As the result of fallout from the ongoing economic crisis, failures associated with existing risk management processes are already generating calls for reform and increased regulatory scrutiny.

SEC Chairman Mary Schapiro said in an April 2009 speech to the Council of Institutional Investors that “the Commission will be considering whether greater disclosure is needed about how a company—and the company’s board in particular—manages risks, both generally and in the context of setting compensation.” In July 2009, the SEC issued its first response through proposed rules that expand proxy disclosure information about the overall impact of compensation policies on the registrant’s risk taking and the role of the board in the company’s risk management practices. Proposals in Congress call for the establishment of board risk committees composed of independent directors, among other reforms.

Credit rating agencies such as Standard & Poor’s have also focused on an organization’s risk management processes, providing an additional incentive for organizations to consider further enhancement of existing risk oversight infrastructure. Without a doubt, expectations for improvements in how boards and senior executives oversee enterprise-wide risks are significantly on the rise. The question is whether organizations are currently in a position to respond with more robust, enterprise-wide risk oversight.

To provide answers to this question, in September 2008 the authors surveyed more than 700 organizations whose 2008 revenues ranged from $14,950 to $115 billion—with a median for the sample of $50 million—to better understand the current state of enterprise risk oversight. This article provides a brief overview of key findings from that research, Report on the Current State of Enterprise Risk Oversight, and identifies potential opportunities to strengthen risk oversight.

EXPECTATIONS FOR TOP-DOWN, HOLISTIC VIEW OF RISK

While organizations have managed risks for centuries, most have traditionally tackled risk oversight by managing individual “risk buckets” or silos. For example, chief technology officers manage the information technology infrastructure to ensure that IT risks are minimized while general counsels manage legal and regulatory risks. However, only rarely do the individuals charged with risk management responsibilities come together to share risk oversight information.

Much of the shift in thinking about risk oversight has centered on ever-growing calls for boards and senior executives to embrace the business paradigm widely known as enterprise risk management (ERM). ERM is championed as an effective approach to identifying, assessing and monitoring risks across organizations and establishing communication protocols to efficiently share this risk information quickly across the entity. The ERM approach emphasizes a top-down, holistic view of the inventory of key risk exposures potentially affecting an enterprise’s ability to achieve its objectives. Proponents argue that a comprehensive ERM process helps to ensure that significant risks are given adequate consideration by senior management and boards of directors in the strategic planning process. Boards and senior executives use this inventory of risks with the goal of preserving and enhancing stakeholder value.

The survey sought information about various aspects of risk oversight within their organizations. It asked respondents to consider the Committee of Sponsoring Organizations of the Treadway Commission (COSO) definition of ERM as they responded to a series of questions about the state of risk oversight in their organizations. The questionnaire emphasized to respondents key aspects of this definition by noting that ERM
is a formal process; that it is enterprisewide; and that it addresses risks in a portfolio manner, where interactions among risks are considered.

To learn more about factors related to the embrace of ERM in organizations surveyed, the research instrument asked a series of questions about the status of ERM implementation in these companies. The survey found that 44% of the respondents have no enterprisewide risk management process in place and they have no plans to implement one. An additional 18% of respondents without ERM processes in place indicated that they are investigating the concept, but they have made no decisions to implement an ERM approach to risk oversight at this time. Thus, on a combined basis, more than 60% of respondents had no formal enterprisewide approach to risk oversight. Only a small number (9%) of respondents believe they possess a complete formal enterprisewide risk management process. An additional 22% noted that they have partially implemented an ERM process, but not all risk areas are being addressed by that process.

Particularly revealing was the finding that in 74% of the organizations responding to the survey, management does not provide a report to the board of directors describing the entity’s top risk exposures. These responses indicate that the level of enterprisewide risk oversight sophistication in the organizations surveyed is fairly immature and not based on a top-down, holistic approach to risk management. The respondents largely agreed with this assessment as 67% admitted that their risk oversight process is very immature or minimally mature.

These results are especially surprising when almost overwhelming numbers of respondents indicated that the volume and complexity of risks encountered by their companies had increased in the past five years. Ninety-one percent of respondents indicated that the increase in volume and complexity of risks they have faced was greater than minimal. Sixty-nine percent of respondents had experienced at least a moderate operational surprise in that same time frame—with 36% reporting the surprise as at least extensive.

