

Enterprise Risk Management

By Dan Lightfuss, CPA

[KB Website](#)

[Publications](#)

[Community Involvement](#)

[Newsletter](#)

(Portions of this work were adapted from various works published by The Committee of Sponsoring Organizations of the Treadway Commission (COSO). Copyright 2004-2011. All rights reserved. The adaptation has been with COSO's permission, which reserves all rights to its original work. COSO has neither reviewed nor approved this modification or adaptation and, therefore, makes no representations of any kind concerning its fitness for any purpose – express, implied, statutory or otherwise. COSO has no affiliation with the author of this work and does not sponsor or endorse, in any way, this modification or adaptation.)

The concept of enterprise risk management has been around for a number of years. In 2001, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) initiated a project to develop a framework that would be readily usable by management to evaluate and improve their organizations' enterprise risk management (ERM). As a result of this project COSO published *Enterprise Risk Management – Integrated Framework* in 2004. Other ERM frameworks have been developed, but the framework that COSO has developed is the most well-known and is the preference of most entities using an ERM framework. This document is meant to familiarize you with ERM. To gain a full understanding of the ERM process and its benefits, you should refer to COSO's framework.



The idea of enterprise risk management is based on the assumption that the purpose of a company is to provide value to its owners. It is management's responsibility to determine how much uncertainty is acceptable while creating value for the owners. Uncertainties have a potential to enhance or diminish an entity's value, and hence to generate opportunities or risks to its owners. The question is: how much risk is acceptable to maximize growth and returns.

What is ERM?

COSO defines enterprise risk management as “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.”

In other words, ERM is a strategy, effected by people at all levels of the organization, designed to identify, manage and monitor risks, geared toward meeting company objectives.

The ERM framework aligns an entity's objectives into four categories:

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

An entity has the ability to control its reporting and compliance objectives; therefore, it would be expected that enterprise risk management can provide reasonable assurance that these objectives will be achieved. Strategic and operations objectives are influenced by external events not always within the entity's control; enterprise risk management can assist in making management and the board aware of how the entity is moving toward achievement of these objectives.

ERM and Internal Controls

In 1992, COSO issued *Internal Control – Integrated Framework*, whose policies and rules have been integrated by thousands of enterprises. Most entities are familiar with the concept of internal control and have used it to better control their activities to achieve their objectives.

Enterprise risk management doesn't replace internal control; rather, ERM expands on internal control to address broader, entity-wide issues. Internal control is a component of enterprise risk management.

Components of ERM

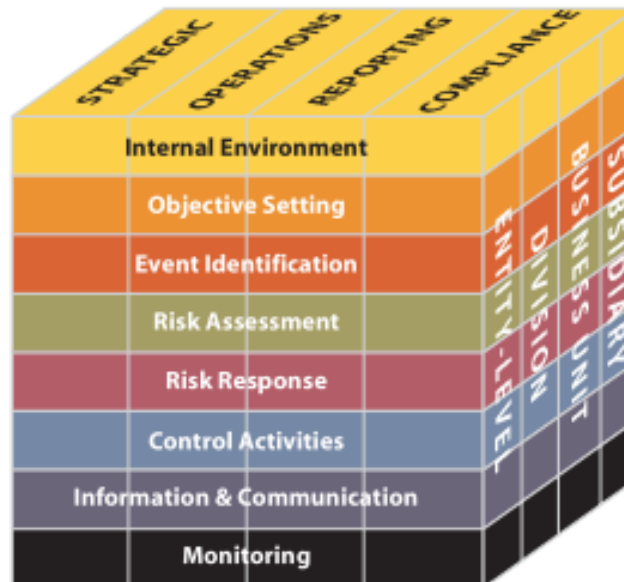
COSO identifies eight interrelated components to ERM: an entity's internal environment, objective setting by management, identification of events, risk assessment, responses to risks, control activities, information and communication, and monitoring.

Following are descriptions of each of these components:

- **Internal Environment** – The tone of the organization; it sets the basis for how risk is viewed and addressed by entity's personnel, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
- **Objective Setting** – Management determines their objectives before they identify potential events affecting their achievement. Enterprise risk management ensures management has a process in place to set objectives and that the chosen objectives support the entity's mission and are consistent with its risk appetite.
- **Event Identification** – An entity identifies the internal and external events affecting the achievement of their objectives, distinguishing between risks and opportunities.
- **Risk Assessment** – Management analyzes risks to determine how they will be managed, while considering their likelihood and impact.
- **Risk Response** – Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the entity's risk tolerances and risk appetite.
- **Control Activities** – An entity establishes and implements policies and procedures to ensure the risk responses are effectively carried out.
- **Information and Communication** – Management identifies, captures, and communicates relevant information in form and timeframe that enables people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity.

