducing the likelihood or impact by transferring or sharing a portion of the risk

**Acceptance**
No action is taken to affect risk likelihood or impact

**Management’s response to risk**
Identifying Risk Responses

<table>
<thead>
<tr>
<th>Impact</th>
<th>Probability</th>
<th>Risk Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>High</td>
<td>Mitigate &amp; Control or Avoid</td>
</tr>
<tr>
<td></td>
<td>Low</td>
<td>Control</td>
</tr>
<tr>
<td>Low</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Source: COSO’s Enterprise Risk Management – Integrated Framework*
Key Implementation Factors

Communication of risk results
- Dashboard of risks and related responses (visual status of where key risks stand relative to risk tolerances)
- Flowcharts of processes with key controls noted
- Narratives of business objectives linked to operational risks and responses
- List of key risks to be monitored
- Management understanding of key business risk responsibility and communication of assignments
Key Implementation Factors

Monitoring

• Collect and display information
• Perform analysis
  - Risks are being properly addressed
  - Controls are working to mitigate risks
What is the Secret Key Implementation Factor?

• This is not a sprint, it is a marathon
  - How about a 5K
  - How about a half marathon
  - Get some wins and build momentum
• Develop a plan to get to the finish line
• Communicate your progress
North Carolina State’s ERM Initiative
http://mgt.ncsu.edu/erm/

Institute of Internal Auditors
http://www.theiia.org/

COSO
http://www.coso.org/
AICPA:
• ERM – Guide for Practical Implementation and Assessment

Professional standards:
• PCAOB Standards Nos. 8-15 – The Risk Assessment Standards
• Auditing Standards – SAS Nos. 104-112
About Elliott Davis Decosimo

Elliott Davis Decosimo ranks among the top 30 CPA firms in the U.S. With sixteen offices across seven states, the firm provides clients across a wide range of industries with smart, customized solutions. Elliott Davis Decosimo is an independent firm associated with Moore Stephens International Limited, one of the world's largest CPA firm associations with resources in every major market around the globe.

For more information, please visit elliottdavis.com.