# Are You Identifying Your Most Significant Risks?

**Results from a COSO-sponsored survey show that companies need to do a better job in this area.**

**By Mark S. Beasley, CPA; Bruce C. Branson; and Bonnie V. Hancock**

The economic meltdown during the last three years continues to cause numerous stakeholders to question how boards and senior executives are overseeing their organizations' most significant risk exposures. Many have argued that some entities failed because they didn't focus enough on identifying, assessing, and managing their most important emerging risks that were threatening stakeholder value. For others, the pursuit of returns and growth through overly aggressive strategies overshadowed the underlying risks that management and the board had assumed to achieve performance targets. In some cases, organizational leaders were blindsided by unknown risks, largely because they lacked sufficient infrastructure to identify, assess, and monitor emerging risks within their enterprises and because they were overconfident about ad hoc approaches to risk management.

In light of these situations, numerous changes in risk oversight have been occurring. In May 2008, Standard & Poor's announced its efforts in evaluating an issuer's enterprise risk management (ERM) processes as an additional component of their credit evaluation procedures. In March 2010, the Securities & Exchange Commission (SEC) required publicly traded companies to begin providing in their annual proxy statements to shareholders disclosures that describe the board's role in risk oversight. In July 2010, President Obama signed the Federal Financial Reform legislation that mandates risk committees for boards of financial institutions and other entities the Federal Reserve oversees. And more changes are likely to be on the horizon.

To gain a sense of the state of risk oversight across numerous industries and organizations, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) commissioned faculty in the Enterprise Risk Management Initiative at North Carolina State University to conduct a survey this past summer (for more information about the ERM Initiative, see www.erm.ncsu.edu). We conducted the research in conjunction with the member organizations of COSO, which are IMA® (Institute of Management Accountants), the American Accounting Association (AAA), American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), and the Institute of Internal Auditors (IIA). We collected data during June and July 2010 through an online survey instrument sent electronically to members of each of those organizations. (The intended individual was a member of senior management.)

We targeted the survey to individuals involved in leading ERM-related processes or who are knowledgeable about those efforts within their organization. We received 460 partially or fully completed surveys. (Not all questions were completed by all 460 respondents. In some cases, the questions weren't applicable because of the respondents' answers to other questions, and, in other cases, the respondents chose to skip a particular question.) Now we'll provide a summary of the key findings from the study and include observations about factors affecting how likely enterprises will embrace ERM going forward.

**Table 1:** Industry Breakdown

| INDUSTRY DESCRIPTIONS | PERCENTAGES |
|---|---|
| Manufacturing (SIC 20-39) | 24% |
| Finance, Insurance, and Real Estate (SIC 60-67) | 20% |
| Services (SIC 70-89) | 20% |
| Not-for-Profit (SIC N/A) | 11% |
| State or Local Government (SIC 91-99) | 7% |
| Wholesale/Distribution (SIC 50-51) | 5% |
| Retail (SIC 52-59) | 4% |
| Construction (SIC 15-17) | 3% |
| All Other Combined (none greater than 2%) | 6% |

## Description of Respondents

Because the term "ERM" is used often but isn't necessarily understood by everyone in the same way, we provided respondents the following definition of enterprise risk management, which is the definition included in COSO's 2004 *Enterprise Risk Management—Integrated Framework:*

*"Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."*

The largest category of respondents is head of internal audit (37%), followed by chief financial officer (CFO) at 23%. Other respondents include the head of risk management or chief risk officer (12%), controller (10%), member of the board of directors (6%), and numerous other executive positions. The respondents claim to be familiar with their organization's approach to enterprise-level risk management. Using a five-point Likert scale where 1 = not at all familiar and 5 = very familiar, more than 64% selected "5 = very familiar," and an additional 23% selected a value = 4. Thus, many survey participants appear to be knowledgeable about the state of ERM within their organizations.

Almost three-fourths of the respondents represent for-profit enterprises. Slightly more than 38% represent publicly traded companies, and 33% represent privately held, for-profit companies. Almost all respondents represent U.S.-based organizations: 52% are from organizations headquartered in the U.S. that have operations only in the U.S., and 39% represent organizations in the U.S. that have operations inside and outside the U.S. The respondents are from a range of industries. The most common industry is manufacturing (24%), followed by finance, insurance, and real estate (20%) and services (20%). See Table 1 for the breakdown.