- **Monitoring** – Management monitors and modifies the enterprise risk management process as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

There is a direct relationship between objectives, which are what an entity strives to achieve, and enterprise risk management components, which represent what is needed to achieve them. COSO illustrates this relationship in a three-dimensional matrix, in the form of a cube.



COSO, 2004

This illustration portrays the ability to focus on the entirety of an entity’s risk management, or by objectives category, component, entity unit, or any subset thereof.

COSO classifies risk into four categories – strategic, operational, reporting, and compliance. Strategic risks relate to how an entity chooses to achieve its objectives. Operational risks relate to possible losses of organizational assets and threats from ineffective or inefficient business processes. Operational risks can also relate to threats to the organization’s reputation. Reporting risks relate to the reliability and accuracy of information, and the decisions made related to this information. Compliance risks relate to knowledge of laws and regulations, as well as internal codes of conduct and contractual requirements.

Compliance failures grab the most headlines and can lead to legal costs, tarnishing an organization’s reputation, and can ultimately lead to a corporate failure; however, all four sources of risk deserve management’s attention and response.

Implementation of ERM

The first two components of the ERM framework, internal environment and objective setting, relate to an entity’s risk culture and philosophy, and how it will manage risk. Setting objectives will form the risk appetite of the entity. Risk appetite is the amount of risk that management is willing to accept in its effort of adding value to the owners. Part of an entity’s risk philosophy will include management’s knowledge of the entity’s risk capacity in terms of the ability of its people and the available capital.

When an entity's environment and objectives are determined, management can then implement a risk management process.

Event Identification

Many organizations use brainstorming sessions as an approach to event identification, although other approaches such as internal analysis, process flow analysis, and event inventories, may be suitable for certain entities. The participants in a brainstorming session should be from all areas of the organization; an affective brainstorming group would include the executive group as well as employees from different operational areas. The occurrence of an identified event could lead to a risk or perhaps an opportunity to the entity.



Following are examples of the four types of risks:

- **Strategic Risks:** changes in supply and demand, competitive structure, new products, mergers and acquisitions, technology obsolescence, internal performance and reward systems
- **Operational Risks:** environmental pollution, strategic equity, stock option programs, reliability of supply chain, performance of new products, ethical conduct of employees, work stoppage, work-related injury, inventory protection, publicity
- **Reporting Risks:** data and reporting accuracy, relevance reliability, and completeness; security of data; efficiency of decision making and reporting
- **Compliance Risks:** compliance with code of conduct, human rights violations, malpractice, misrepresentation, operational errors

Management should identify which risks they are most likely subject to and the events that would lead to the occurrence of these risks.

Risk Assessment

Risks that have been identified as potentially important should be assessed as to the magnitude of monetary loss or severity of effect they could have on the organization if the event occurs. The probability of a negative event should also be determined. The organization can obtain a better understanding of the potential effects of a risk by determining both the probability of its occurrence and the expected losses. By also assessing the benefits of an appropriate response to the risk, an organization will be able to determine the payoff of a risk management initiative.

Risk Response

In responding to a risk, it is important for management to consider the type and magnitude of risk it should embrace and determine the extent of loss owners will accept if the risk materializes. If controls and processes already exist to address a risk and they are found to be insufficient or excessive, and therefore not cost-effective, management may need to reallocate capital or resources in relation to the identified risk.

There are five ways to respond to a risk:

- **Acceptance** – either the organization accepts the risk because it can withstand the impact, transfers the risk, or reduces the risk to a tolerable level
- **Sharing** – transfer or otherwise share a portion of the risk with a third party
- **Transfer** – pass risk to an independent, financially capable third party, usually through insurance but could include sharing risk through joint venture investments, outsourcing, and contractual agreements
- **Reduction or mitigation** – adding controls within the organization can reduce or mitigate risk
- **Avoidance** – discontinue the activities that create the risk

Choosing a response to risk will be influenced by an organization and its owners' risk appetite. Additionally, an organization should consider the costs of its operating controls in relation to the benefits obtained in managing its risks.

Control

Control policies and procedures are necessary to ensure the chosen risk responses are being carried out properly and in a timely manner. Control activities would include top-level reviews, activity and process management, and segregation of duties, as well as the use of physical controls and performance indicators.

Information and Communication

Communication throughout the organization is essential to ERM. Employees at all levels must understand the definition of risk, the corporate attitude toward risk, the organization's exposure to different risks, the consequences of those risks, and the organization's responses to them. Management must provide communication to employees that address behavioral expectations and the risk-related responsibilities of personnel.

Communication at the board level includes business threats and opportunities, the types of controls being implemented, and the relationship between the achievement of strategic and operational objectives and risk performance measures.

Owners would be interested in the risk policy of the organization, the specific risks to which the organization is exposed, and the way in which those risks are managed.

