

# CHAPTER 15: ENTERPRISE RISK MANAGEMENT - SUPPLEMENTAL MATERIAL

***Robert N. Charette***

From the book *The Next Wave of Technologies: Opportunities in Chaos* by Phil Simon

---

## ERM Frameworks—Competition for Hearts and Minds

Today, it is generally accepted that ERM consists of at least the integration of strategic, operational, financial and insurable risk management disciplines. But beyond this, there is much room for debate.

For instance, some argue that corporate governance (i.e., the system by which business corporations are directed and controlled) and corporate compliance (i.e., the process of meeting the expectations of others) are elemental components of the enterprise risk management process. Still, others argue that they are separate, albeit inter-related, processes.<sup>i</sup> What is and is not included in ERM varies from organization to organization.

Over the past several years, the US non-profit Open Compliance & Ethics Group (OCEG) has been trying to define industry and government-wide accepted guidelines and standards for integrating organizational governance, risk management, and compliance processes. The OCEG has defined a set of benchmarks against which organizations can assess their risk management maturity. It also provides means to help organizations improve their practice. In September of 2008, the OCEG released an updated version of its *GRC (Governance, Risk and Compliance) Capability Model* (aka Red Book 2.0).<sup>ii</sup>

Over the past decade plus, there have been several attempts to define frameworks for implementing enterprise-wide risk management. Two have risen to prominence, and both are fighting for the enterprise risk management “hearts and minds” of corporations and governments. One framework has come out of the international standards bodies, while the other has come out of the accounting profession. Let’s start with the latter framework first.

# COSO

The most prominent enterprise risk management framework to date is that developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and which was published in 2004 under the title “The COSO Enterprise Risk Management—*Integrated Framework*.”<sup>iii</sup> To understand the origins of the framework, a little history lesson is required.<sup>iv</sup>

Originally formed in 1985, COSO was created under the joint sponsorship of several US professional accounting associations and organizations. An independent private-sector initiative, COSO focused on the issues surrounding fraudulent corporate financial reporting in public corporations, with an aim of developing recommendations to minimize this type of deception.

In 1987, COSO published the “Report of the National Commission on Fraudulent Financial Reporting (NCFFR)” which was meant to identify the factors that could lead to fraudulent financial reporting, along with defining steps that could be used to reduce its occurrence.<sup>v</sup> The report made several recommendations to deal with falsified financial reporting, two of which were to develop guidance that could assist corporations in improving their internal financial control systems as well as guidance concerning how to judge their effectiveness.

As a result of the NCFFR report recommendations, in 1992 COSO published its “Internal Control—Integrated Framework.”<sup>vi</sup> The goals of the framework were to:

- create a common definition of internal control for organizations;
- to produce a standard against which organizations could evaluate their control systems,
- provide a path for corporations to decide how to improve their internal control mechanisms.

COSO's Internal Control framework defines five key elements necessary for internal control:

- **The control environment**—the tone of the organization that top management takes seriously in terms of its control responsibilities
- **Risk assessment**—the identification and analysis of relevant risks to achievement of corporate objectives;
- **Control activities**—the policies and procedures that ensure that management directives are carried out;
- **Information and communication**—the information about internal and external events, activities, and conditions necessary to informed business decision making and external reporting, and;
- **Monitoring**—the process that assesses the quality of the system's performance over time.

During the late 1990s, the COSO internal control reporting framework became a US benchmark against which to measure a corporation's internal controls. The Sarbanes-Oxley Act of 2002 specifically cites the 1992 COSO framework as an acceptable mechanism for organizations to demonstrate to outside auditors that they have implemented adequate financial controls.

Several COSO member organizations argued that corporations needed to expand their domain of risk management beyond financial control and management to include a wider set of business risks. Hence the development of COSO's ERM integrated framework. The framework provides corporations a broader view of the risks that must be managed (e.g., operational and strategic, not just financial), the necessary organizational structures (e.g., the appointment of a chief risk officer), and the means by which an organization's risks can be managed in a more integrated fashion.