The questionnaire also asked about the risk culture in their organizations. The results showed that more than half of the firms would describe themselves as risk-averse (41%) or strongly risk-averse (10%). Ironically, 47% indicated that they are unsatisfied with the nature and extent of reporting to senior management about the entity’s top risk exposures. Hence, while a significant majority of organizations have experienced a risk climate growing increasingly more complex and featuring more frequent and significant operational surprises, extant risk management programs remain fairly immature and not up to the task of providing timely, comprehensive data to inform senior management and the board of directors of potentially disastrous near-horizon events.

**PERCEIVED BARRIERS TO ERM**

Given the apparent disconnect between a need for a more robust risk management process and the lack of embrace of ERM as an approach to develop rigorous and disciplined risk oversight, we asked respondents about perceived barriers to ERM implementation. The two most common responses were the existence of competing priorities within the organization and insufficient resources to devote to an ERM implementation. Other barriers frequently noted included a lack of perceived value (for an ERM program), lack of board or senior management leadership for ERM, and the perception that ERM translates into added bureaucracy for the organization. Exhibit 1 provides additional data on these responses.
CALLS FOR CHANGE

Despite these perceived barriers, the research indicates that expectations for improving risk oversight in these organizations are on the rise. For 75% of the organizations surveyed, the board of directors is asking senior executives to increase their involvement in risk oversight at least moderately (45% are asking extensively for increased oversight). The data indicate that much of the board’s interest in strengthening risk oversight is being funneled through the audit committee. For respondents in organizations that have an audit committee in place, 86% of the audit committees are asking executives to increase their risk oversight at least moderately (58% are making that request extensively).

Collectively, these results tell that requests for more senior management involvement in risk oversight are pervasive. Internal audit also appears to be placing additional risk management expectations on executives. For those entities with an internal audit function, 83% of the respondents indicated that internal audit is making at least moderate requests for more senior management involvement in risk oversight. Exhibit 2 provides details on these responses. These results indicate that pressures on senior executives to strengthen risk oversight appear to be significantly increasing among the organizations represented.

---

**Exhibit 1**

Reported Barriers to ERM Implementation

<table>
<thead>
<tr>
<th>Description of Barrier</th>
<th>Extensive</th>
<th>Very Significant</th>
<th>Combined Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Competing Priorities</td>
<td>40%</td>
<td>21%</td>
<td>61%</td>
</tr>
<tr>
<td>Insufficient Resources</td>
<td>43%</td>
<td>17%</td>
<td>60%</td>
</tr>
<tr>
<td>Lack of Perceived Value</td>
<td>34%</td>
<td>14%</td>
<td>48%</td>
</tr>
<tr>
<td>Lack of Board or Senior Executive ERM Leadership</td>
<td>28%</td>
<td>10%</td>
<td>38%</td>
</tr>
<tr>
<td>Perception ERM Adds Bureaucracy</td>
<td>26%</td>
<td>11%</td>
<td>37%</td>
</tr>
<tr>
<td>Legal or Regulatory Barriers</td>
<td>4%</td>
<td>1%</td>
<td>5%</td>
</tr>
</tbody>
</table>

**Exhibit 2**

Source of Requests for Increased Risk Oversight

<table>
<thead>
<tr>
<th>Extent of Requests for Increased Senior Executive Involvement in Risk Oversight Coming From:</th>
<th>Moderate</th>
<th>Extensive</th>
<th>A Great Deal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Board of Directors</td>
<td>30%</td>
<td>36%</td>
<td>9%</td>
</tr>
<tr>
<td>Audit Committee</td>
<td>28%</td>
<td>46%</td>
<td>12%</td>
</tr>
<tr>
<td>Internal Audit</td>
<td>30%</td>
<td>43%</td>
<td>10%</td>
</tr>
</tbody>
</table>
ROLE OF BOARD IN RISK OVERSIGHT
For organizations that have already delegated risk oversight responsibility to a specific board committee, we were interested in which committee had received that charge and the types of risks regularly monitored by that committee. As might be expected, a majority of respondents who delegated risk oversight to a committee of the full board assigned that responsibility to the audit committee (55%). Other committees that were reported with some frequency were the executive committee of the board (21% of responses) or a separately established risk committee (18%).

