

Making Sense of COSO's New Framework for Enterprise Risk Management

By David M. Bowling and Lawrence A. Rieger

Enterprise risk management (ERM) has been widely discussed for more than a decade but has taken root in only a few, primarily larger, financial institutions. Interest has built slowly since the mid-1990s, when the Economist Intelligence Unit created an extensive ERM framework. Professional associations—from internal audit groups to business risk managers to chief financial officers—have been discussing the potential of ERM at conferences, in papers and in trade publications for several years. But corporate interest was driven primarily by intellectual curiosity and internal audit experimentation.

ERM can provide a solid foundation upon which companies can enhance corporate governance and deliver greater shareholder value. Very few attempts, however, have come close to fully achieving these objectives. Many financial institutions that launched ERM initiatives began by assessing and then roughly quantifying risks across their enterprises. Most of the attempts did not progress to aggregating risks, creating formal strategies or implementing plans to address the risks, let alone developing frameworks to test for risk or take corrective action.

The time for widespread ERM implementation, however, finally seems to be dawning for at least two reasons:

1. **The logical next step after Sarbanes-Oxley.** Public financial institutions are coming off an intense period of initial implementation of the Sarbanes-Oxley Act of 2002 (SOA), Section 404 in particular. The resulting increased emphasis on corporate governance and the related mounting compliance costs are motivating company leaders to consider

if enterprisewide approaches to risk management will generate greater value from their considerable investments in SOA compliance. They see ERM as the next step in a logical progression for the development of their risk management activities. At its fullest, ERM has the potential to reduce compliance costs, improve operational performance, enhance corporate governance and deliver greater shareholder value.

2. **Release of COSO's new framework.** The Committee of Sponsoring Organizations (COSO) of

the Treadway Commission¹ in late September released its long-awaited Enterprise Risk Management—Integrated Framework (COSO ERM Framework). Three years in the making, the ERM model describes key

components and risk-management principles for organizations regardless of size.

ERM takes a broad portfolio view of risk, an important advance compared to the fragmented, silo-structured activities at many organizations. ERM focuses on the causes and effects that can keep companies from achieving their strategic business objectives. In the first of this two-part series, we will explain what is new in the COSO ERM Framework. In the second installment, we will chart the likely success factors for making an ERM journey.

ERM can provide a solid foundation upon which companies can enhance corporate governance and deliver greater shareholder value.

David M. Bowling is an Executive, Corporate Governance and Enterprise Risk Management, at Crowe Chizek and Company LLC, Lexington, Kentucky. He can be reached at dbowling@crowechizek.com.

Lawrence A. Rieger is an Executive, Corporate Governance and Enterprise Risk Management, at Crowe Chizek and Company, LLC, Chicago, Illinois. He can be reached at lrieger@crowechizek.com.

CCH INCORPORATED

Setting the Stage for a New Framework

The development period of the new COSO ERM Framework “was marked by a series of high-profile business scandals and failures where investors, company personnel, and other stakeholders suffered tremendous losses.”² In response, Congress passed the Public Company Accounting Reform and Investor Protection Act of 2002 (better known as Sarbanes-Oxley, or SOA). Section 404 of SOA mandated that companies use a suitable, recognized control framework for evaluating the effectiveness of internal controls.

COSO’s framework for internal control had existed for a decade without generating great enthusiasm. But SOA requirements in the past two years elevated dialogue about the framework to near-water-cooler proportions in some corporate offices.

The original model, which looks like a colorful Rubik’s Cube® puzzle, was not a simple concept to grasp or implement. This might explain its slow uptake before 2002, when SOA was signed into law. When all of the components, rows and columns seem equally important in a visual model, where does one

start? Without an obvious starting point, how does the process flow?

Since COSO’s new ERM cube adds even more rows and columns, more puzzlement is likely to arise. COSO’s two-sentence definition of ERM is also not easy to grasp, but highlighting some key words helps (see “Understanding Enterprise Risk Management”).

A process, effected by an entity’s board of directors, management, and other personnel, applied in a 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 organizational objectives.³

Perhaps because of a desire to be an all-inclusive definition for use by all companies—for not-for-profits as well as public and private for-profit ventures—this two-sentence definition is necessarily complex and broad.

