COSO

Committee of Sponsoring Organizations of the Treadway Commission

Thought Leadership in ERM

BOARD RISK OVERSIGHT

A PROGRESS REPORT

Where Boards of Directors Currently Stand in Executing Their Risk Oversight Responsibilities

By

protiviti®

Risk & Business Consulting.
Internal Audit.

Author

Protiviti (www.protiviti.com) is a global business consulting and internal audit firm composed of experts specializing in risk, advisory and transaction services. The firm helps solve problems in finance and transactions, operations, technology, litigation, governance, risk, and compliance. Protiviti's highly trained, results-oriented professionals provide a unique perspective on a wide range of critical business issues for clients in the Americas, Asia-Pacific, Europe and the Middle East.

Protiviti has more than 60 locations worldwide and is a wholly owned subsidiary of Robert Half International Inc. (NYSE symbol: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

protiviti®
Risk & Business Consulting.
Internal Audit.

COSO Board Members

Preface

This project was commissioned by COSO, which is dedicated to providing thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control, and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations. COSO is a private sector initiative, jointly sponsored and funded by the following organizations:

American Accounting Association

American Accounting Association (AAA)

AICPA

American Institute of Certified Public Accountants (AICPA)

fei

Financial Executives International (FEI)

ima

Institute of Management Accountants (IMA)

IIA

The Institute of Internal Auditors (IIA)

COSO
Committee of Sponsoring Organizations of the Treadway Commission

www.coso.org

Thought Leadership in ERM

BOARD RISK OVERSIGHT

A PROGRESS REPORT

Where Boards of Directors Currently Stand in Executing Their Risk Oversight Responsibilities

Research Commissioned by

COSO

Committee of Sponsoring Organizations of the Treadway Commission

December 2010

www.coso.org

Introduction

Risk oversight is a high priority on the agenda of most boards of directors. Recently, the importance of this responsibility has become more evident in the wake of an historic global financial crisis, which disclosed perceived risk management weaknesses across financial services and other organizations worldwide. Based on numerous legislative and regulatory actions in the United States and other countries as well as initiatives in the private sector, it is clear that expectations for more effective risk oversight are being raised not just for financial services companies, but broadly across all types of businesses. Boards are taking a fresh look at the qualifications of their members, how they operate, and the extent to which they avail themselves of the appropriate officers of the organization and other expertise to understand the enterprise's risks and how those risks are being managed. Directors are also looking into whether their board's committee structure and the information to which each committee has access are conducive to effective risk oversight.

To develop deeper knowledge of the risk oversight process as it is applied by today's boards of directors, and to understand both the current state and desired future state of board risk oversight as viewed by directors, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) commissioned Protiviti, a global business consulting and internal audit firm, to conduct a survey regarding the risk oversight responsibilities of the board of directors and how those responsibilities are being performed. As detailed in the following pages, the results shed new light on how boards are fulfilling their risk oversight obligations, the maturity of their processes for meeting these responsibilities, and key areas offering opportunities for improvement as the risk oversight playbook evolves.

Respondents included more than 200 current and past board members from a broad range of industries and organization sizes. See the Methodology and Demographics sections for details.

We at Protiviti, along with the COSO board, want to thank all of the participants for their time and contributions to our survey. We hope this study will be of interest to you, your board and your organization. We would welcome your opinions and feedback on the results of this research.

protiviti®
Risk & Business Consulting.
Internal Audit.

December 2010

Content Outline

Page

Executive Summary

Board Risk Oversight: Some Progress With Opportunities for Further Improvement

In assessing the overall results of the Board Risk Oversight Survey, we found there are mixed signals about the effectiveness of board risk oversight across organizations. While many boards of directors believe they are performing their risk oversight responsibilities diligently and achieving a high level of effectiveness, a strong majority indicate that their boards are not formally executing mature and robust risk oversight processes. Just over half of the respondents rate the risk oversight process in their organizations as effective or highly effective.

The results were somewhat better among respondents from public companies, particularly large ones; these organizations continue to believe they are proactive in their risk oversight efforts. However, responses to several questions about key elements of risk oversight suggest the board's risk oversight is not always supported by robust underlying processes and there is overall dissatisfaction among a significant number of directors in several areas, including how risks are considered in the context of the organization's strategy. Notable variations in results exist across various organizations, including differences across the nature of the entity (i.e., publicly traded, privately held, not-for-profit), size of entity, and industry represented.

The results of this study reveal a number of areas for improving board risk oversight. These improvements would enable boards to advance the maturity of the risk oversight process. These points are summarized below and detailed in the following pages.

There Is an Opportunity to Improve the Robustness of the Risk Oversight Process

More than half of the survey participants noted the board's risk oversight process is either "effective" or "highly effective"; however, there also is general agreement among respondents that there should be a more structured process for monitoring and reporting key risks to the board. While just over half of the respondents believe there are processes for understanding and challenging assumptions and inherent risks associated with the business strategy and that there are processes in place to monitor the impact of changes in the environment on the strategy, fewer than 15 percent of respondents noted that the board is fully satisfied with those processes.