For those organizations where the audit committee had primary risk oversight responsibility, in 19% of the cases only financial risks were being monitored. For an additional 63% of these organizations, operational and compliance risks were also being monitored (in addition to financial risks). Surprisingly, in only 18% of the responses was the committee charged with risk oversight responsibility actively monitoring all entity risks (defined as including strategic risks in addition to the risks named above). Hence, broad oversight of all types of risks does not appear to be a widespread practice for audit committees—the committee most commonly charged with risk oversight.

On the positive side, emerging trends demonstrate that some of the best practices for developing effective board and senior management risk oversight are in place for some organizations. Boards of directors, especially through their audit committees, are increasing their focus on risk issues. When boards are explicitly focusing on risk, they are working with their audit committees, risk committees and executive committees to tackle the complex challenges of top-down risk oversight. Management is also demonstrating a growing interest in creating a more structured approach to risk oversight. Some are responding by establishing senior executive risk leadership positions in their organizations. When they do, those positions are reporting directly to the top of the organization, either through the board or CEO.

CRITICAL FIRST STEPS FOR IMPROVEMENT
Given the growing pressures for more effective risk oversight that are emerging from the recent financial crisis, and the relative immaturity of enterprisewide risk oversight across a wide spectrum of organizations, organizations have a significant opportunity to embrace a top-down, enterprisewide perspective of risk oversight. Results from this survey suggest that there is an urgent need to evaluate existing risk management processes in light of perceived increases in the volume and complexity of risks and operational surprises being experienced by management. That, coupled with a self-described aversion to risk, is likely to spawn greater focus on improving existing risk oversight procedures in organizations today.

CPAs have significant opportunities to contribute to the development of ERM programs in organizations where they may be employed, serve as members of the board of directors, or provide advisory services. CFOs are often charged with the overall responsibility for developing an ERM infrastructure—and persons serving in that role can powerfully influence the scope and breadth of the risk management function.

A starting point for individuals in those positions may be the facilitation of a relatively simple information gathering process (either through interviews, surveys, workshops, table-tops or other information gathering tools) whereby key management personnel consider and describe their views of the top five-to-10 risk exposures the organization is likely to face in a defined time horizon, such as the next three to five years.

An effective approach to generate this kind of thinking is for these individuals to first review the organization’s strategic plan or business unit objectives currently used to drive the organization’s performance to identify specific risk events that might positively or negatively affect the achievement of those plans or objectives. Compilations of these individual views of key risk exposures are likely to highlight differences in views that can then be the focus of subsequent discussions and examinations by executive management and the board.

Once the list of top risk exposures is compiled, it can then be reconciled to existing risk management activities already ongoing within the organization. A basic mapping of risk exposures with existing risk management efforts may quickly reveal gaps in risk oversight capabilities that should be considered by management and the board. Likely to be revealed are key strategic risks that are not currently the focus of any existing risk management activities within the organization.

Board members serving on audit committees are often delegated the responsibility to provide direct oversight of management’s process of overseeing risks and to report on the completeness and effectiveness of that process to the full board. In both these roles (as CFO or as a member of the audit committee of the board), a solid understanding of ERM and general risk management principles is a core requirement in the current environment.

For those working within the internal audit function of their organizations, a major opportunity exists to contribute to the development of an enhanced risk management infrastructure. In 2008, PricewaterhouseCoopers released a survey-based research report titled Internal Audit 2012, which included this statement:
Throughout the next five years, the value of the controls-focused approach that has dominated internal audit is expected to diminish. As this occurs, internal audit leaders must redefine the function’s value proposition and adopt risk centric mindsets if they expect to remain key players in assurance and risk management. … Study results indicate that five identifiable trends—globalization, changes in risk management, advances in technology, talent and organizational issues, and changing internal audit roles—will have the greatest impact on internal audit in the coming years. By understanding these trends and their implications, internal audit leaders can help senior management identify and manage risk, thereby providing added value from the internal audit function.”

As risk management processes become increasingly embedded within organizations, the internal audit function will likely be tapped to ensure that the ERM process is functioning within design parameters and to serve as an independent source of key risk information to be benchmarked against the outputs from the ERM process itself. Many organizations are also asking for assistance from external advisers in developing and refining their risk management efforts. The use of an external consultant to help them with this process can lend objectivity and knowledge of best practices to that effort.

