ERM Definition and Framework

Definition

For the purposes of its work, the Committee developed the following definition:

"ERM is the process by which organizations in all industries assess, control, exploit, finance, and monitor risks from all sources for the purpose of increasing the organization's short and long term value to its stakeholders."

Framework

The ERM Framework is organized by Risk Type and by sequential steps within the Risk Management Process.

Risk Types

- *Hazard* risks, such as:
  - Liability suits (e.g., operations, products, environmental)
  - Fire and other property damage
  - Windstorm and other natural perils (including catastrophes)
  - Theft and other crime
  - Personal injury, disease, disability (including work-related injuries and diseases)
  - Business interruption
- *Financial* risks, such as:
  - Price (e.g. asset value, interest rate, foreign exchange, commodity)
  - Liquidity (e.g. cash flow, call risk, opportunity cost)
  - Credit (e.g. default, downgrade).
  - Inflation/purchasing power
  - Hedging/basis risk
- *Operational* risks, such as:
  - Business operations (e.g. customer satisfaction, human resources, product development, capacity, efficiency, product/service failure, trademark/brand erosion)
  - Empowerment (e.g., leadership, change readiness)
  - Information technology (e.g. relevance, availability)
  - Integrity (e.g., management fraud, reputation)
  - Information/business reporting (e.g., budgeting and planning, accounting information, pension fund, investment evaluation, taxation)
- *Strategic* risks, such as:
  - Competition
  - Customer wants
  - Demographic and social/cultural trends
  - Technological innovation
  - Capital availability
  - Regulatory and political trends

Risk Management Process

- *Establishing Context* – Achieving a full understanding of the present conditions in which the organization operates; this includes understanding the external context (e.g., organization/environment relationship, stakeholder communication policies), the internal context (e.g., business objectives, oversight structure, key performance indicators), and the risk management context (e.g., units covered, degree of coordination throughout organization).

- *Identifying Risks* – Documenting the conditions and events that represent material threats to the organization’s achievement of its objectives or represent areas to exploit for competitive advantage.

- *Analyzing/Quantifying Risks* – Calibrating and, wherever possible, creating probability distributions of outcomes for each material risk.

- *Integrating Risks* – Aggregating all risk distributions, reflecting correlations and portfolio effects, and expressing results in terms of impact on the organization’s key performance indicators (i.e., the “aggregate risk profile”).

- *Assessing/Prioritizing Risks* – Determining the contribution of each risk to the aggregate risk profile, and prioritizing accordingly.

- *Treating/Exploiting Risks* – Developing strategies for controlling or exploiting the various risks.

- *Monitoring and Reviewing* – Continual gauging of the risk environment and the performance of the risk management strategies.

The Framework “Grid”

Some Risk Management Process steps apply to each Risk Type individually, and some, to all Risk Types in the aggregate, according to the following grid, which the Committee used to guide our work and organize our findings.

Process Step	Risk Type			
	Hazard	Financial	Operational	Strategic
Establish Context				
Identify Risks				
Analyze/Quantify Risks				
Integrate Risks				
Assess/Prioritize Risks				
Treat/Exploit Risks				
Monitor & Review				