There Is an Opportunity to Enhance Risk Reporting to the Board

Respondents reported on the types of risk reporting their boards receive at least annually along with those that they do not receive. The most common types of risk reporting received at least annually by boards include a high-level summary of top risks for the enterprise as a whole and its operating units; a periodic overview of management's methodologies used to assess, prioritize and measure risk; and a summary of emerging risks that warrant board attention. Among those not received annually by most boards include scenario analyses evaluating the effect of changes in key external variables impacting the organization; a summary of exceptions to management's established policies or limits for key risks; and a summary of significant gaps in capabilities for managing key risks and the status of initiatives to address those gaps. The results show that, if reports are not received at least annually, they are generally received on an as needed basis or not at all.

These findings reveal an opportunity for organizations to improve the risk reporting process and increase the regularity of reporting according to the nature of the organization's operations and risk profile as well as the board's specific needs.

There Is an Opportunity to Improve the Risk Appetite Dialogue

The survey results suggest that within many organizations efforts are underway to understand better the entity's risk appetite (i.e., understanding the boundaries and limits that the organization sets on behavior for its strategy and operating model). However, the findings show that boards and their organizations can benefit from a more rigorous process. While respondents generally indicated they have routine discussions regarding risks that are acceptable for the organization to take, just 14 percent reported that this activity is sufficient for the board's purposes. It is important to note, though, that responses in this part of the study were higher consistently among directors from public companies, with the highest level of satisfaction with the risk appetite dialogue reported by directors from large public companies, underscoring the maturity of the risk oversight process in these organizations.

There Are Opportunities to Improve Monitoring of the Risk Management Process

While the survey focused exclusively on the perspective of board members regarding risk oversight, the link between risk oversight and the effectiveness of the risk management process is inextricable. According to the results of the study, nearly two-thirds of the respondents noted that board monitoring of the organization's risk management process is not done at all or is carried out in an ad hoc manner. About half of the respondents reported that their boards have no formal processes to assess periodically whether the organization's risk management system is resourced sufficiently. Again though, the view is more positive among public companies, where such board monitoring is more robust (64 percent overall, with public companies with annual revenue greater than $1 billion reporting 74 percent). Of note, while most respondents reported that there is a process followed by management to provide timely information to inform the board's risk oversight process, an overwhelming majority of directors noted that this process could be improved.

Many Organizations Can Do More to Apprise the Board of Significant Risk Matters

The results suggest that while many companies have a process to inform the board regarding the most significant risks and how those risks are being managed, in relatively few organizations is this process sufficiently defined and rigorous. Based on the survey's findings, there are opportunities to improve processes to notify the board when the organization has exceeded its risk limits, and to ensure that risk issues are addressed in an appropriate and timely manner. In addition, 44 percent of the directors reported that management does not have a process to ensure that deficiencies are remediated appropriately and timely, and 37 percent noted that the organization does not assess extreme high impact/low likelihood events (some of which may be so-called "black swans"). As noted with other findings, the results for public companies evidenced a higher percentage of organizations with functioning processes addressing these matters.

Boards Can Self-Evaluate the Risk Oversight Process Better and More Frequently

Almost one-third of the respondents noted that the board does not self-evaluate its risk oversight processes to determine if it is meeting its oversight responsibilities, while an additional one-third only do so on an ad hoc basis. Less than one in 10 rate this self-evaluation to be a robust and mature activity, with the board satisfied with the supporting self-assessment process.

Overall Conclusions

While many board members perceive that their board's risk oversight process is operating effectively, particularly those directors from larger publicly held organizations, there are opportunities for improvement for most organizations as well as several noted obstacles to be considered. The findings of this survey provide valuable insights into how an organization, regardless of how the board organizes itself for risk oversight, can advance this critical process to a more mature stage so that it is more systematic, robust and repeatable. These opportunities are identified and detailed throughout this report. A summary of Protiviti's recommendations to improve board risk oversight effectiveness, based on the results of the survey, is also presented at the end of this report.

Methodology

COSO commissioned Protiviti to conduct the Board Risk Oversight Survey in the third quarter of 2010. By invitation (Protiviti used a variety of lists of directors, including subscription lists from two publications serving boards of directors), more than 200 board members completed all or portions of an online questionnaire designed to assess the current state and desired future state of risk oversight as applied by boards on which respondents serve or served as directors. Specific areas addressed included board involvement in issues related to the entity's risk philosophy and risk appetite, risk management practices, portfolio of existing risks in relation to risk appetite, and appraisal of significant risks and related responses.

Because completion of the survey was voluntary, there is some potential for bias if those directors choosing to respond have significantly different views on matters covered by the survey from those who did not respond. This is an issue inherent in most studies of this nature. Therefore, our study's results may be limited to the extent that such a possibility exists. In addition, some directors answered certain questions while not responding to others. Despite these limitations, we believe the results herein will be of interest to directors seeking insight regarding the current state of maturity of the board's risk oversight process and what can be done to advance the maturity of the process.

Demographics

Survey participants were asked to provide demographic information about the nature, size and location of their organizations, as well as their specific experience as a board member. All demographic information was provided voluntarily. Among the notable demographics of the respondents:

- More than 50 percent represent publicly held organizations.
- A majority have served either as a member or as a chair of the audit committee.
- More than 40 percent have served on their boards for 10 years or more and at their current organization for more than four years.
- Almost 80 percent are from organizations based in the United States (see Table 1).
- The most-represented industry groups are financial services, not-for-profit, consumer products and services, and healthcare and life sciences (see Table 2).

