COMPLIANCE WEEK
THE LEADING RESOURCE ON CORPORATE GOVERNANCE, RISK, AND COMPLIANCE

New ERM framework links risk to strategy, performance

Courtesy of COSO, companies have a new risk framework to consider that has the potential to drive a new risk mindset deeper into the organization. **Tammy Whitehouse** has more.

In the continued evolution of corporate approaches to risk management, companies now have a new tool to consider that has the potential to drive a new risk mindset deeper into the organization.

A U.S.-based think tank has issued its recently updated enterprise risk management framework to promote a more strategic, performance-based approach to risk—one meant to rid any stigmas around risk and integrate it into decisions made at every level. The Committee of Sponsoring Organizations of the Treadway Commission, better known as COSO, is a group of thought leaders representing accounting, auditing, and finance professionals across capital markets and private enterprise alike.

COSO is no stranger to the production of game-changing frameworks. It is the author of the Internal Control—Integrated Framework, which has become the most accepted basis for U.S. corporate compliance with internal control reporting provisions under Sarbanes-Oxley. COSO's 2004 "Enterprise Risk Management—Integrated Framework" followed Sarbanes-Oxley but preceded the 2008 financial crisis, which had a profound effect on how entities look at risk.

After updating the internal control framework in 2013, COSO decided its ERM framework was due for a refresh as well. The new framework reflects big changes that have occurred in the global marketplace over that 13 years.

"Since 2004, a number of initiatives have placed, more explicitly, responsibility on the board for risk oversight," says Mark Beasley, an ERM professor at North Carolina State University and a member of COSO's advisory council. Those include requirements from the New York Stock Exchange and the Securities and Exchange Commission for boards and audit committees to do more and report more about what they do in terms of risk oversight.

During the same time period, companies have dealt with greater complexity in the business landscape, says Beasley. Companies can develop long lists of risks arising from rapid changes in technology, geopolitical activity, and cyber activity, for example.

That and more inspired COSO to take a fresh look at its ERM framework to see if it could drive a fresh look at ERM across business globally. The new framework puts a heavy emphasis on integrating consideration of risk into the strategy-setting of the organization and sizing up risk alongside performance.

"We're really pushing this idea that ERM is not some separate thing or set of activities," says Bob Hirth, chairman of COSO. The framework recognizes companies already take on and manage risk to some extent simply by being in business, and that they have some kind of mission, visions, and values as the basis for a governance strategy. "We intentionally don't want to interfere with that."

Instead, the new COSO framework represents a way for companies to benchmark whatever they're currently doing to manage risk and see where they can get more value out of a more integrated approach, says Michael Wilson, a partner at KPMG. "If I was the head of risk for a company or sitting on the board, I'd use this as an opportunity to reflect on the processes we have and whether or not we're clearly getting value out of the program," he says.

Jim DeLoach, managing director at consulting firm Protiviti, says companies should not necessarily begin their assessment under the framework with a blank sheet of paper.

Think of it more as a gap analysis, he says. "Lay out what you're doing agains the identified principles and use that as a basis to identify opportunities to improve your implementation of ERM," he says.

The structure of the framework will be familiar to anyone who knows COSO's internal control framework. The ERM framework asserts there are five key components to an effective approach to ERM. They encompass governance and culture, strategy and objective-setting, performance, review and revision, and information and reporting.

Each of those five components are then supported by a total of 20 principles that describe practices that can be applied throughout the organization to give management and the board a reasonable expectation that the organization has its arms around its risks. That format is similar to the components and principles COSO established in its internal control framework.

The structure is intended to help companies assure they will get more out of their risk activities, says Dennis Chesley, a partner at PwC who helped lead the project to revise the framework. In its research interacting with more than 400 organizations globally, the team learned companies wanted to know how to get more value out of the work they were putting into ERM, he says.

"They wanted an increasing range of opportunities, identifying risks entity-wide and increasing the outcomes," says Chesley. That led the team to assure the framework would contemplate a wide variety of organizations and circumstances. "We put together a pretty comprehensive framework to achieve a wider range of benefits than have been achieved before."

Risk professionals who study the framework should come away from it with an understanding that they need to assure they approach risk not just with a downside focus, but with an upside focus as well. Chesley says he's quite familiar with the common criticism of risk professionals—that they are sometimes regarded as the bucket of cold water on strategic ideas or initiatives.

"If strategy is going to invite risk to the table, they've got to be able to add to the discussion and not just look at everything that could possibly go wrong," says Chesley. "They've going to convert their language to opportunity to successfully manage risks to positive outcomes. It's up to risk professionals to do that."

Risk functions today are typically more focused on risk mitigation than risk management, says Beasley. The new framework would pull companies further along the maturity continuum, he says. "This is saying we want to manage risk in an intelligent way, which may mean we might want to take on more risk," he says. "ERM is not about telling people you can't do something. It's about how to be smarter about the risk you take with every strategy."

There's no regulatory body or governing organization requiring companies to adopt the new framework, but DeLoach says companies would be wise to see it as an opportunity to bring ERM approaches into sync with modern business realities. "A lot of risk management methodologies we see in corporate America today are rooted in the 20th century," he says. "It's an analog approach in a digital world."

Yet companies that decide to dig into the framework can expect some of the traditional obstacles to such initiatives, especially when they are undertaken voluntarily—support

COSO RESOURCES

A brief summary of the COSO ERM Framework and resources is below.

In keeping with its overall mission, the COSO Board commissioned and published in 2004 the Enterprise Risk Management—Integrated Framework. Over the past decade, that publication has gained broad acceptance by organizations in their efforts to manage risk. However, also through that period, the complexity of risk has changed, new risks have emerged, and both boards and executives have enhanced their awareness and oversight of enterprise risk management while asking for improved risk reporting. This update to the 2004 publication addresses the evolution of enterprise risk management and the need for organizations to improve their approach to managing risk to meet the demands of an evolving business environment. The updated document, titled Enterprise Risk Management—Integrating with Strategy and Performance, highlights the importance of considering risk in both the strategy-setting process and in driving performance.

2017 COSO ERM framework executive summary

2017 COSO ERM framework resources

ERM Framework FAQs

Source: COSO

"Since 2004, a number of initiatives have placed, more explicitly, responsibility on the board for risk oversight."

Mark Beasley, ERM Professor, North Carolina State University

from the top, resistance to change, resources, skepticism, etc. "Sometimes there a fear that if I do this new framework, I've got to hire more people, buy more software, and so on," says Beasley. "That's not the intended message at all. The resistance will be thinking this will be more complex than it will be."

The ultimate goal in integrating risk into the strategy and performance of the organization is to change the cultural approach to risk, says Wilson. "Just putting in protocols, procedures, and trappings of risk management templates doesn't get to the value needed from a risk standpoint," says Wilson. "If you want to get to value, you have to get to the underlying culture. It's a cultural change, and that can't be underestimated." ■