



RISK MANAGEMENT/BUSINESS AND INDUSTRY

Businesses can use ERM to manage a wide variety of risks.

Enterprising Views of Risk Management

BY RUSS BANHAM

EXECUTIVE SUMMARY

- **ENTERPRISE RISK MANAGEMENT (ERM) IS A STRATEGY** organizations can use to manage the variety of strategic, market, credit, operational and financial risks they confront. ERM calls for high-level oversight of risks on a portfolio basis, rather than discrete management by different risk overseers.
- **ERM HAS GIVEN RISE TO A QUESTION:** Who should head the risk management process—internal audit or a chief risk officer? Some believe internal audit should take a back seat to preserve the checks and balances the audit function provides. Others say risk leadership should depend on what a company is comfortable with.
- **USING ERM ENABLES AN ENTITY TO ASSESS** risk across the enterprise instead of looking at it on a per-project basis. It also gives the company a means to assess the controls in place to handle each risk and identify any gaps. This consistent approach also offers businesses an opportunity to determine authority and responsibility and allocate resources appropriately.
- **TO EXTRACT RISK DATA, MANY ORGANIZATIONS** use business intelligence

software. Many packages feature “traffic-light” systems that show a red light if risk exceeds acceptable levels. The chief risk officer then can “drill down” to see the reasons and make more informed decisions.

■ **OVERALL RESPONSIBILITY FOR ENTERPRISE RISK** is changing because of new standards from the Institute of Internal Auditors. They require the internal audit function in a company to monitor and evaluate the effectiveness of the organization’s risk management and control systems.

RUSS BANHAM is a business journalist and frequent contributor to the *Journal of Accountancy*. His most recent book is *The Ford Century* (Artisan, 2002), a 100-year history of the Ford Motor Co. His e-mail address is bzwriter@aol.com.

Industry insiders tout enterprise risk management (ERM) as the most effective strategy an organization can use to manage a plethora of risks, running the gamut from strategic, market, credit, operational and financial exposure to the daunting array of man-made and natural disasters. New ERM committees led by chief risk officers identify, quantify and monitor these risks via a holistic, portfolio-based management system. However, new internal audit standards from the Institute of Internal Auditors (IIA) (www.theiia.org) may change the paradigm; they require internal auditors to assume responsibility for monitoring enterprise risk, creating tension in some organizations over who is in charge. CPAs with internal audit or risk management responsibilities can use this article to determine whether ERM is a strategy that will benefit their organizations and who should be responsible for overseeing risk management.

ERM BASICS

The difference between ERM and more traditional ways of managing risk (see the exhibit on page 68 for more details) is that ERM calls for high-level oversight of a company’s entire risk portfolio rather than for many different overseers managing specific risks—the so-called silo or stovepipe approach. ERM, in effect, centralizes management under a chief risk officer or ERM committee who manages the individual overseers to help identify overall how much risk the entity can tolerate, assess mitigation tactics and otherwise take advantage of risk opportunities.

The idea of viewing risk as an opportunity may surprise some CPAs. ERM adherents explain that absorbing, hedging or transferring risk requires capital—dollars a business might otherwise direct

to other, more productive and profitable endeavors. “Since entities must hold capital to absorb the risk of loss, there is less to invest in other profit-producing activities,” explains Peter Nakada, executive vice-president of ERisk, a New York-based ERM consulting firm and software provider. “ERM helps determine the right amount of capital companies should direct toward risk.”

How does ERM help a company arrive at this figure? It’s done by gathering or otherwise polling risk overseers to determine the threats to the organization, the financial impact and the effectiveness of risk mitigation options. “The goal of the process is to determine the appropriate amount of capital you need. You can’t get that number unless you identify and measure all the risks threatening the organization,” Nakada says. “Once you know you can determine where to direct capital.”

Embracing ERM

In a survey of 200 senior finance and risk management executives,

- 41% said their companies were implementing some form of enterprise risk management (ERM).
- 90% whose companies were pursuing ERM were very confident in their ability to manage risk, compared with just 45% of those not using ERM.
- 84% believed ERM could help improve their companies’ price/earnings ratios and cost of capital.

Source: *Enterprise Risk Management: Implementing New Solutions*, The Economist Intelligence Unit and MMC Enterprise Risk, www.mmcer.com.

Why should CPAs care about ERM? “Because it will directly affect how and why they do their job,” says William Spinard, senior vice-president in the Washington, D.C., office of Marsh Inc., a large multinational insurance broker that works with clients to develop ERM strategies and systems. “With ERM an entity establishes risk definitions and tolerance levels, as well as policies. It defines procedures to measure risk and creates monitoring activities. ERM will basically be the standard bearer for risk management in a company, a role traditionally handled by internal audit.” The question now emerging, Spinard says, is “Who should head ERM: the internal audit department—given the new Institute of Internal Auditors standards—or chief risk officers and other traditional risk overseers from finance?”