Table 1

Geography	Percent of Response	Percentage of Mix Within Each Geography		
		Public	Private	Not-for-Profit
U.S. based – domestic operations	53%	52%	19%	29%
U.S. based – domestic and international operations	24%	81%	9%	10%
Internationally based	23%	27%	47%	26%

Table 2

Industry	Percentage
Financial services	25%
Not-for-profit	17%
Consumer products and services	15%
Healthcare and life sciences	10%
Technology, media and communications	9%
Industrial products	8%
Energy	7%
Multi-industry	5%
Government	4%

Based on the distribution of responses, we analyzed the results for different segments of the population to determine whether the results were skewed by any segment overall. For example, we sought to understand the impact that the comparatively large number of participants from the financial services industry had on the overall results. In addition, given the distinctive differences of a not-for-profit or government organization compared to a commercial enterprise, we analyzed the specific results from those respondents to understand any potential bias that may have affected the overall results. We also took note of key differences in the results between public and private companies as well as the impact of the financial services industry and size within the public company respondents.

Overall, there were more distinct differences noted when analyzing public company responses, including differences between financial services and other sectors overall as well as the impact of larger companies with revenue over $1 billion. These differences are detailed throughout the report.

Survey Results: Key Findings and Analysis

For purposes of this study, "risk oversight" describes the role of the board of directors in the risk management process. The risk oversight process is the means by which the board determines that management has in place a rigorous process for identifying, prioritizing, managing and monitoring its critical risks and that this process is improved continuously as the business environment changes. It also involves board understanding of the most significant risk exposures and evaluation of whether those exposures are within the enterprise's appetite for risk-taking. By contrast, "risk management" is what management does. Risk management focuses on the design and implementation of processes to manage risks, including appropriate supervision and monitoring to ensure policies are carried out and processes are executed in accordance with the board-approved strategy and management's selected performance goals and risk tolerances. Effective risk management ensures that risk exposures are within the organization's appetite for risk taking.

COSO's *Enterprise Risk Management – Integrated Framework* points out that through the risk oversight process, the board should:

- Understand the entity's risk philosophy and concur with the entity's risk appetite.
- Know the extent to which management has established effective enterprise risk management of the organization.
- Review the entity's portfolio of risk and consider it against the entity's risk appetite.
- Be apprised of the most significant risks and whether management is responding appropriately.

The board's oversight process should be distinguished from executive management's responsibility to provide supervision of the organization's risk management process. The information in this report should be reviewed with this distinction in mind.[1]

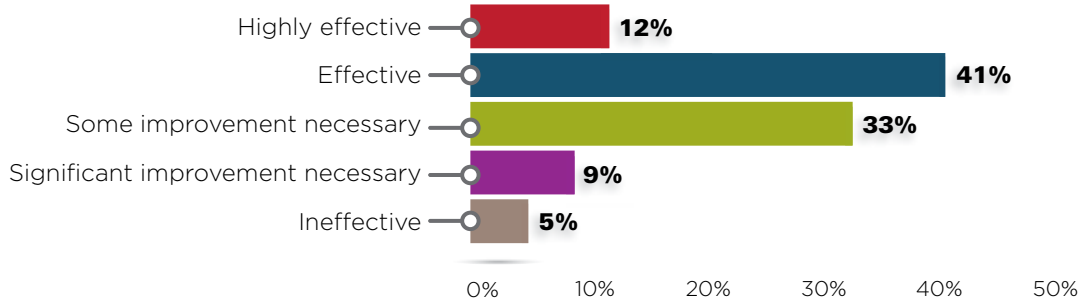
Each of the following sections contains detailed results and analysis. Some also contain commentary that is provided under a separate subhead.

Directors Believe the Robustness of the Risk Oversight Process Can Be Improved

Respondents agree that there should be a structured process for monitoring and reporting key risks to the board, and that the board has overall responsibility for risk oversight. However, for a large majority of the survey questions, marginally positive responses were received with regard to whether key elements of risk oversight are routinely in place, and in most instances these elements are not supported by robust underlying processes. A strong majority of respondents – 71 percent – indicated that their boards are not formally executing mature and robust risk oversight processes. While the results were the same among respondents from public companies, within this group, 50 percent of directors from companies in the financial services industry reported that their boards are not executing mature and robust risk oversight processes, whereas the response from those with nonfinancial services companies was much higher (78 percent).

Overall, 53 percent of the survey respondents noted the board's risk oversight process is either "effective" or "highly effective." However, responses to questions regarding specific aspects of the process did identify a number of key areas for improvement. (These areas are discussed later in this report.)

What is the overall effectiveness of the board's risk oversight process?



[1] For more information about the board's role in enterprise risk oversight, see COSO's *Effective Enterprise Risk Oversight: The Role of the Board of Directors*, 2009 (www.coso.org).

Looking across demographics and the directors' perceived effectiveness of the risk oversight process, there is some variation in the results based on size and type of organization. For example, 59 percent of all public company respondents and 65 percent of respondents from public companies with annual revenue greater than $1 billion indicated their risk oversight processes are either effective or highly effective. Directors from public companies with less than $1 billion in revenue, private companies, not-for-profits and government organizations reported a much lower level of effectiveness. For example, only 13 percent of not-for-profit organization directors reported that risk oversight is either effective or highly effective. Within public companies, more respondents from financial services institutions reported that their risk oversight process is either effective or highly effective (74 percent) than respondents from nonfinancial companies (54 percent).

