Enterprise Risk Management Framework

Enterprise risk management is a framework to enable organizations to manage the risks and the uncertainties they face. The framework determines how much uncertainty management is willing to accept as it strives to maximize stakeholder value. A formal definition of enterprise risk management is as follows:

“Enterprise risk management is 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.”

Enterprise risk management is an ongoing process that requires a collaborative effort from employees at every level of an organization. If properly implemented, the framework can leverage an organization to achieve the following:

- Align company’s risk acceptance criteria with business strategy to maximize profit and reduce losses
- Identify and manage multiple and cross-enterprise risks
- Enhance risk response decisions (risk avoidance, reduction, sharing, and acceptance) when risk is identified
- Enhance resource management and seize new business opportunities
- Comply with laws and regulations

Objectives

Enterprise risk management, a leading business consulting company, helps organizations achieve four categories of objectives:

- **Strategic** – high-level goals, aligned with and supporting the company’s mission
- **Operations** – effective and efficient use of company’s resources
- **Reporting** – reliability of reporting
- **Compliance** – compliance with applicable laws and regulations

This overlapping categorization of entity objectives allows a focus on separate aspects of enterprise risk management. This categorization also allows distinctions between what can be expected from each category of objectives and the events that affect the achievement of each objective.

Components of Enterprise Risk Management

Enterprise risk management framework consists of eight steps which are integrated with the management process. These components are:

©2010 Enterprise Risk Management, Inc. All rights reserved.
- **Internal Environment** – The internal environment examines the tone of an organization, and sets the basis for how risk is viewed and addressed by management and staff, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.

- **Objective Setting** – Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity’s mission and are consistent with its risk appetite.

- **Event Identification** – Internal and external events affecting achievement of an entity’s objectives are identified and characterized as either risks or opportunities. Opportunities are channeled back to management’s strategy or objective-setting processes.

- **Risk Assessment** – Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.

- **Risk Response** – Management selects risk responses – avoiding, accepting, reducing, or sharing risk and develops a set of actions to align risks with the entity’s risk tolerances and risk appetite.

- **Control Activities** – Policies and procedures are established and implemented to help ensure risk responses are effectively carried out.

- **Information and Communication** – Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and throughout the organization.

- **Monitoring** – The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

Enterprise risk management is not a serial process, where one component affects only the next. Every component influences the others and contributes to the determination of risk management practice effectiveness. Moreover, these steps are not applied identically in every organization. Application in small and mid-size entities, for example, may be less formal and less structured.

**Roles and Responsibilities**

Everyone in an organization has some degree of responsibility for enterprise risk management. The chief executive officer is ultimately responsible and should assume ownership of it under the oversight of the board of directors. Other managers such as risk officer, financial officer, and internal auditor play key roles in supporting risk management and ensuring compliance with it. Other personnel are responsible for executing enterprise risk management in accordance with established policies and procedures.

**Measuring the Effectiveness**

Enterprise risk management is successful when the eight components are functioning effectively. For the components to be effective there can be no material weaknesses and risk must be accepted by management.
When all the four categories of objectives are met, management can have reasonable assurance that strategic and operations objectives are being achieved, and that the organization is in compliance with reliable and applicable laws, regulations and reporting.

References
COSO Executive Summary

Enterprise Risk Management: At a Glance

ERM brings clients the highest level of expertise to assess and address risks, comply with standards and regulations and mitigate risks, using integrated and reasonably priced security services and solutions.

Our practice provides organizations with the tools they need to address the compliance and risk management issues of today, as well as the broader and ever-increasing security challenges of the future.

Services
IT Security
Regulatory Compliance
IT Audit
Computer Forensics
Risk Management
Attestation

Certifications
Certified Public Accountant (CPA)
Certified Information Systems Security Professional (CISPP)
Certified Information Systems Auditor (CISA)
Certified Information Systems Manager (CISM)
Certified Information Technology Professional (CITP)
GIAC Security Essentials Certification
GIAC Systems and Network Auditor
Qualified Security Assessor (QSA)
Approved Scanning Vendor (ASV)

Some of our Clients
ABN-AMRO Private Banking
Bacardi-Martini, Inc.
Bancafe International
Banco Industrial de Venezuela
Banco ITAU
Bank United
Caja Madrid Bank
Carnival Cruise Lines, LLC
CitiBank
Coconut Grove Bank
Commerce Bank
E-data Financial
Florida International University
Florida Power & Light Company
Heico Aerospace
Helm Bank
Knight Ridder
Nova Southeastern University
Rinker Materials
Rudy, Exelrod & Zieff, LLP
Seabourn Cruise Line
TecniCard, Inc.
The International Bank of Miami
TransAtlantic Bank
U.S. Century Bank

For more information, visit www.emrisk.com
E-mail: info@emrisk.com
Phone: 305-447-6750
800 Douglas Road
North Tower, Suite 835
Coral Gables, FL 33134