The Institute of Internal Auditors
Progress Through Sharing

Bringing ERM Into Focus

A new COSO study provides some much-needed clarity and structure to the fluid topic of enterprise risk management.

By CHRISTY CHAPMAN

ENTERPRISE RISK MANAGEMENT (ERM) — THE PROCESS of identifying and analyzing risk from an integrated, companywide perspective — has been circulating as a business concept for several years. Although most organizations are aware of ERM, few have a clear picture of exactly what the process entails. Even fewer possess a solid plan for implementing ERM within their organizations. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) seeks to change all that. The venerable assembly, composed of the American Institute of Certified Public Accountants, the American Accounting Association, Financial Executives International, The Institute of Internal Auditors Inc., and the Institute of Management Accountants, hopes to alleviate some of the ambiguity around risk with its latest study, *Enterprise Risk Management Framework.*

"Although a lot of people are talking about risk, there is no commonly accepted definition of *risk management* and no comprehensive framework outlining how the process should work, making risk communication among board members and management difficult and frustrating," notes John J. Flaherty, chairman of COSO and retired general auditor for PepsiCo Inc. "The COSO board felt that this situation was similar to that which existed prior to the publication of *Internal Control– Integrated Framework*. Just as that study helped get everybody singing off the same song sheet when it came to internal control issues, our goal is that the *ERM Framework* will offer boards and management a commonly accepted model for discussing and evaluating an organization's risk management efforts."

The initiative began in early 2001, when COSO commissioned a group of University of Virginia professors to determine whether or not a risk management framework was even needed. "We didn't want to waste our time reinventing the wheel," Flaherty says. "After a lot of literature study, the team, which was composed of experts in the risk management area, came back to us and confirmed that clear guidance was indeed needed to help organizations build effective programs for identifying, measuring, prioritizing, and responding to risk."

Once this need was identified, COSO assembled a Project Advisory Council with representatives from its five member organizations and hired PricewaterhouseCoopers to write the framework document. A draft is expected to be available for public comment in July*, with a final version of the framework to be published by year-end.

A NEED IDENTIFIED

To a large degree, COSO's work is in response to the stated needs of board members and senior

management. It's difficult, if not impossible, for most organizations to expend the resources required to develop their own ERM process from scratch. "In this day and age of lean and mean organizations, most are struggling just to accomplish their day-to-day activities," Flaherty says. "They simply don't have the time, talent, energy, or money to undertake such a massive project on their own."

Yet, the mandate for ERM is clear. In surveys of board and audit committee members, corporate risk and risk governance consistently top the list of concerns. In addition, recent business headlines have made everyone aware of how dangerous it is to overlook or ignore potential risks. "As events have transpired in recent years, we've come to realize that we can't consider risk in a silo anymore," says Andrew Jackson, a member of the Project Advisory Council to COSO and assistant general auditor at General Motors Corp. "What we've seen is that you have to look at risks across the enterprise, and you have to look at the interdependencies of those risks. Otherwise, risk management is ineffective."

Many organizations are also seeking to build risk information into their front-end decision-making processes. "This is especially true when it comes to capital allocation," Jackson notes. "For companies seeking to provide value, rationalizing capital from a risk-return point of view is increasingly important. But, to do that, senior leadership and the board need more enterprisewide information, including the measurement of risks across the entity."

ANSWERING THE CALL

ERM, as outlined by the COSO framework, is well-suited to meet these needs. For example, the framework emphasizes the importance of identifying and managing risks across the enterprise from a portfolio perspective. Many organizations perform risk management within each subdivision, but part of the overall vision of ERM is that the risks that occur in the subunits and sublevels of the entity are aggregated and viewed from the top as an overall portfolio of risk.

"That's important for several reasons," says Douglas F. Prawitt, member of the Project Advisory Council to COSO and associate professor at Brigham Young University. "Sometimes there may be risks that magnify each other that you want to know about. Other times there may be risks in different units that offset each other. As a result, the organization may be more or less willing to allow one subunit to take on a level of risk, because another aspect in a different part of the organization would mitigate or magnify it. It's also important to develop an integrated response to risks, so that the right hand isn't unaware of what the left hand is doing."

In addition, the framework takes into consideration the strategic opportunities often associated with risk, while at the same time clearly defining risk as a negative occurrence. In doing so, the framework clarifies an ongoing debate regarding the definition of *risk*.

"An individual's background and responsibilities within an organization really drive that individual's definition of *risk*," Jackson says. "If you talk to a business unit leader who has to generate profits for a company, he or she may view risk as opportunity. However, if you talk to auditors or treasurers, they will likely view risk as downside exposure that needs to be managed. As a result, there has been a tendency to insist that any definition of *risk* include both the idea of opportunity and adversity."

The framework, however, does not claim that risk is both positive and negative. Instead, risk is clearly defined as "the possibility that an event will occur and adversely affect the achievement

of objectives." The framework covers the upside of risk by calling for management to identify all potential events that could affect the organization's ability to successfully implement its strategy and achieve its objectives. Those events with potentially negative consequences represent risks to be addressed through the risk management process. Those events that may have positive outcomes, however, are defined as opportunities, which the framework indicates should loop back into the organization's strategy and objective-setting processes.