The elements contained within subsequent sections of this report discuss in detail some of the insights provided by the respondents regarding areas for improvement, as well as suggestions for how organizations can advance their capabilities to a higher stage of maturity related to these areas.

Protiviti Commentary

Given the attention directed over the last 10 years to public companies improving corporate governance and risk management, particularly with respect to financial reporting, it is not surprising that directors from larger public organizations expressed a higher level of satisfaction with the risk oversight process than their counterparts from smaller organizations, private organizations and not-for-profits. Also, given the intensive regulatory environment, it would be expected that financial services institutions are more likely to have robust risk oversight processes, although some observers believe that the financial crisis has challenged that perception.

It may appear that there is a disparity between the findings that (a) 71 percent of respondents indicated that their board is not formally executing a mature and robust risk oversight process and (b) 53 percent of the survey respondents noted the board's risk oversight process is either "effective" or "highly effective." One possible explanation for these findings is some respondents may be of the view that, given the company's circumstances, a robust and mature process is not necessary to attain effective results. Also, there may be confusion over what a robust and mature process is.

What is a more robust and mature process? Generally it is one that is repeatable over time, well-defined, supported by rigorous methodology and analytical frameworks and applied periodically over time as opposed to on an "as needed" basis. Process inputs and requirements, process activities and the expertise needed to execute them are articulated clearly, with nonessentials eliminated and outputs quantitatively determined, anticipated and used for decision-making. The requisite skills and experience needed to execute the process are in place, with role models evident. The process is supported by effective communications, collaboration and knowledge sharing to improve the process continuously. Finally, the activities may be embedded within core management business processes. For example, robust information about risks arising across the organization exists if there is common risk language, a rigorous process and methodology for creating the information, a clear view as to who needs the information and why, effective systems and reliable internal and external data sources, and alignment with the strategy setting and/or business planning processes.

For a Majority of Organizations, Risk Oversight Responsibility Resides With the Full Board

In a substantial majority of cases, the board retains overall responsibility for risk oversight.

Does the full board retain overall responsibility for risk oversight?

Response	Percentage
Yes	84%
No	16%
Total	**100%**

Public companies report an even higher percentage, with almost nine out of 10 charging the full board with overall responsibility.

We also inquired about the role of board committees in the risk oversight process. Of the board committees, the results reveal:

- More than nine out of 10 respondents (93 percent) reported that their boards have an audit committee (95 percent for public companies and 98 percent for public companies with revenues greater than $1 billion). The audit committee consistently has the most involvement in the board's risk oversight process, either overall or related to specific risks germane to the committee's activities.

- More than eight out of 10 respondents (83 percent) reported that their boards have a governance committee (88 percent for public companies and 92 percent for public companies with revenues greater than $1 billion). In addition, 44 percent of respondents reported that their boards have a risk committee (29 percent for public companies and 20 percent for public companies with revenues greater than $1 billion).

Risk committees and governance committees also play substantial risk oversight roles in organizations where they have been established.

- Another finding of particular interest relates to the deployment of risk committees by boards of public companies: When comparing financial services board members to those from nonfinancial services organizations, the response as to whether a risk committee existed was 47 percent versus 24 percent.

With regard to the use of the committee structure to assist in the fulfillment of these responsibilities, the results indicate that 98 percent of audit committees play an active role in risk oversight. The response was split almost evenly between the audit committee having a pervasive view across all enterprise risks and a focused involvement for specific risks germane to the committee's activities. For respondents from public organizations with an audit committee, 59 percent noted that the audit committee has a more expansive role in the overall risk oversight process as opposed to being limited to the risks germane to the committee's normal ongoing activities, with the corresponding results for public companies with revenues greater than $1 billion being 65 percent. By contrast, directors from private and not-for-profit organizations indicated that this is less often the case. However, across all organization types the audit committee is actively involved in the risk oversight process.

For the audit committee, indicate the level of involvement in the board's risk oversight process.

Organization Type	Extensive Involvement Across Risk Oversight	Involvement Relative to Risks Germane to Committee Activities
Public	59%	39%
Private	42%	58%
Not-for-profit	38%	56%

In looking at the location of the organizations, 94 percent of respondents of U.S.-based organizations believe the audit committee is actively involved. However, only 77 percent of directors with organizations based outside the United States noted this to be the case.

Protiviti Commentary

These survey findings suggest boards are gaining valuable support by assigning aspects of their risk oversight responsibilities to their various standing committees, with such responsibilities addressing, at a minimum, the risks inherent in the scope of each delegated committee's activities as set forth in the respective committee charter. For example:

- Audit committees typically oversee financial reporting risks and certain compliance-related risks that can have financial reporting implications. In addition, for New York Stock Exchange-listed organizations, the audit committee charter must include the committee's duties and responsibilities to discuss risk assessment and risk management policies.
- Governance committees oversee such governance risks as board leadership and composition, board structure, and other matters.
- Risk committees oversee the risks specifically included within their scope. These risks vary widely based on the nature of the industry and the complexity of the organization's risks, requiring focused expertise to provide appropriate oversight.
- Compensation committees oversee risks related to how the compensation structure drives behavior within the organization.
- Strategy and finance committees oversee strategic risks.