The inherent complexity of the model and the definition will undoubtedly create work for consultants to help organizations implement the model and realize the benefits. Without guidance, there will likely be a lack of initial focus and understanding about the many components and interrelationships.

Creating a visual model of something as broad as ERM, admittedly, is difficult. A comprehensive management approach that covers the entire organization’s ERM strategy will never be a quick fix. But let us attempt to understand some essential distinctions between the two COSO models (Exhibits 1 and 2).

Understanding Enterprise Risk Management

To get a better understanding of the ERM framework, COSO’s ERM Executive Summary suggests taking a closer look at key words in the definition:

- **A process:** a means to an end
- **Effected by people:** in contrast to exclusive reliance on written policies, surveys or forms
- **Applied in strategy setting:** take a big-picture view
- **Across the enterprise:** take a portfolio (rather than narrow) view of risk
- **Identifying events:** consider in the context of the entity’s appetite for risk
- **Reasonable assurance:** no absolute guarantees
- **Achievement of organizational objectives:** can occur in one or more overlapping categories

Deconstructing the Latest Cube

Two of the most popular films of the year were sequels (*Shrek 2* and *Spider-Man 2*); coincidentally, 2004 was also the year for a sequel in business oversight. The new COSO ERM Framework builds on the internal-control framework released in 1992. Why reinvent the wheel—or, in this case, the cube?

The top of the cube reveals four objectives: strategic, operations, reporting and compliance. Compared to the previous model, the only entirely new objective is *strategic*: a small but vitally important concept to grasp. ERM requires first a focus on an organization’s

overriding business objectives. Broad recognition of the bank's growth goals, for example, can help all employees consider the actions they take daily and how they can help the bank to reach or hinder the bank from reaching its goals.

The eight horizontal rows represent what is needed to achieve each of the four objectives. Reading from top to bottom, the eight components start with Internal Environment and conclude with Monitoring, and there is a clear sequence of activities. In other words, an organization needs first to understand its appetite for risk as part of its internal environment before it sets objectives, identifies events, assesses risks and responds to those risks. (For more detail on these first five components, see "A Closer Look at the First Five Risk Components," right) The final three components in the sequence of eight follow logically: control activities, information and communication, then monitoring on an ongoing basis.

The remaining visible side of the cube outlines different levels of the organization. Most importantly, it starts with the broadest level, the entity (or entire enterprise) and proceeds to a subsidiary level. This model, of course, needs adjustment depending on a bank's size and structure.

Application of the model in small and mid-sized banks may be less formal and less structured.

Exhibit 1: COSO's Internal Control Framework, 1992



A Closer Look at the First Five Risk Components

The first five components (horizontal rows) in the Enterprise Risk Management-Integrated Framework:

- **Internal environment.** Bankers know they are in the business of risk management. This component reflects how company leaders need to agree on a risk management philosophy and their appetite for taking risk. This component also includes organizational structure, board of directors, human resource policies and practices, assignment of responsibility and ethical values.
- **Objective setting.** This layer represents the process of establishing objectives in four areas: strategy, operations, reporting and compliance (each of which correlates to a column revealed on the top surface of the ERM cube).
- **Event identification.** In simple English, what can go wrong? What are the internal and external factors that might affect achievement of a bank's objectives? Both risks and opportunities are identified here, and opportunities are channeled back to management for revising strategy and objectives.
- **Risk assessment.** Risks are analyzed, considering the likelihood and impact as a basis for determining how they should be managed. (This component also appears in COSO's framework for internal control.)
- **Risk response.** What will you do to manage various risks? Avoid? Reduce? Share? Accept? Actions align risks with your bank's risk tolerances.

The remaining three components in descending order—control activities, information and communication and monitoring—are more familiar as they are key components of COSO's framework for internal control. For further information, see www.coso.org.

Nonetheless, small companies still can have effective ERM as long as each of the components in the model is present and functioning properly. Beyond these distinctions between the two models, let's look at some of the most important themes in the new COSO ERM framework.

ERM Requires Top-Down Management

Whereas risk management in the past has often been fragmented and driven from the bottom up, ERM requires a top-down approach. Banks are already getting increasingly accustomed to this approach, because Section 404 of SOA calls for strong ownership of financial reporting controls by top management.