While Spinard advocates that internal audit take a back seat to more traditional risk managers—“to effectively preserve the checks-and-balances element of the audit function”—some organizations are designating internal audit as the über risk manager. “Having set the standards for internal controls, the auditors are now setting the benchmarks for ERM,” Spinard adds. But should internal audit manage the entity’s ERM strategy? “Rather than be in charge of the process,” Spinard says, “it should be critiquing it” and making suggestions for improvements.

BEGIN AT START

ERM's departure from silo-based risk management doesn't preclude decentralized risk management. Rather it establishes a hierarchy with discrete risk managers typically reporting to a central figure using so-called dashboard technology—business intelligence software that extracts risk-based information, collates it and reports it to the chief risk officer or ERM committee, which has overall responsibility.

Take the case of Capital One Financial Corp., a McLean, Virginia-based financial services organization with \$71 billion in managed assets. “We have four legs to the stool—a chief risk officer who heads an ERM team that sets methodologies and reporting standards and educates the company at large; functional groups throughout the enterprise that manage risks in their own sectors and report the results to the ERM team; internal audit which is responsible for ensuring the risk management process works throughout the company as intended; and risk stewards or advisers who are experts in each individual risk category and provide guidance,” says Michael Glotz, Capital One audit director for North American business lines and head of the company's new ERM audit team.

Such a bird's-eye view of risk is not available with more traditional risk management where insurance risk managers address hazard and liability risks, internal audit manages financial reporting risks, business units handle project risks, treasury deals with foreign-exchange risks and so on. “Previously, we had been less proactive in instituting processes and reporting around risk management, with each functional area responsible for its own,” Glotz explains. “That made a single version of the truth, in terms of full enterprise risk, hard to come by.”

As in other organizations, Capital One's ERM strategy rests on a thesis that managing risks holistically offers value, in terms of identifying the breadth of organizational risks, quantifying them and distinguishing both risk correlations (two risks that may moderate each other's impact) and risk relationships (one risk that begets another, such as a product recall that creates a public-relations nightmare). In the past, certain risks hedged others, but the company overlooked or undervalued the correlations because of discrete risk management practices. Someone needed to be in a position to discern enterprise risks from 70,000 feet, observing their interplay, the effectiveness of mitigation options and the aggregate costs of the different risk transfer strategies. “Someone has to bring risk management into the strategic planning process to ensure business strategies are aligned with the organization's overall appetite for risk,” says Glotz.

That someone at Battelle Memorial Institute is Jane Cozzarelli, CPA, vice-president of internal audit at the \$1 billion Columbus, Ohio-based research and development entity. Cozzarelli is spearheading the development of an enterprise-level risk management process at the not-for-profit organization, an effort motivated by Battelle's rapid growth. “We're doing a lot of contract research for commercial clients and want to take ownership of the intellectual property we develop,” says Cozzarelli. “These new businesses and markets create new risks—unfamiliar territory for us.” She says Battelle is entering a whole new world involving joint ventures,

acquisitions and the like. “While we were confident about the traditional risks we confronted in a research context, we were leery of taking on new commercial-type risks without a framework.” Cozzarelli says the institute decided to “assess risk across the enterprise to obtain a portfolio approach”—hence, she says, the ERM strategy.

Previously, Battelle had looked at risk on a per-project basis, which limited its ability to appreciate the opportunities proper risk management creates. “Risk isn’t necessarily bad,” Cozzarelli, says. “By measuring your risks, you can direct capital to them more efficiently. You also are better able to understand the upside and downside of undertaking a risk.” For example, if Battelle undertook a \$50,000 project on behalf of a pesticide company, and the Environmental Protection Agency approached it to do a similar project for \$2 million, the resulting conflict of interest would cause it to lose the larger project because it didn’t understand the strategic risk of doing the pesticide company project. “We had no systematic process for looking at risks across the breadth of the organization,” Cozzarelli says.

Battelle sent out requests for proposals to consulting firms to help develop an ERM infrastructure, selecting Marsh. The broker undertook an initial assessment that involved interviews with senior managers about their risk concerns—“the stuff that keeps them awake at night from an organizational and individual market sector standpoint,” Cozzarelli says. Each manager had particular market responsibility, from medical products to environmental issues to transportation. Following this initial assessment Marsh sent out an electronic questionnaire to 250 Battelle product-line managers and research support staff eliciting their perspectives on risk. The organization conducted several workshops to examine the results of the initial assessment and survey responses. Ultimately, Battelle identified its top 10 risks. Using anonymous voting techniques, it rated them for potential likelihood and impact and mapped the risks on a matrix.