To enhance the transparency of the oversight process, organizations may want to consider documenting formally the roles and responsibilities related to risk oversight in the board and/or committee charters. Specifically, they may want to clarify which responsibilities and duties will be handled by the full board and which of these will be delegated to the responsible standing committees to ensure major gaps and overlaps in oversight of top risk exposures do not occur.

There Is an Opportunity to Enhance Risk Reporting to the Board

Forming the backbone of risk oversight is the board's ability to obtain substantive risk information from internal sources and, when appropriate, from outside sources. To obtain a perspective regarding the type of information provided to the board on a periodic basis, the survey provided a listing of nine illustrative examples of risk reporting. Respondents were asked to identify the frequency with which each is received in their respective organizations.

The top three reports designated by the respondents as being received by the board at least once a year are:

- High-level summary of top risks for the enterprise as a whole and its operating units (71 percent)
- Periodic overview of management's methodologies used to assess, prioritize and measure risk (65 percent)
- Summary of emerging risks that warrant board attention (59 percent)

The top three reports designated by the respondents as not being received by the board at least annually are:

- Scenario analyses evaluating impact of changes in key external variables impacting the organization (49 percent)
- Summary of exceptions to management's established policies or limits for key risks (49 percent)
- Summary of significant gaps in capabilities for managing key risks and the status of initiatives to address those gaps (53 percent)

Following are the overall results for risk information received by the board:

The board receives the following risk information:

Information Received:	Quarterly	2–3 times a year	Annually	Subtotal (at least annually)	Less than once a year	Ad hoc, e.g., as requested by board	Not at all
Periodic overview of management's methodologies used to assess, prioritize, and measure risk	19%	17%	29%	**65%**	3%	19%	13%
High-level summary of the top risks for the enterprise as a whole and its operating units	22%	18%	31%	**71%**	4%	16%	9%
Summary of emerging risks that warrant board attention	25%	21%	13%	**59%**	3%	25%	13%
Summary of significant gaps in capabilities for managing key risks and the status of initiatives to address those gaps	21%	12%	20%	**53%**	4%	23%	20%
Risk reports, such as trends in key risk indicators	30%	13%	15%	**58%**	5%	12%	25%
Report on effectiveness of responses for mitigating the most significant risks	28%	12%	16%	**56%**	3%	23%	18%
Summary of significant changes in the assumptions and inherent risks underlying the strategy and their effect on the business	21%	13%	22%	**56%**	4%	21%	19%
Summary of exceptions to management's established policies or limits for key risks	25%	11%	13%	**49%**	5%	21%	25%
Scenario analyses evaluating the impact of changes in key external variables impacting the organization	16%	10%	23%	**49%**	4%	20%	27%

There is little variation in the results across different organizational demographics, with the exception that public organizations are providing more regular reporting to the board on risk-related matters, showing more favorable results for all nine illustrative examples in terms of receiving the reports at least once a year. Furthermore, directors from public companies with revenue of $1 billion or more reported even more favorable results for all nine illustrative examples. Finally, the financial services industry reflected the highest marks among all industry categories in seven of the nine illustrative examples in terms of receiving the reports at least once a year. That said, regardless of how the data is cut, there is evidence that there are organizations receiving reports less than once a year, on an ad hoc basis or not at all.

The Risk Appetite Dialogue and Connection to Strategy Planning and Executive Management Require Improvement

While it appears there are efforts underway to understand the concept of risk appetite (i.e., understanding how much risk the organization can accept in the execution of its strategy and operating model), the survey results suggest that boards and their organizations can benefit from a more defined and rigorous process. Starting with the business strategy itself, just over half of the respondents (52 percent) reported that the board develops an understanding of, and appropriately challenges, the organization's strategy, including its underlying assumptions and inherent risks. Likewise, a majority of respondents (55 percent) reported that there is effective monitoring of the environment for changes that could impact both the strategy and the associated risks. However, on both of these points, less than 15 percent of respondents noted that the board is satisfied with the processes underlying these activities, i.e., the other respondents reported that either improvements are needed or the supporting processes are ad hoc in nature.

On another matter, 59 percent of respondents reported that the board monitors the company's culture and incentive compensation structure to ensure that the proper tone is set towards managing risk. For U.S. listed companies, this assessment is necessary for purposes of responding to the proxy disclosure requirements of the Securities and Exchange Commission (SEC). This point is relevant to risk appetite because an organization's culture and compensation structure can impact its propensity to take risk.

A majority of respondents (56 percent) indicated they have routine discussions regarding risks that are acceptable for the organization to take in achieving strategic objectives. These discussions help boards and management understand the risks inherent in the organization's value creation strategies (see commentary on the following page). However, just 14 percent of respondents reported that the board is satisfied with the processes underlying this activity, and only 40 percent indicated they routinely express risk appetite in either quantitative or qualitative terms. Interestingly, a similar percentage noted that the board approves management's expression of risk appetite for purposes of establishing limits on risk-taking activities, suggesting that risk appetite may not always be driven down into the business to set risk tolerances and operating limits.