## State of Risk Management Practices

Despite growing complexities in the risk environments of most organizations, the level of risk management sophistication in these organizations remains fairly immature. When asked to describe the level of maturity of their organization's enterprise risk management process on a five-point scale where a value of 1 = very immature to a value of 5 = very mature, 14.5% of the respondents described their organization's level of functioning ERM processes as "very immature," 27.9% described their processes as "minimally mature," 36.8% described theirs as "between mature and immature," 17.4% said theirs were "somewhat mature," and 3.4% called theirs "very mature." On a combined basis, 42.4% described the sophistication of their risk oversight as immature to minimally mature. Given that our respondents represent a variety of organizations, including not-for-profit and government entities, we analyzed results for publicly traded companies separately (187 of the 460 respondents represent publicly traded companies). While only 4.7% of those from publicly traded companies rated their ERM maturity as "very mature," which was similar to the full sample, fewer (7.1%) rated their ERM as "very immature." Public company respondents tended to rate their ERM processes in the middle category of somewhere between mature and immature (47.3%).

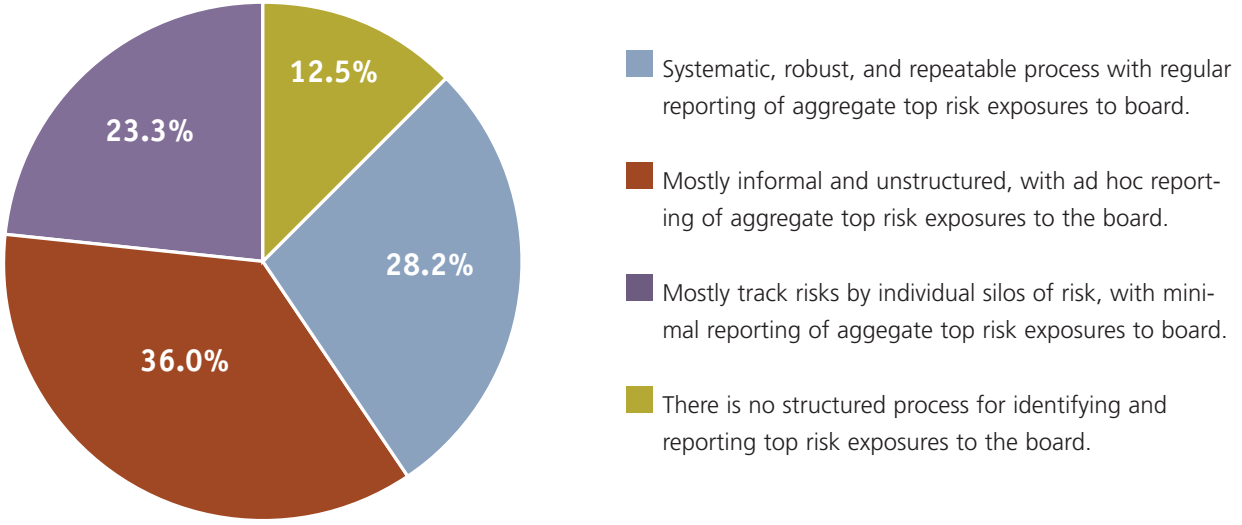
We also asked respondents to pick a statement that best describes their organization's current stage of ERM implementation (see Figure 1). In this case, only 28% of all respondents described their current stage of ERM implementation as "systematic, robust, and repeatable," with regular reporting to the board, while almost 60% of respondents said their risk tracking is mostly informal and ad hoc or tracked only within individual silos or categories as opposed to enterprise-wide. Another 12.5% indicated that their organization has no structured process for identifying and reporting top risk exposures to the board.

The results for publicly traded companies mostly mirror the results reported in Figure 1 for the full sample. Sixty-one percent of publicly traded companies said their risk tracking is mostly informal or ad hoc or tracked only within individual silos or categories. Slightly more publicly traded companies (36.1%) compared to the full sample (28.2%) indicated their current state of ERM implementation is "systematic, robust, and repeatable."

## Governance, Strategy, and Enterprise Risk Oversight

To gain some insight into current practices, we asked respondents to provide more specifics about reporting risk to their organization's board of directors and the delegation of risk oversight to board-level committees. Only 33.6% of all respondents (and 43.2% of publicly traded companies) indicated that the extent to which their boards have formally assigned risk oversight responsibility to a board committee is "significant" or "a great deal" (a score of 4 or 5 on the five-point scale). More than half (52.2%) of all respondents indicated that this had been done not at all or only minimally. When it comes to formally assigning a member of management the responsibility for risk oversight, the results are higher.