Since top executives are liable for shortcomings in financial reporting, they have the greatest interest in using ERM to manage risks from the top down and to generate greater shareholder value from the ongoing effort. The added SOA expenses and elevation of ultimate responsibility for internal controls over financial reporting to

the C-suite have pushed business executives to look beyond their initial-year efforts for added benefits. They are asking how they can avoid risk from accounting mistakes and also derive greater value from compliance. As Joanne Sammer wrote in the April 2004 issue of *BUSINESS FINANCE*, "By leveraging their compliance efforts and investments to enhance ERM, finance executives can wrest considerable value from a complex, expensive and mandatory process that many companies have resented ever since the act was signed into law."

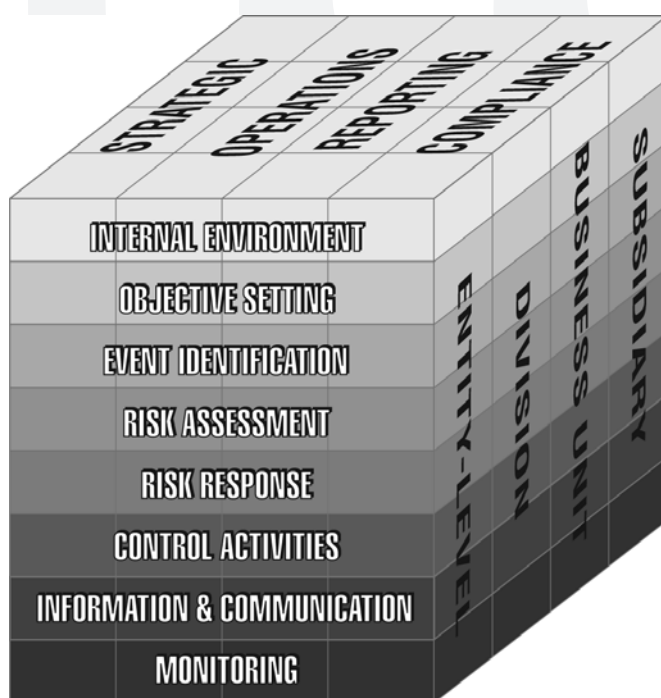
Strong support for ERM from CEOs and CFOs instills a sense of responsibility for risk management throughout the bank. Key process owners are then expected to extend the self-assessments they are now familiar with from Section 404 compliance to a larger number of business risks (not merely controls having to do with financial reporting).

Abandon "Risk-Silo" Mentality, Embrace Holistic Approach

As mentioned above, previous approaches to risk have been confined to various departments. In addition, aggregation of risk and development of an overall risk strategy have usually been lacking. Consider the example of a large bank whose asset-liability management group manages interest-rate risks and whose loan-review group watchdogs credit-risk management. The bank also has separate compliance activities for consumer and commercial areas. Add in security groups (internal and external), as well as loss prevention, insurance and other risk management activities. Along with internal audit, the bank might manage 20 different silos of risk with a different set of risk tolerances for each. One group might accept virtually no risk at all (no risk, no reward), whereas a different group might take on massive risks (destined to cause unpleasant surprises).

ERM, on the other hand, provides the bank's executives with a framework to consider all of these risk areas in total. In performing this aggregation, the bank will gain greater long-term value from its risk activities. Since the bank already conducts these compliance and risk-related activities, the move to ERM is a logical progression, not a

Exhibit 2: COSO's ERM Framework, 2004



duplication of effort. Connecting compliance to a common framework reduces the overall cost and increases shareholder value.

“Enterprise-wide risk management looks within and across business lines and activities of the organization as a whole,” Federal Reserve Governor Susan Schmidt Bies explained at the Risk Management Association and Consumer Bankers Association Retail Risk Conference in Chicago in July 2004. The ERM advantage, she added, is “to consider how one area of the firm may affect the risks of the other business lines and the enterprise as a whole. This approach is in marked contrast with the silo approach to risk management, which considers the risks of activities or business lines in isolation, without considering how those risks interrelate and affect other business lines.”