From a demographics standpoint, the survey results suggest that boards at public organizations more routinely challenge the corporate strategy and its underlying assumptions than boards of private organizations and not-for-profits (62 percent compared to 39 percent). More directors from public organizations indicated that there is a routine process to use risk appetite to set risk limits and tolerances compared to directors within private and not-for-profit organizations (49 percent versus 35 percent). Finally, directors of public organizations noted that there is more regular monitoring of the external environment to identify changes in critical strategic assumptions and risks than was noted by respondents representing private and not-for-profit organizations (66 percent compared to 41 percent).

With respect to public companies, larger organizations (greater than $1 billion in revenue) reported a higher level of routine performance of processes pertaining to understanding and challenging strategic assumptions and risks, monitoring the external environment for changes, monitoring the company's culture and incentive compensation structure, and fostering a periodic dialogue on acceptable risks, ranging from 10 to 13 percentage points higher than the overall public company results. Also, there is a clear distinction in the responses among not-for-profit organizations and the underlying risk appetite activities and discussions being less robust. For the five questions related specifically to risk appetite, responses from directors with not-for-profit organizations were, on average, 12 percent lower when assessing whether activities are performed on a routine basis. For individual questions, these ranged from 7 to 20 percent. Finally, 77 percent of directors from financial services organizations reported that there is a process for expressing the organization's risk appetite as compared to just 33 percent for their nonfinancial public company counterparts.

Protiviti Commentary

Given that risk levels and uncertainty have changed significantly over recent years for most organizations, the board and management may find it beneficial to engage in a dialogue on a periodic basis regarding risk appetite, possibly covering such topics as the maximum acceptable level of performance variability in specific operating areas, targeted operating parameters, upside/downside debates on significant matters, the risks and assumptions inherent in the corporate strategy, the "hard spots" and "soft spots" in the business plan, and the implication of changes in the operating environment on the core assumptions inherent in the strategy, including the desired appetite for risk. The board also may want to consider when and under what circumstances it should be informed of exceptions and near misses to the organization's risk tolerance parameters and any planned actions to address them through policy and process improvements.

In addition to fostering an active dialogue between the board and management, the formal articulation of a statement of risk appetite establishes a common understanding of the approach to risks that underpin the enterprise's strategy. The challenges in articulating risk appetite for many organizations include the forward-looking and intangible nature of risk; the reality that some of the enterprise's more significant risks may not be susceptible to quantification; and the potentially distracting buzz pertaining to such behaviors described as "risk-averse," "opportunistic," or "risk-taking." In defining risk appetite, consideration should be given to the historical strategic and operational boundaries that management applies on a continual basis to manage the business.

A risk appetite statement might include several assertions around the strategic, operational and financial parameters that, taken together, frame the organization's risk appetite. The assertions must be viewed together rather than as an individual stand-alone assertion. Following is an example of a risk appetite statement with several assertions for a nonfinancial company without significant commodity or currency exposure:

- **Market growth:** We will aggressively pursue regional strategies to meet our market growth objectives (increase of 2 percent in market share) and invest in and develop key markets, including China and Latin America.
- **Reputation and brand image:** When making decisions at all levels of the company, we will consider the impact to our reputation and brand.
- **Investment limits:** We will place a ceiling on our funding of new acquisitions, capital expenditures, and R&D at $300 million, $150 million, and $40 million, respectively, during the next 24 months.
- **Target debt rating:** We will seek to maintain an enterprise-level debt rating of investment grade or better.
- **Self-sustaining growth:** New business will maintain our working capital ratio between 1 percent and 1.5 percent.
- **Financial strength:** We will maintain an EBIT/interest ratio between 4 percent and 5 percent.
- **Loss exposure:** We will manage our operational activities and exposures to avoid losses to pre-tax operating margins of more than $25 million.
- **Customer dependence:** A single customer will not account for more than 10 percent of total sales.

By initially stating risk appetite in this way, the risks the organization is intent on taking are articulated and the parameters within which those risks are taken become more evident to management and the board. Often, these parameters already exist to some degree, enabling authority and limits to be cascaded down through the organization in the form of delegations and policies. If applied appropriately, this process facilitates the risk appetite dialogue at the board level and the controlled consideration of risk in day-to-day activities. The objective is for management and the board to arrive at a shared understanding of risk appetite so that the activities of the organization and designated individuals will be aligned with the mutually agreed-upon risk profile. Risk appetite thus becomes a benchmark for discussing value creation opportunities as they arise. Changes in risk appetite would ordinarily require a review of the established limits to ensure there is continued alignment to the current risk appetite.

COSO is publishing a thought paper in the not-too-distant future, ***Enterprise Risk Management – Better Understanding and Communicating Risk Appetite and Risk Tolerance***, to provide further insight on this important element of enterprise risk management. Monitor the COSO website (www.coso.org) for issuance of that document.

Monitoring of Risk Management Can Be Improved

While the survey focused exclusively on the perspective of board members regarding risk oversight, the link between risk oversight and the effectiveness of the risk management process is inextricable. Nearly two-thirds of respondents (65 percent) indicated that monitoring of the risk management process is not done at all, is ineffective, or is carried out through an ad hoc process. Just over half of the participants (53 percent) replied that their organizations receive a report on the top enterprise risks. Not surprisingly, boards of public companies receive more regular reporting on top enterprise risks to inform the board's risk oversight process than those at private organizations and not-for-profits (64 percent compared to 40 percent). Larger public companies (revenue greater than $1 billion) reported higher results, at 74 percent. Finally, among public companies, 82 percent of directors with financial services institutions reported that they receive periodic risk profile information regarding significant enterprise risks, compared to 58 percent reported by their nonfinancial company counterparts.