**Figure 1:** Risk Tracking—Current Stage of ERM Implementation



## Table 2: Risk Oversight Responsibility

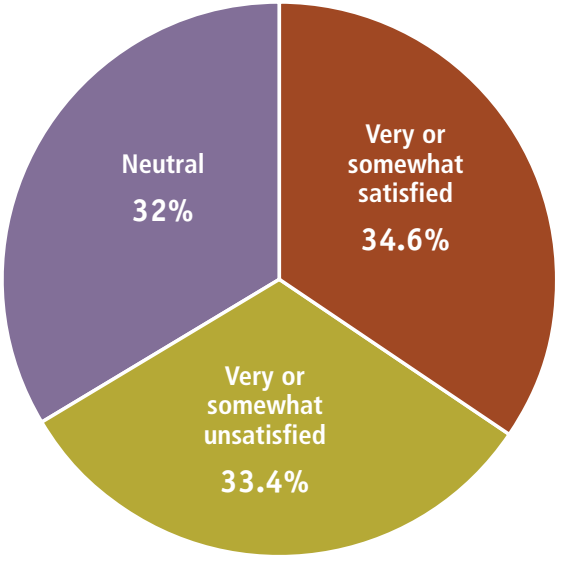
| WHAT IS THE EXTENT TO WHICH EACH OF THE FOLLOWING EXISTS? | NOT AT ALL 1 | 2 | 3 | 4 | A GREAT DEAL 5 |
|---|---|---|---|---|---|
| The board has a subcommittee(s) with primary responsibility for oversight of risk and reporting back to the full board. | 38.5% | 13.7% | 14.2% | 16.2% | 17.4% |
| A member of senior management has formally been assigned responsibility for enterprise-wide risk oversight. | 24.3% | 11.5% | 15.4% | 21.6% | 27.2% |

Almost half the respondents (48.8%) indicated that the extent to which this had been done was "significant" or "a great deal." For the subset of publicly traded companies, 63.4% noted the assignment of responsibility to a member of management was "significant" or "a great deal." See Table 2 for a breakdown.

It's possible that some boards haven't assigned primary responsibility for risk oversight to one of their committees because the full board has retained that enterprise-wide risk oversight role. To gain a sense of the level of board engagement in risk oversight activities, we asked a series of questions.

We prompted respondents to describe the extent to which management formally reports its top risk exposures to the board on a regular, scheduled basis. In this case, almost two-thirds (62.7%) responded that the extent to which this is done is either "moderate," "significant," or "a great deal" (a score of 3, 4, or 5 on the five-point scale), as shown in Table 3. Results for public companies were even stronger, with 79.4% responding in that manner.

## Figure 2: Satisfaction with Risk Oversight Process




In answers to a related question regarding the existence of processes for identifying and monitoring emerging strategic risks, the results declined somewhat, indicating room for improvement. In 44.4% of all responses (and 30.1% of public companies), there was either no process or only minimal processes for identifying and tracking emerging risks. When we asked about management and board monitoring of a robust set of key risk indicators that track emerging risks, the results declined even further, indicating a more specific need for the development of key risk indicators. In this case, slightly more than half (50.3%) of all respondents (and more than 40% of public companies) indicated that this was either not done at all or done only minimally. Collectively, responses to these questions suggest that management's reporting of top risk exposures to the board is occurring, but the underlying process of reporting risk information and related focus on emerging risks and key risk indicators may be casual and less structured or robust.

The survey also revealed that many organizations haven't formally articulated their appetite for risk taking in the context of their stated objectives. Only 27.5% of all respondents indicated that the extent to which they had articulated their risk appetite was "significant" or "a great deal," and more than half (51.7%) have done this not at all or only minimally. Although public companies leaned slightly more toward a formal articulation of risk appetite, the results reported in Table 3 are similar to those unique to public companies.

When asked about their level of satisfaction with their organization's approach to managing its most significant risks, respondents were fairly evenly divided among being

## Table 3: Monitoring Risk

| WHAT IS THE EXTENT TO WHICH EACH OF THE FOLLOWING EXISTS? | NOT AT ALL 1 | 2 | 3 | 4 | A GREAT DEAL 5 |
|---|---|---|---|---|---|
| Management formally reports the entity's top risk exposures to the board on a regular, scheduled basis (e.g., annually). | 20.3% | 16.9% | 18.0% | 24.5% | 20.3% |
| There are structured processes for identifying and monitoring emerging strategic risk exposures. | 21.1% | 23.3% | 25.5% | 18.1% | 12.0% |
| Management and the board regularly monitor a robust set of key risk indicators that track emerging risks. | 26.0% | 24.3% | 24.7% | 16.9% | 8.1% |