Traditional RM vs. ERM: Essential Differences	
Traditional risk management	ERM
Risk as individual hazards	Risk in the context of business strategy
Risk identification and assessment	Risk portfolio development
Focus on discrete risks	Focus on critical risks
Risk mitigation	Risk optimization
Risk limits	Risk strategy
Risks with no owners	Defined risk responsibilities
Haphazard risk quantification	Monitoring and measuring of risks
“Risk is not my responsibility”	“Risk is everyone’s responsibility”

Source: KPMG LLP.

The next step was to assess the controls in place to address each risk and identify any gaps. “That

gave us a starting point to know where we needed to focus our resources,” Cozzarelli says. Marsh then worked with Battelle to draft a new risk management structure governed by an executive risk management group. “We’re trying to determine levels of authority and responsibility,” Cozzarelli says. “Once we decide that, we will implement dashboard technology to monitor and report on risk across the enterprise.”

Businesses “want a process to assess all risks in a systematic, consistent way,” says Spinard, who led the Battelle project at Marsh through late 2003 when Battelle decided to continue its ERM implementation in-house. Others agree about the need for a systematic approach. “What you want to do with ERM is get all the overseers together to pinpoint and measure the critical risks confronting the company and then develop a systematic way to manage them,” says Ted Senko, CPA, national partner in charge of risk advisory services in the Denver office of KPMG LLP. “You end up taking something that is typically a cost center—risk—and turning it into something that can give you a return. But you can’t do that unless you meet with officers and key business unit managers to talk about the risks they face in trying to meet their respective goals.”

To elicit candid responses, KPMG tries to assemble all of the individual overseers in a conference room “to develop a frame of reference around risk.” Senko says, “if that isn’t feasible, we conduct a structured interview process with the overseers. We then develop a map that pinpoints ‘high impact probability’—the critical risks the company must monitor and control.”

Senko recalls working with a *Fortune* 50 consumer products company to execute this process. “The company runs fairly autonomous business units. As we assembled the risk overseers, we learned that although the units confront many similar risks, such as commodity hedging, they had very different risk profiles as to when and how they would hedge.” Senko says the company learned a very tangible lesson. “Because it didn’t have a consistent hedging strategy, some business units had higher or lower risk tolerances than the overall corporate threshold. By having all businesses understand the company risk tolerance, they were able to optimize their individual strategies to be consistent.” In effect, Senko says, “they changed their hedging strategies to be consistent with the common risk framework, which saved them money. Synchronizing their commodity program globally enabled them to enhance their return on capital.”

In his consulting work with dozens of companies undertaking an ERM project, Spinard says strategic risks typically dominate the discussion. “Companies cite things such as market erosion and competitors’ actions as the real threats,” he says. “A risk that impedes growth targets or has significant stock implications is the one usually plotted on the section of the matrix depicting the greatest impact or severity, things such as new product development or customer issues.” Spinard says his firm just consulted with a food service company that cited customer obesity concerns as presenting enormous risk.

Once a company has mapped major risks on a matrix, it must align business processes to ensure data relating to each risk are routinely stored in a database the chief risk officer or executive risk

committee can monitor for exceptions—risks extending beyond tolerance or threshold levels. “A large part of ERM rests on the efficient and correct collection and organization of data,” says Dennis Ceru, director of retail brokerage and investing at Needham, Massachusetts-based Tower Group, a research and advisory firm. “That’s where technology comes into play to determine potential risk trends, such as the interplay of economic factors with market trends. Provided on a timely basis, such intelligence can guide improved decision making.”

To extract risk data and observe them on a dashboard, organizations can use business intelligence software packages available from companies such as Hyperion Solutions (www.hyperion.com), Cognos Inc. (www.cognos.com), Algorithmics Inc. (www.algorithmics.com), SAP (www.sap.com) and Crystal Decisions (www.businessobjects.com), among others. The cost of such packages typically is in the six-figure range. At RBC Financial Group, a Toronto-based financial institution with an ERM strategy in place for two years, chief risk officer Suzanne Labarge uses business intelligence technology from Portiva Corp. (www.portiva.com) that features a traffic-light system, with red, yellow and green lights. “We mapped all our risks on a matrix and have clear data reporting responsibilities in place to ensure a constant flow of risk-based intelligence,” Labarge says. “If a particular risk exceeds acceptable levels, a red light pops up on the dashboard. I can then ‘drill down’ into the reasons, enabling me to make more informed decisions.”

WHO'S ON FIRST?

While the process of building an ERM strategy is similar, overall responsibility for enterprise risk is changing because of the IIA standards. The added risk responsibilities for internal audit are fomenting a controversy of considerable interest to CPAs over who should manage enterprise risks—traditional risk overseers from finance like Labarge or internal auditors such as Cozzarelli.