Please assess the following statement:
There is effective monitoring of the risk management process, including monitoring the environment for changes that could impact both the strategy and associated risks.

Response	Percentage
Performed as a robust and mature activity, with the board satisfied with the supporting process	13%
Performed as a rigorous defined activity with an ongoing process; however, improvements needed	22%
Performed routinely; however, the supporting process is ad hoc	20%
Performed on an as-needed basis, as decided by the board or management	19%
Not performed, but under development	14%
Not performed, with no plans to perform	12%
Total	**100%**

A majority of directors (55 percent) said there is a process followed by management to provide adequate and timely information to enlighten the board's risk oversight process. While the respondents noted that this process is in place, 85 percent indicated it could be improved. Finally, just over half of respondents (53 percent) indicated that there is a periodic assessment of the resources supporting the risk management system. As with other findings, results for public companies evidenced a higher percentage of organizations with functioning processes.

Please assess the following statement:
The board periodically assesses whether the organization's risk management system (including policies, processes, people and reporting) is sufficiently resourced.

Response	Percentage
Performed as a robust and mature activity, with the board satisfied with the supporting process	14%
Performed as a rigorous defined activity with an ongoing process; however, improvements needed	21%
Performed routinely; however, the supporting process is ad hoc	18%
Performed on an as-needed basis, as decided by the board or management	20%
Not performed, but under development	15%
Not performed, with no plans to perform	12%
Total	**100%**

Protiviti Commentary
As reported earlier, there is an opportunity to enhance risk reporting. This theme is related to the finding regarding the monitoring of risk and risk management, and suggests that risk monitoring processes require more attention and greater access by the board. To this end, COSO's thought paper, *Developing Key Risk Indicators to Strengthen Enterprise Risk Management*, is designed to help management develop key risk indicators (KRIs) to heighten board and management enterprise risk awareness (see www.coso.org).

Many Organizations Need to Do More in Apprising Their Boards of Significant Risk Matters

While a majority of respondents (59 percent) indicated there is a process to inform the board of how the company's most significant risks are being managed, less than one-third of those respondents are of the view that this process is sufficiently robust and mature. Surprisingly, just over half of the respondents (54 percent) indicated there is a process to notify the board when the organization has exceeded its risk limits. Of the remaining 46 percent of directors, almost one-fourth (11 percent of total respondents) reported that the board has no plans to address this matter. Similarly, 10 percent do not, or have no plans to, ensure that risk management deficiencies are addressed in an appropriate, timely manner. By contrast, 56 percent of directors reported that management has a process to ensure that such deficiencies are remediated appropriately and timely.

Just over 60 percent of respondents noted that the organization assesses extreme high impact/low likelihood events (some of which may be so-called "black swans") periodically, either routinely or on an ad hoc basis. (Such assessments are considered to be different from scenario analysis, which as reported earlier by 51 percent of respondents, is being performed less than annually, on an ad hoc basis or not at all.) Just over half (54 percent) noted that there is a periodic, routine process to review the alignment of strategy, incentives, risk responses and internal controls.

With regard to the reporting of risk, directors of U.S.-based organizations responded more favorably than those of organizations outside the United States, noting that they have more reporting related to how significant risks are being managed and where specific limits are exceeded. In addition, risk reporting at not-for-profit organizations is viewed as less rigorous. As noted with other findings, the results for public companies evidenced a higher percentage of organizations with functioning processes addressing the above matters. For example:

- 68 percent of respondents from public companies (74 percent for public companies with revenue over $1 billion) noted that the organization assesses extreme high impact/low likelihood events (some of which may be so-called "black swans") periodically, either routinely or on an ad hoc basis.

- Almost six of 10 (59 percent) – and 67 percent for public companies with revenue over $1 billion – noted that there is a periodic, routine process to review the alignment of strategy, incentives, risk responses and internal controls.

Protiviti Commentary
Risk management and reporting is not as meaningful when appropriate limits and delegated authorities are not established. For that reason, it should be determined what needs to be escalated to the board as well as when and why. In addition, given the riskiness and volatility of the times, organizations may want to consider allocating more time and resources to understand what it is they don't know by employing techniques that foster out-of-box, big-picture thinking focused on the critical assumptions underlying the corporate strategy. As they do so, they will likely identify opportunities to further enhance and focus the board risk oversight process. For example, earlier we noted that the survey results found that less than 15 percent of respondents noted that the board is fully satisfied with the processes for understanding and challenging assumptions and inherent risks associated with the corporate strategy and monitoring the impact of changes in the environment on the strategy. Implementation of, or enhancements to, these processes may assist the board in addressing two questions that are fundamental to the risk oversight process – "What do we do if the critical assumptions underlying our strategy are no longer valid?" and "How would we know if our assumptions are no longer valid?"

For a Majority of Organizations, a Periodic Board Self-Evaluation of the Risk Oversight Process is Either Not Performed or Can Be Improved

In the survey, 29 percent of respondents indicated that their boards are not self-evaluating the board risk oversight process. Another 34 percent of respondent boards are only doing a self-evaluation on an as-needed basis. Of the remaining respondents, 22 percent are performing at least a rigorous self-evaluation to identify inconsistencies and gaps with expected performance and to suggest improvements, and 15 percent are conducting a self-evaluation routinely.