## Table 4: Requests for Senior-Executive Involvement

| EXTENT OF REQUESTS FOR INCREASED SENIOR-EXECUTIVE INVOLVEMENT IN RISK OVERSIGHT COMING FROM: | PERCENTAGES | | |
|---|---|---|---|
| | MODERATE | SIGNIFICANT | A GREAT DEAL |
| Boards of Directors | 24.3% | 25.0% | 9.8% |
| Audit Committee | 20.6% | 25.0% | 17.4% |
| Chief Executive Officer | 26.7% | 23.3% | 15.2% |
| Internal Audit | 21.6% | 25.7% | 18.1% |

very or somewhat dissatisfied (34.6%), neutral (32%), and very or somewhat satisfied (33.4%) (see Figure 2). Overall, this would seem to indicate that a majority of respondents may want to see an improvement in the management of their key risks. Public companies were only slightly more satisfied (24.8% were very dissatisfied or somewhat dissatisfied, and 42% were very or somewhat satisfied).

## Emerging Calls for Strengthening Enterprise-Wide Risk Oversight

The survey results indicate that expectations for improving risk oversight in the respondents' organizations are coming from a number of sources (see Table 4). Respondents noted that in 9.8% of the organizations surveyed, the board of directors is asking senior executives to strengthen their risk oversight "a great deal," and 25% are asking for significantly increased oversight. About 24% indicated "moderate" board interest in increasing senior-executive risk oversight.

Increased external pressures now being placed on boards could be prompting these expectations. In general, boards and audit committees are beginning to challenge senior executives about existing approaches to risk oversight, and they are demanding more information about the organization's top risk exposures.

Much of a board's interest in strengthening risk oversight appears to be driven by the audit committee. For organizations that have an audit committee function in place, 17.4% of the respondents say that audit committees are asking executives to increase their risk oversight "a great deal," and 25% are making a significant number of requests for increased oversight. Another 20.6% of respondents at organizations with existing audit committees are experiencing moderate levels of requests from their audit committees for increases in senior-management oversight of risks.

Collectively, these results suggest that 59.1% of the full boards and 63% of audit committees are making "moderate" to "significant" to "a great deal" of requests for more senior-management involvement in risk oversight. In addition, and perhaps because of the board and audit commit-

tee's interest in strengthened risk oversight, the chief executive officer (CEO) is also calling for increased senior-executive involvement in risk oversight. More than 65% of the respondents indicated that the CEO is making "moderate" to "significant" to "a great deal" of requests for increased management involvement in risk oversight. Results related to board, audit committee, and CEO requests for improvements in risk oversight for the subset of public companies are very similar to those of the full sample.

Internal audit also appears to be placing additional expectations on executives regarding risk oversight. For those entities with an internal audit function, 65.4% of the respondents indicated that internal audit is making "moderate" to "significant" to "a great deal" of requests for more senior-management involvement in risk oversight. Interestingly, respondents don't appear to be experiencing significant pressure from external parties to strengthen risk oversight. Sixty-five percent indicated that regulators are "not at all" or "minimally" asking for greater risk oversight, 73% indicated that key stakeholders are either asking "not at all" or "minimally," and 69% noted the same extent of pressure coming from others, such as credit rating agencies, stock exchanges, or other governance reform advocates.

When organizations look for guidance in implementing ERM, they overwhelmingly (54.6%) look to COSO's ERM framework (as do 65% of public company respondents). COSO's ERM framework is by far the most well-known of the frameworks, with 36.7% of respondents reporting they are very familiar with the framework and only 7.9% of respondents indicating they aren't at all familiar with it. The other three frameworks listed—Joint Australia/New Zealand 4360-2004 Standards, ISO 31000-2009, and the Turnbull Guidance—aren't very well known at all, with respondents having no familiarity with them (72.6%, 46.4%, and 51.3%, respectively). Responses from the subset of public companies were very similar.

## Still Immature

Overall, the results of the survey indicate that the state of ERM in most organizations is still relatively immature and underdeveloped and that most respondents are dissatisfied with current risk oversight processes. Although a majority of respondents indicated that management and their board of directors are discussing the organization's top risk exposures, there appears to be a lack of formal process or structure, including the presentation of key risk indicators, to provide the underlying basis or foundation for that discussion. There seems to be room for improvement in underlying processes and procedures to strengthen an organization's identification, assessment, and reporting of key risk exposures arising across all aspects of the enterprise. Results don't differ significantly when considering responses from public companies.

The relatively immature state of risk oversight processes in organizations surveyed may be attributable to several potential factors. Many people may question the value proposition for investing further in their organization's risk management infrastructure. Some may view risk management as mainly serving a compliance function or merely adding levels of unnecessary bureaucracy to the organization, so they fail to see any value to enhancing risk oversight.

