Enterprise Risk Management — Integrated Framework

Tony Bediako

May 20, 2014
Today’s organizations are concerned about:

- Risk Management
- Governance
- Control
- Assurance
Main attributes of Corporate Governance

- Reduction of risk
- Stimulation of performance
- Improved access to capital markets
- Enhancement of marketability of goods and services
- Improved leadership
- Demonstration of transparency and social accountability
Standards

COSO’s Enterprise Risk Management—Integrated Framework. Committee of Sponsoring Organizations of the Treadway Commission (COSO) expanded the Internal Control—Integrated Framework to provide guidance for a comprehensive enterprise-wide approach to managing risk. Published in 2004, the COSO enterprise risk management framework, as an extension of the COSO internal control framework.

ISO 31000. Published in 2009 by the International Organization for Standardization (ISO), This is the only internationally recognized enterprise risk management standard.
Definition

“… 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.”

Is a process; it is ongoing and following through an entity.

- Affected by people at every level of an organization.
- Applied in a strategy setting.
- Applied across the enterprise, at every level and every unit, and includes entity-level portfolio view of risk.
- Designed to identify potential events that, in the event of their occurrence, will affect the entity and manage the risk within its risk appetite.
- Able to provide reasonable assurance to the management and board of directors of an entity.
- General toward the achievement of objectives in one or more separate but overlapping categories.

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.
Why ERM Is Important cont.

ERM supports value creation by enabling management to:

• Deal effectively with potential future events that create uncertainty.

• Respond in a manner that reduces the likelihood of downside outcomes and increases the upside.
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.
Entity objectives can be viewed in the context of four categories:

- Strategic
- Operations
- Reporting
- Compliance
The ERM Framework

ERM considers activities at all levels of the organization:

- Enterprise-level
- Division or subsidiary
- Business unit processes
The ERM Framework

Enterprise risk management requires an entity to take a portfolio view of risk.
The ERM Framework

- Management considers how individual risks interrelate.

- Management develops a portfolio view from two perspectives:
  - Business unit level
  - Entity level
The ERM Framework

The eight components of the framework are interrelated …
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.
Objective Setting

- 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.
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.
Event Identification cont.

- 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.
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.
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.
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.
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.
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.
Monitoring

Effectiveness of the other ERM components is monitored through:

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

A strong system of internal control is essential to effective enterprise risk management.
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.”
ERM Roles & Responsibilities

- Management
- The board of directors
- Risk officers
- Internal auditors
Internal Auditors

- 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:
  - Monitoring
  - Evaluating
  - Examining
  - Reporting
  - Recommending improvements
Assess Risk

Risk assessment is the identification and analysis of risks to the achievement of business objectives. It forms a basis for determining how risks should be managed.
Example: Risk Model

Environmental Risks

- Capital Availability
- Regulatory, Political, and Legal
- Financial Markets and Shareholder Relations

Process Risks

- Operations Risk
- Empowerment Risk
- Information Processing / Technology Risk
- Integrity Risk
- Financial Risk

Information for Decision Making

- Operational Risk
- Financial Risk
- Strategic Risk
## Impact vs. Probability

<table>
<thead>
<tr>
<th>Impact</th>
<th>Probability</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Low</td>
<td>Control</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>Mitigate &amp; Control</td>
</tr>
<tr>
<td>High</td>
<td>High</td>
<td>Share</td>
</tr>
<tr>
<td></td>
<td>Low</td>
<td>Low Risk</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>Medium Risk</td>
</tr>
</tbody>
</table>
IDENTIFY RISK RESPONSES

- Quantification of risk exposure

- Options available:
  - Accept = monitor
  - Avoid = eliminate (get out of situation)
  - Reduce = institute controls
  - Share = partner with someone (e.g. insurance)

- Residual risk (unmitigated risk – e.g. shrinkage)
Contingency Plan

- Plan objective
- Implementation criteria
- Roles and Responsibilities
- Resource Requirements
- Operational procedures
- Discontinuation criteria
Thanks