The basic requirement for the internal audit function, as contained in the new IIA standards, is to monitor and evaluate the effectiveness of an organization’s risk management and control systems. Standard 2110 of the *International Standards for the Professional Practice of Internal Auditing*, for example, says the internal audit activity should help the organization manage risk by identifying and evaluating significant exposures to risk and contributing to the improvement of risk management and control systems. Standard 2120 says the internal audit activity should evaluate the effectiveness and efficiency of the organization’s control processes.

Spinard says “several auditors are now saying they want to run ERM, and their organizations are letting them. They say ERM is a natural step forward for internal audit because they typically set and validate internal control standards. Based on their expertise they believe they should manage all controls, including risk.” And, says Spinard, that’s not necessarily a bad thing. “But others believe ERM should be a management function—something it needs to do because it will help it run the business better.”

Cozzarelli has a different opinion and notes that Battelle is considering her to become its chief

risk officer. “It would make sense for internal audit to get the information we need to do risk-based audit plans, monitor risk to give management insight and report to the board,” she says. “That seems to be where we’re headed. I don’t believe ERM needs to be a separate process with a separate group running it.” Risk management, she says, should be “integrated into everyone’s normal strategic planning, literally imbedded in everybody’s job description. Then internal audit could reinforce both the governance and internal control issues to make sure processes were in place to adequately safeguard assets.”

Cozzarelli concedes that Battelle’s senior management isn’t certain audit should lead risk oversight. The IIA standards, she says, are “kind of fuzzy. Risk leadership should depend on what a company is comfortable with.” Obviously, she points out, you can’t audit something you put together. “We need to remain objective and independent. But once processes are in place, I don’t think there is any problem with audit overseeing them.”

The issue boils down to whether a separation of church and state makes financial sense, explains James Lam, president of James Lam & Associates, a Wellesley, Massachusetts-based risk consultant. Although auditing and risk management are complementary, says Lam, they serve different purposes. “Risk management is very broad and comprehensive whereas internal audit is episodic and deep,” he maintains. “When you think about risk management, it is global and real-time, anticipating future exposures and developing contingency plans and strategies to deal with them.” On the other hand, Lam says, audit works on an annual cycle that is not necessarily real-time or anticipatory. Auditors go deep in terms of looking at policies and procedures and compliance. The truth, he emphasizes, is that audit “should check risk management to ensure it is being performed appropriately, while risk management should do the actual identification, monitoring and mitigation.”

Glitz from Capital One notes that in large, sophisticated financial services companies, risk management traditionally is its own organization. “It’s really in smaller entities where we’re seeing the chief auditor taking on ERM responsibility,” he says. “In financial services, the management of risk is a separate function.” Still, he says, he is not sure whether the IIA standards insist that internal audit necessarily should manage risk. “We’re certainly part of the ERM process, and our head of audit sits on the ERM executive committee, but we don’t run the show.”

ERM has changed Capital One, Glitz asserts. “The risk and control processes in our business units and functional groups are more formalized, which has begun to make internal audit more efficient,” he says. “Now that we’ve identified the key risks and have processes in place to control them, internal audit’s risk assessment obviously is more effective. ERM gives us more proactive risk and control management to evaluate the business and certify controls. It formalizes what—in areas other than credit and financial risk—heretofore was pretty much ad hoc risk management.”



PRACTICAL TIPS TO REMEMBER

- ERM can help CPAs determine the right amount of capital companies should direct toward risk by gathering or otherwise polling risk overseers to identify the threats to the organization, their financial impact and the effectiveness of risk mitigation options.
- Companies can use ERM to assess risk across the enterprise. Considering risk solely on a per-project basis can limit an entity's ability to appreciate the impact the risk associated with that project can have on the entire organization.
- By mapping major risks on a matrix, companies can align their business processes to ensure they are routinely collecting and storing related information in a database the chief risk officer or executive risk committee can monitor. This will make it easier to identify exceptions—risks extending beyond the company's tolerance or threshold levels.
- Organizations should use business intelligence software packages to extract risk data and display them on a “dashboard.” Many of these systems feature a traffic-light system, with red, yellow and green lights. If a risk exceeds acceptable levels, a red light pops up, permitting the responsible party to “drill down” into the reasons and make more informed decisions.

A PERMANENT FIXTURE

In the wake of the Sarbanes-Oxley Act of 2002 and more stringent corporate governance and compliance regulations, ERM—no matter who is in charge—is here to stay, says Lam. “To comply with the new governance rules in Sarbanes-Oxley and from the stock exchanges, you need to dig into the underlying operational processes that give rise to the financial statements,” he explains. “That requires continuous monitoring and measuring of these processes. And by the way, they all involve risk.” CPAs, whether as internal auditors or as financial managers, can play a critical ongoing role in the process of minimizing and managing risk. ■



[go back](#)
[©2004 AICPA](#)