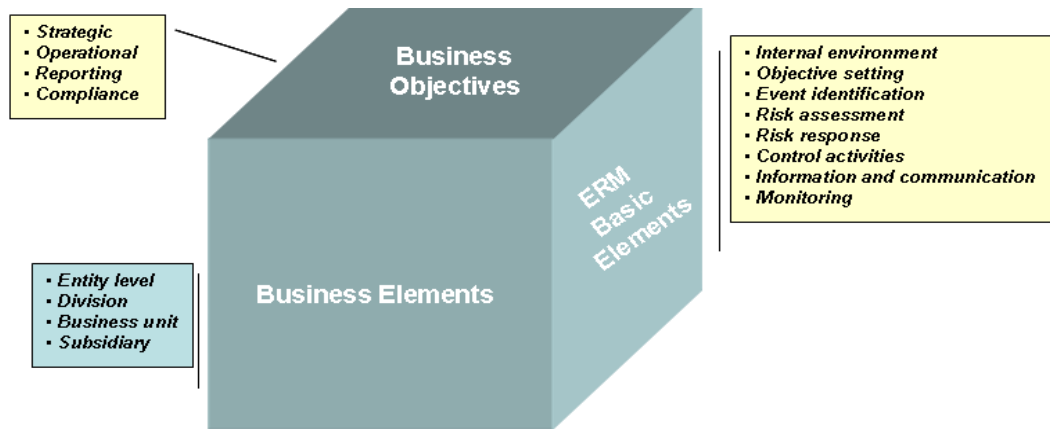
COSO's ERM framework builds on top of the five key elements of the COSO internal control framework rather than starting from scratch. The reasoning is that since many corporations had already invested in the COSO internal control framework, they could build ERM more easily on their existing structure and decision framework.

The COSO ERM framework consists of eight interrelated components derived from COSO conception of how management both runs an organization and integrates risk management into its other management processes. The result is a three-dimensional, four-by-four-by-eight cube model that encompasses the totality of an organization's ERM approach (according to COSO's definition, anyway).

The COSO Model can be represented visually as shown in Figure 1.

As shown, one axis of the cube features COSO's eight basic components of ERM:

- Internal environment (i.e., the organizational risk culture);
- Objective setting (i.e., the organization's objectives);
- Event identification (i.e., the events that might affect objectives);
- Risk assessment (i.e., how risks are assessed);
- Risk response (i.e., how risks are managed);
- Control activities (i.e., the policies and procedures ensuring that risk responses are carried out);
- Information and communication (i.e., how risk information is communicated); and
- Monitoring (i.e., how ERM as a whole is performing and whether it needs improvement).



**Figure 15.1: The COSO ERM Framework**

These eight components of ERM are then mapped against another axis representing an organization's business elements (entity level, division, business unit, and subsidiary) as well as against a third axis representing an organization's business objectives in several categories (strategic, operational, reporting, and compliance).

Just as has happened with its internal control framework, COSO wants organizations use its ERM framework as a benchmark with which to assess and implement corporate ERM. COSO and many in the accounting domain want government regulators to “encourage” that their ERM framework become the *de facto* ERM standard and, even better, that regulators begin to measure organizations' ERM compliance as they measure organizations' internal financial controls.

While government regulators haven't totally embraced the COSO ERM framework as a standard, corporate credit rating agencies like Standard & Poor's, Fitch Ratings, and Moody's Investors Service have given it more credence. For instance, they have begun in the past two years to evaluate aspects of a corporation's ERM practice, specifically in regard to insurers and financial institutions, when developing their ratings. They have hinted at expanding this to most public and private entities they rate (e.g., Standard & Poor's has begun evaluating has public utility organizations against their ERM criteria).

It is only a matter of time, I think, before ERM practice will be used to evaluate most public and private organizations in regard to their credit-worthiness.

## **The Competitor: ISO 31000:2009**

The newer, yet older, ERM framework in competition with COSO's ERM framework is ISO 31000:2009. This is a set of risk management standards being developed by the International Organization for Standardization (ISO), the world's largest developer and publisher of International Standards, such as ISO 9000 on quality management. ISO 31000 is in the later stages of development and is

expected to be published as an internationally accepted standard late in 2009 or early 2010.

The “family” of standards included in ISO 31000 so far are the following:

- ISO 31000: Principles and Guidelines
- IEC 31010: Risk Management - Risk Assessment Techniques
- ISO/IEC 73: Risk Management - Vocabulary

The goal of ISO 31000 is to provide a set of operating principles and generic implementation guidelines on risk management that can be used by any association, group or individual, public or private. A major goal of the standard is to try to reach agreement on a common set of risk management vocabulary. This has been a fundamental issue in the risk management community for years.