Monitoring

Since businesses and circumstances change constantly, risk management must evolve with them. Therefore, risk identification, measurement, response, and control need to be monitored. Risks can be monitored in two ways, either through ongoing activities or by means of a stand-alone evaluation.

Why is ERM Important and How Can it Benefit an Organization?

As mentioned previously, every entity exists to realize a value for its owners. Value is either created, preserved, or eroded by the decisions management makes. ERM allows management to deal with potential future events and enables them to respond to these events in a manner that reduces poor outcomes or increases the likelihood of a good outcome.

When management has identified risks to the entity and has formulated reactions to these risks, the entity will be able to better react to events that include these risks.



Keys to Successfully Implementing ERM

The process of ERM can seem overwhelming, so starting ERM on a small scale and building it over time can greatly increase the success of an ERM initiative. Following are some key ideas to keep in mind when implementing an ERM program.

Support is necessary from the top of the organization. The ERM initiative should be an enterprise-wide effort and seen as an important strategy by the board and senior management. The board won't necessarily manage the ERM activities, but the directors should demonstrate support for the initiative and oversee what management has designed and implemented to manage the important risks.

Use incremental steps to build ERM. Success in implementing an ERM initiative can be accomplished over time; undertaking a large ERM process all at once can be overwhelming to everyone involved. A few enterprise-wide key risks can be communicated to the board along with an action plan. This could be followed up by a more detailed risk assessment. As the organization get more comfortable with the ERM process, management and the board may broaden the organization's risk management activities.

Begin by focusing on a small number of critical risks before expanding the scope of ERM. Another approach to manage ERM initially is by focusing on one business area or unit, and then expanding the process across other areas of the organization.

A barrier to beginning the ERM process may be the view that significant additional resources are necessary. The use of existing personnel can be used to form an ERM team or committee. The committee could be formed from a wide variety of personnel within the organization who have a good knowledge of the organization's business model and associated risks.

Build on risk management and control activities that are already in place. Starting with familiar practices, and enhancing and expanding them, could bring immediate benefits to the organization.

The ERM effort should be applied across the entire organization. It will be led by top management but should involve people at every level of the organization.

Initial steps of implementation could be seeking the Board and senior management's leadership and oversight, selecting an ERM leader, establish a risk committee, conduct the initial enterprise-wide risk assessment and action plans, identify current risk management practices, develop a risk reporting format, and develop future action plans and how information will be communicated.

Current State of ERM

During 2010, COSO conducted a survey of organizations to determine how ERM is being implemented and the strengths and weaknesses of COSO's ERM model. COSO received 460 responses; following is a summary of those responses.

It appears that ERM is in its infancy. Only about one-fourth of the respondents described their implementation of ERM as being systematic and in-depth with regular reporting to the board. Over half say their risk tracking is informal and concentrated in specific areas rather than entity-wide.

Almost half of the organizations have assigned risk oversight to a member of management, but in over half of the organizations the board has not assigned risk oversight to one of its subcommittees.

It appears that management reports top risk exposures to the board on a regular basis, but the form of risk oversight is casual and unstructured.

Over half of the respondents indicated that they were fairly familiar or very familiar with COSO's framework, and very few were familiar with other ERM frameworks. COSO's framework was the overwhelming choice as the basis for implementing ERM.

Most believe that the COSO framework is theoretically sound and clearly describes key elements of a robust ERM process. About one-quarter of the respondents indicated that the COSO framework was overly vague.

If your organization is not very familiar with the ERM process or the theory behind it, you are not alone. During the past few years many organizations have been exposed to a variety of strategic and operational risks. By implementing an ERM initiative your organization may be better armed to combat the risks that lie ahead.

Additional Information

COSO's Enterprise Risk Management – Integrated Framework (2004) two volume set is available from the AICPA online bookstore. Volume One includes an executive summary and the entire framework. Volume Two includes application techniques of ERM. The bookstore can be accessed from the AICPA's or COSO's websites. COSO's website also includes links to free summaries and papers related to ERM.

Sources of Information

This summary of enterprise risk management was developed from information included in the following sources:

Enterprise Risk Management – Integrated Framework, Executive Summary, Committee of Sponsoring Organizations of the Treadway Commission, September 2004

Identifying, Measuring, and Managing Organizational Risks for Improved Performance, by Marc J. Epstein and Adriana Rejc Buhovac, published by The Society of Management Accountants of Canada, the American Institute of Certified Public Accountants, and The Chartered Institute of Management Accountants, 2005

Embracing Enterprise Risk Management: Practical Approaches for Getting Started, by Mark L. Frigo and Richard J. Anderson, commissioned by Committee of Sponsoring Organizations of the Treadway Commission, January 2011

COSO's 2010 Report on ERM: Current State of Enterprise Risk Oversight and Market Perceptions of COSO's ERM Framework, Committee of Sponsoring Organizations of the Treadway Commission, December 2010