ABOUT THE RESEARCH STUDY
This article describes insights gleaned from a September 2008 survey of CFOs or persons in equivalent positions conducted by North Carolina State University ERM Initiative faculty and supported by a management accounting research grant from the AICPA Business, Industry, and Government group. Survey responses were received from 701 individuals representing organizations that span numerous industries and company sizes.

The most highly represented industry (based on two-digit SIC codes) was manufacturing (22%), closely followed by services (21%), finance, insurance, and real estate (19%), not-for-profit (14%), and wholesale/distribution (9%). Reported 2008 revenues ranged from $14,950 to $115 billion—with a median for the sample of $50 million.

Because the term ERM is used often, but not necessarily consistently understood, respondents were provided the definition of enterprise risk management that is included in COSO’s Enterprise Risk Management—Integrated Framework (see sidebar, “ERM Defined,” below).

The full study, Report on the Current State of Enterprise Risk Oversight, is available at tinyurl.com/mx3kk8.

ERM DEFINED
COSO’s Enterprise Risk Management—Integrated Framework, defines enterprise risk management as follows:

“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.”

—Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2004)

EXECUTIVE SUMMARY

- Expectations for improvements in how boards and senior executives oversee enterprise-wide risks are on the rise. The authors surveyed more than 700 organizations in September 2008 to better understand the current state of enterprise risk oversight. This article provides a brief overview of key findings from that research and identifies potential opportunities to strengthen risk oversight.

- Organizations have traditionally tackled risk oversight by managing individual “risk buckets” or silos. The survey found that 44% of the respondents have no enterprise wide risk management process in place and they have no plans to implement one. An additional 18% of respondents without ERM processes in place indicated that they are currently investigating the concept, but they have made no decisions to implement an ERM approach to risk oversight at this time.

- The two most common perceived barriers to ERM implementation were the existence of competing
priorities within the organization and insufficient resources to devote to an ERM implementation. Despite the barriers, 75% of the organizations indicated the board of directors is asking senior executives to increase their involvement in risk oversight at least moderately.

- A majority of organizations who delegated risk oversight to a committee of the full board assigned that responsibility to the audit committee (55%). Other committees that were reported with some frequency were the executive committee of the board (21% of responses) or a separately established risk committee (18%).

- Steps for improvement include: information gathering to identify the top five-to-10 risk exposures the organization is likely to face in the next three to five years; reconciling the top risk exposures with existing risk management activities already ongoing within the organization; and prioritizing any newly identified unmanaged risks.

Mark S. Beasley (mark_beasley@ncsu.edu) is the Deloitte Professor of Enterprise Risk Management and director of the ERM Initiative at North Carolina State University. Bruce C. Branson (bruce_branson@ncsu.edu) is a professor of accounting and associate director of the ERM Initiative at N.C. State. Bonnie V. Hancock (bonnie_hancock@ncsu.edu) is the executive director of the ERM Initiative and an executive lecturer in accounting at N.C. State.

To comment on this article or to suggest an idea for another article, contact Matthew G. Lamoreaux, senior editor, at mlamoreaux@aicpa.org or 919-402-4435.

AICPA RESOURCES

JofA articles
- “Rising Expectations,” April 08, page 44
- “Checklist: Implementing Enterprise Risk Management,” March 08, page 31
- “Eight Habits of Highly Effective Audit Committees,” Sept. 07, page 46

Use journalofaccountancy.com to find past articles. In the search box, click “Open Advanced Search” and then search by title.

CPE
- Common Frauds and Internal Controls for Revenue, Purchasing and Cash Receipts, a CPE self-study course (#753350)
- Internal Control Essentials for Financial Managers, Accountants and Auditors, a CPE self-study course (#731855)

For more information or to place an order, go to cpa2biz.com or call the Institute at 888-777-7077.

Web site
Audit Committee Effectiveness Center, aicpa.org/audcommctr

Management Accounting Guidelines
- Integrating Social and Political Risk into Business Decision Making
- The Reporting of Organizational Risks for Internal and External Decision Making
- Identifying, Measuring and Managing Organizational Risks

AICPA members may download Management Accounting Guidelines for free at tinyurl.com/5f3v62.

OTHER RESOURCES

Web site
ERM Initiative at North Carolina State University’s College of Management, erm.ncsu.edu