ISO 31000 does *not* provide a detailed framework like COSO does. Instead, it provides the information needed by an organization wishing to create an ERM framework based on its specific business or governmental context and the information needs of organizational decision makers.

ISO 3100 is an outgrowth of the risk management standard AS/AZ 4360:1995 Risk Management originally published in 1995 by two standard bodies—Standards Australia and Standards New Zealand. AS/AZ 4360 was the first official standard on how risk management should be addressed throughout an organization. The standard, which has been updated several times since 1995 and will be replaced by ISO 31000, broadly defines the scope of risk management to include financial, operational, political (i.e., reputational), social, client-related, cultural and the legal aspects of an organization’s function. A main idea found in AS/AZ 4360 and which is reflected in ISO 31000 is that risk management should be embedded into other management activities, and not be a standalone, separate activity.

The developers of ISO 31000 would like to see it replace the COSO ERM framework. Absent that, they want the COSO framework to be revised to meet the standard. It is not clear at this time whether or when either will happen.

## **Comparing the Frameworks**

The ISO 31000 and the COSO frameworks are not entirely unrelated. First, they are both based on the idea that there must be a common process of accessing and managing risk. This process must be used in a consistent manner across different elements of an organization, from the senior management level down through the operational level of the organization. Second, both recognize that different contexts and perspectives must be supported—one view of risk (or opportunity) does not fit all situations equally. Third, there is the idea that the framework’s implementation must support a risk-taking ethic. In other words, it

must provide a means to move organizational behavior from being reactive to being pro-active in the face of changing situations. Open communication of risk across the organization is essential.

The COSO ERM framework model has a more top-down, accountancy slant than does ISO 30001. This stems from the fact that COSO's heritage emanates from a US accountancy-based framework. COSO's ERM decision making perspective is still mainly that of the CEO and CFO and the risks that he or she believes are essential. The reason is simple: they are the persons most on the legal hot seat, especially regarding corporate compliance risks as defined by SOX.

ISO 31000 is more generic in nature than the COSO framework. As a result, it can be used to support both a top-down and bottom-up approach to ERM better than the COSO ERM approach can. The flow of risk information from the bottom to the top of the organization is important for one very important reason: any enterprise level risk analysis and management results are only as good as the bottom level information that feeds it.

Former Intel Chairman Andy Grove, for instance, once noted that Intel's corporate strategy was formulated at the "fingertips" of his people: Intel's employees could create or destroy the corporation's strategy (and reputation) through the thousands of small decisions they made daily in their dealings with customers and suppliers. Unless there is a mechanism to help the enterprise level of an organization understand the risks (and opportunities) being taken or pursued at its operating level, organizations will have—at best—a very incomplete picture of enterprise risk.

ISO 31000's strength is also its weakness. Since it is a generic framework, organizations may find that the effort needed to define their own ERM framework is too time-consuming and costly. As a result, they may find the COSO ERM framework a better choice, although it is more prescriptive and constrained. This may be truer in the US, with its strong corporate compliance emphasis, than elsewhere in the world.

---

<sup>i</sup> Charette, Robert. "Enterprise Risk Management Framework: Surveying the Landscape, Moving Towards Governance," Cutter Consortium, 2 (8), 2005.

<sup>ii</sup> OCEG. *GRC Capability Model: "Red Book" 2.0*, 2008.

<sup>iii</sup> COSO. "Enterprise Risk Management -- Integrated Framework<" Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2004.

<sup>iv</sup> This information is based in part from Robert Charette's "Enterprise Risk Management Framework: Surveying the Landscape, Moving Towards Governance," Cutter Consortium, 2 (8), 2005.

<sup>v</sup> COSO. "Report of the National Commission on Fraudulent Financial Reporting," Committee of Sponsoring Organizations of the Treadway Commission (COSO) and the National Commission on Fraudulent Financial Reporting, October 1987.

---

<sup>vi</sup> COS. "Internal Control--Integrated Framework," Committee of Sponsoring Organizations of the Treadway Commission (COSO), 1992.