Build Risk Management into Daily Processes

Just as a superb motorcar is built with quality at each step of the way, true ERM provides greater value when it builds in risk management as an intrinsic component for all business processes. Auto manufacturers realized in the 1980s that it was not cost-efficient to inspect auto quality only at the end of the assembly line and then recall, repair and reinspect. Similarly, many financial services companies understand it is not cost-efficient to treat risk management as an afterthought, considered each quarter or, worse, each year. One of the reasons ERM implementations have failed, or fallen short of their promise, is that they are after-the-fact inspections, as opposed to designed into daily work activities. The emphasis on quarterly results causes too many business leaders to focus on meeting financial targets every three months, rather than on managing processes for long-term advantage. Processes should produce results, not the other way around.

Exhibit 3:
Enterprise Risk Management to Strengthen Corporate Governance



Use ERM to Strengthen Corporate Governance

ERM is a vital engine for strengthening corporate governance (Exhibit 3). Corporate governance is composed of the systems and processes an organization uses to protect the interests of its diverse shareholders. The ideal form addresses the needs of all stakeholders—shareholders, employees, customers, lenders, vendors and the community—since all share a common interest in the successful perpetuation of the business. Well-governed organizations recognize that satisfying stakeholders’ interests is vital for sustaining the organization in the long run and enabling it to prosper over time.

ERM enters the picture because good corporate governance requires sound risk-taking, including the following:

- Monitoring risks with the right processes
- Ensuring management has a comprehensive un-

derstanding of how to manage those risks

- Learning to take intelligent risks, because without risk there is no reward

"Organizations worldwide now recognize the linkage between corporate governance, enterprise risk management and entity performance," COSO Chair John J. Flaherty stated in releasing the new ERM model in late September.

"Successfully managing risk drives better business performance, and facilitates achievement of strategic, operations, reporting and compliance objectives."⁴

COSO's new ERM framework is thorough but acknowledges its limitations. As stated in the Executive Summary, "limitations result from the realities that human judgment in decision making can be faulty."⁵ Simple errors can result in breakdowns in responding to risk. And, of course, fraud will never disappear entirely as long as businesses are run by human beings. Two or more people can collude to circumvent controls, and management retains the ability to override ERM decisions. The COSO ERM definition, as mentioned above, includes two key words: "reasonable assurance."⁶

ERM Framework Likely to Become the Standard

The ERM framework, despite its limitations, is a major step in the right direction, and it is likely to become the gold standard for ERM frameworks. The model can serve as a common reference guide for boards of directors, management and regulators.

By putting in place an ERM framework—based on a shared risk language, technologies and tools—bank executives will find they can manage risk more effectively and reduce the total cost of compliance over time. More important, they can learn where pockets of undiscovered value may lie.

Initiatives to implement ERM and strengthen corporate governance will help set the right tone

from the top of the organization, one that will likely be reflected in the bottom line. A study by the University of Michigan Business School, as well as articles in the WALL STREET JOURNAL, BUSINESS WEEK, COLUMBIA LAW REVIEW and JOURNAL OF ECONOMICS, assert that strong corporate governance programs lead to higher stock valuations and increased shareholder returns.

In the second installment, we will examine how companies can take the COSO ERM Framework, adapt it to fit their organizations, and work in increments to achieve the benefits. So

stay tuned: In part two, we intend to look at various ERM challenges, such as management buy-in and leadership, education issues and resource demands. While the journey to genuine ERM will not be accomplished overnight, incremental steps can be taken with significant benefits realized each step along the way.

Endnotes

¹ COSO is a voluntary, private-sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls and corporate governance. It was formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, known as the Treadway Commission. COSO members include the American Institute of Certified Public Accountants, American Accounting Association, Financial Executives International, Institute of Management Accountants and the Institute of Internal Auditors.

² The Committee of Sponsoring Organizations (COSO) of the Treadway Commission, *Enterprise Risk Management—Integrated Framework, Executive Summary*, Sept. 2004, at v.

³ *Id.*, at 8.

⁴ COSO press release, Sept. 29, 2004, available at www.coso.org/Publications/ERM/erm_pressrelease_20040929.htm.

⁵ The Committee of Sponsoring Organizations (COSO) of the Treadway Commission, *Enterprise Risk Management—Integrated Framework, Executive Summary*, Sept. 2004, at 5.

⁶ *Id.*, at 8.

ERM requires first a focus on an organization's overriding business objectives.

Copyright of Bank Accounting & Finance (Aspen Publishers Inc.) is the property of Aspen Publishers Inc. and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.