**As individuals continue to focus on the need for more effective risk oversight, the level of robustness in risk oversight processes is likely to increase over time.**

In some instances, organizational leaders may not see the interconnectivity of risk oversight and strategy execution, as evidenced by almost half (44.4%) of the organizations having no or only minimal processes for identifying and monitoring emerging strategic risks. A reminder about the fundamental relationship between risk and reward may help some organizations realize the strategic benefits of strengthening risk oversight so that they are more likely to achieve strategic objectives. Refocusing on the reality that risks must be taken to achieve specific return objectives may help organizational leaders realize that more intelligent and focused management of risks will increase the odds that their strategic goals and objectives will actually be achieved. COSO's thought paper, "Strengthening Enterprise Risk Management for Strategic Advantage," may be a helpful resource that articulates the strategic value of effective ERM. (You can find the paper at www.coso.org/guidance.htm.)

In other organizations, the lack of risk oversight maturity is attributable to overconfidence by management and the board of directors in how they currently approach risk oversight. Many organizational leaders believe their ad hoc and informal approaches are ade-

quate and appropriate. In those instances, it may be difficult to make progress until greater external pressures are placed on management and the board or until a significant risk occurs that creates a crisis-management event for organizational leaders to address reactively. Perhaps greater training for management and the board about effective risk oversight processes or engaging external evaluators who can provide objective analysis or benchmarking of existing risk oversight processes against best practices may help highlight weaknesses before an actual value-destroying risk event occurs. COSO's thought paper "Effective Enterprise Risk Oversight: The Role of the Board of Directors," discusses four core responsibilities of boards in the oversight of management's risk processes and top risk exposures arising out of those processes. (You can find the paper at www.coso.org/guidance.htm.)

Fewer than half the organizations surveyed either have no process or only minimal processes for identifying and tracking emerging risks, and more than half do no tracking of key risk indicators at the board or senior-management level. These findings, in combination with the overall levels of dissatisfaction with existing risk oversight, suggest that organizational leaders may desire more robust enterprise-wide risk oversight but are struggling to determine what they should do beyond already existing risk management functions within the entity (e.g., internal audit, legal, insurance, treasury, etc.). Although they are convinced conceptually about the benefits of ERM, they may be struggling to translate concepts into practical application and to pinpoint ways to implement fundamental principles of ERM into already existing processes and functions. The observation that few of the respondents were aware of Volume 2 of COSO's *Enterprise Risk Management—Integrated Framework: Application Techniques*, which contains numerous application examples, suggests that they may need to be reminded about Volume 2 and may need case studies and other implementation techniques and tools known to be helpful in organizations further along in the evolution of their risk oversight processes. (You can download the Executive Summary and find out how to order Volume 2 at www.coso.org/-ERM.htm.)

Change is on the horizon for many of the survey respondents' organizations. Just fewer than two-thirds of the respondents indicated that the board of directors is asking management for moderate to a great deal of increased risk oversight. That, in turn, is resulting in similar calls by the CEO for strengthened risk oversight. In about half the organizations surveyed, a member of management has been formally assigned the responsibility for risk oversight. Thus, as these individuals continue to focus on the need for more effective risk oversight, the level of robustness in risk oversight processes is likely to increase over time. It will be interesting to observe the state of risk oversight in five to 10 years. **SF**

**Note:** Readers should monitor COSO's website (www.coso.org) for resources and materials to help manage enterprise-wide risks. The full report summarizing our survey is available there.

*Mark S. Beasley, CPA, Ph.D., is the Deloitte Professor of Enterprise Risk Management and director of the ERM Initiative at North Carolina State University. A COSO Board member, he specializes in the study of enterprise risk management, corporate governance, financial statement fraud, and the financial reporting process. You can reach him at (919) 515-6064 or mark_beasley@ncsu.edu.*

*Bruce C. Branson, Ph.D., is a professor of accounting and associate director of the Enterprise Risk Management (ERM) Initiative at North Carolina State University. His teaching and research are focused on financial reporting and include an interest in the use of derivative securities and other hedging strategies for risk reduction/risk sharing. You can reach him at (919) 515-4435 or bruce_branson@ncsu.edu.*

*Bonnie V. Hancock is the executive director of the Enterprise Risk Management (ERM) Initiative and is an executive lecturer in accounting at North Carolina State University's College of Management. She has held executive positions at Progress Energy and currently serves on the board of directors for AgFirst Farm Credit Bank and Powell Industries. You can reach her at (919) 513-7425 or bonnie_hancock@ncsu.edu.*