"By talking about potential events that may have either positive or negative outcomes, the framework supports both the individuals who see risk as opportunity and those who are dedicated to managing the downside aspects," Prawitt says. "Yet, it maintains its focus on risk management as a process for managing possible negative outcomes and their impacts. That's important, because if you try to put together a framework that incorporates both the positive and the negative in the definition of risk, the discussion of risk management gets unwieldy. Plus, it doesn't really fit with a lot of people's conception of what constitutes risk."

RISK AND CONTROL

A key strength of the framework, at least in the eyes of the COSO Board and Project Advisory Council, is that it *incorporates*, rather than *replaces*, COSO's groundbreaking 1992 study, *Internal Control–Integrated Framework*. "Many organizations have adopted the COSO control framework, various audit standards rely on that framework, and it looks like the internal control reporting required under Sarbanes-Oxley will be heavily based on the COSO internal control model," Prawitt notes. "So it was absolutely critical that the new risk framework not undermine COSO's earlier work."

In addition, not every organization is looking to implement ERM. "Given the size and nature of certain companies, it may not be cost beneficial to migrate to an ERM process," Jackson says. "They can, however, still assure the board and stakeholders that the control environment is effective, because it is possible to have an effective internal control environment without enterprise risk management. The original control model needs to remain intact to serve these organizations."

COSO's ERM framework is therefore broad enough to become widely accepted as a common reference point yet still ties into the COSO internal control model. Instead of simply building ERM into the risk assessment component of the control model — a move that was seen as too narrow and limiting — the project team decided to construct the ERM framework around the existing control model. The new ERM model consists of eight components: internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring (see "ERM Defined").

Although five of the eight components are taken from *Internal Control–Integrated Framework*, the ERM Framework is nonetheless quite different. Author PricewaterhouseCoopers estimates that 60 percent of the new document is leveraged from COSO's earlier work. But because risk is a more all-encompassing topic than internal control, the resulting discussion found in the new framework is much more comprehensive than its predecessor. "We view the *ERM Framework* as a turbo-charged or deluxe version of *Internal Control–Integrated Framework*," Jackson says. "Not only does the *ERM Framework* include the three additional components of objective setting, event identification, and risk response, but the five taken from the control model are broader in their descriptions and in terms of the practical guidance."

USING THE FRAMEWORK

The COSO Board and Project Advisory Council envision the final ERM product as one that will prove extremely useful to boards and senior management. At the organizational level, for example, the framework is designed to:

- Help management align risk appetite and strategy.
- Make the risk appetite of the organization explicit and ensure alignment exists between the risks actually being taken and the level of risk the organization desires.
- Ensure effective risk-response decisions are being made.

The key to the framework's usefulness in these areas will be the more detailed practical application guidance, which is expected to accompany the final version of the framework later this year.

Use of the framework is also expected to enhance internal audit efforts. For instance, the framework calls for managers at the business unit, function, or even process level to develop their own composite assessment of risks for their area. "Internal auditors will want to compare their own risk assessments of an area to those developed by area management to see if adjustments should be made to their audit plan," Jackson says. "In some instances, internal auditors may be able to avoid redundancy by testing management's risk assessment for reliability, then basing their audit work on it instead of performing their own risk assessment of the area."

The development of an entity-wide portfolio of risk, which is the capstone of any ERM program, should also aid the internal auditor. "If management has compiled good information in terms of an entity-wide perspective, it may alter the auditor's view of the ultimate impact or exposure of an issue at a functional or process level," Jackson says. "One challenge that's consistently posed to the chief audit executive by senior management, the audit committee, and the board is to explain what an audit finding means to them — to put the one issue in the context of the entire organization. In the past, it's been very difficult for auditors to provide that entity-wide perspective. We traditionally look at functions and activities independently, making it difficult to see the interrelationship of risks across an entire entity. With ERM, the audit team may be able to put more of their audit findings into the context of risk to the entire organization by linking their audit results to the entity-wide risk assessment."

From a broader perspective, the framework is expected to be a useful tool that boards and other stakeholders can use to measure how well their management teams are handling the risks they face. "The question, 'Do we have a risk management program in place in our organization?' is being heard more and more," Flaherty says. "This framework can be used to respond to that question by assessing the organization against the principles outlined in the document and then using that assessment to communicate to the board and other stakeholders that there is indeed an effective program to identify, measure, prioritize, and respond to risk."

LIMITATIONS

Those involved with the project are careful to point out that neither ERM nor the framework is a panacea. "No matter how well it is designed and operated, ERM cannot ensure an organization's success or guarantee the achievement of objectives," Jackson cautions. "It doesn't provide the proverbial silver bullet against bad judgment and human failure."

That said, much care has been taken to ensure that the framework is as robust and effective as possible. "The Advisory Council comprises people from various backgrounds — academics, internal auditors, certified public accountants, chief financial officers, and private business owners — each of whom brings a certain perspective and strength to the table," Jackson says. "It's been incredible to watch the synergy between the mix of people in the room."

COSO also hopes that exposing the framework for public comment will help ensure its validity and power. "We're not smug enough to think we have all the answers," Flaherty says. "Risk is such an important topic that we want to get as much input as we can, from as many people as we can."

"It's a challenge to obtain consensus from all elements," Jackson adds. "But in the end, that give-and-take makes for a much better product."

* *The draft* ERM Framework *will be available after July 15 at www.coso.org.*

CHRISTY CHAPMAN is the former executive editor of Internal Auditor.

To comment on this article, e-mail the author at cchapman@theiia.org.