Please assess the following statement:
The board's risk oversight process is periodically evaluated to determine if the board is achieving its oversight objectives.

Response	Percentage
Performed as a robust and mature activity, with the board satisfied with the supporting process	8%
Performed as a rigorous defined activity with an ongoing process; however, improvements needed	14%
Performed routinely; however, the supporting process is ad hoc	15%
Performed on an as-needed basis, as decided by the board or management	34%
Not performed, but under development	17%
Not performed, with no plans to perform	12%
Total	**100%**

Protiviti Commentary

Over the years, expectations have been established that boards periodically self-evaluate their performance at the full board, committee and individual director levels. Depending on the nature of the business and its risks, one practical approach for self-evaluating the risk oversight process is to incorporate an assessment of it within the board's existing periodic self-assessment process such that the evaluation of the risk oversight process is conducted at least as often as the overall assessment of board effectiveness. If the board were to undertake this approach, we suggest that the nature of the board's self-assessment questions touch on appropriate components of this survey.

Of note, the results suggest that organizations outside the United States believe they are doing a more robust job with self-evaluations of the risk oversight process than U.S.-based organizations. Nearly 60 percent of respondents from organizations outside the United States indicated that there is a process in place to self-evaluate the results of the risk oversight process, whereas less than 40 percent of U.S. respondents stated they have a formal process to do so. In addition, 26 percent of respondents from non-U.S. organizations indicated that this is a mature and robust activity, compared to 3 percent from U.S.-based organizations. Finally, whereas 22 percent of all respondents reported having a formal self-evaluation process, almost twice as many respondents from financial services organizations (41 percent) reported having such a process.

There Are Obstacles to Improving Risk Oversight

While participating board members acknowledged that the risk oversight process is in need of improvement, they also reported on some of the key obstacles to improving it. Providing a list of possible obstacles, we asked participants to list the top three. Of the respondents completing all of the questions in the survey, only nine chose not to list any obstacles, implying there were none. Almost three-fourths of the respondents selected three obstacles. The remaining respondents selected anywhere from one to all of the obstacles. In summary, substantially all of the respondents reported that there were one or more impediments to improving risk oversight. The five obstacles that were selected most often were:

- More pressing needs for the organization
- Don't see the value in pursuing an enterprise risk management process
- Lack of understanding and/or acceptance of enterprise risk management by board members
- Risk management is viewed as a compliance-related activity and/or treated as an appendage to performance management
- Lack of clarity around or inability to agree on the entity's risk philosophy

Following is a tabulation of the results:

What are the top obstacles that inhibit the risk oversight process? (multiple responses permitted)

Response	Percentage
There are more pressing needs, e.g., executing strategy and/or making sure the organization survives	40%
Lack of understanding/acceptance of enterprise risk management by board members	31%
Lack of perceived value of pursuing an ERM approach to risk management	31%
Organizational culture, e.g., risk management is viewed as a compliance activity, treated as an appendage to performance management, etc.	29%
Lack of clarity around/inability to agree on the entity's risk philosophy	28%
Availability of dedicated resources	26%
Disparate systems/processes make an enterprisewide view of risks difficult	19%
Inadequate risk management reporting, methodologies, systems and data	19%
Decentralized organization with highly autonomous business units	17%
Lack of understanding/acceptance of enterprise risk management by management	15%
Difficulty in getting on the same page with management with respect to the entity's risk appetite	14%
Other	8%

While the prior page tabulation provides a view as to the frequency with which each listed obstacle was selected by respondents, it also implies a "good news" message in that, for each individual obstacle, a majority of participants in the survey did not see it as an impediment. The overriding message is twofold: First, almost all respondents reported that there were one or more obstacles inhibiting the risk oversight process in their organizations. Second, the nature of the obstacles faced varies with each organization.

Protiviti Commentary

These obstacles are not surprising. If the risk management process is mired in minutiae rather than focused on the "vital few," the lack of focus will frustrate efforts to improve risk oversight. From the standpoint of making meaningful progress, boards and management may find it beneficial to direct their focus on the assumptions underlying the corporate strategy and ensure that changes in the environment over time do not invalidate those assumptions. This may be a logical starting point for aligning the oversight process with the rhythm of how the business is managed. In effect, through this approach, risk oversight and risk management start at the same place – with understanding the strategy and the critical assumptions underlying the strategy.

Currently, most organizations are operating in a world of scarcity. There are limited resources to get things done as these resources are focused on critical needs of the organization, including, in some cases, survival. If risk management is viewed as an appendage, both management and board members will retain a high level of skepticism regarding implementation because of the lack of tolerance for activities that have limited value add. That is why we are seeing some organizations incorporate risk management within existing management processes rather than leave it as a stand-alone appendage. The perception that enterprise risk management is a compliance activity or serves as an appendage is one that must be overcome.

COSO's thought paper, ***Enterprise Risk Management: Approaches for Getting Started***, is designed to help management and boards address the question of "where to start" and may assist directors in overcoming some of the above obstacles (see www.coso.org).

The SEC Proxy Enhancements Are Raising Awareness of the Need for Risk Oversight

According to the respondents, the three most common impacts of the SEC's 2010 proxy enhancements requiring disclosure of the board risk oversight process are:

- More discussion of risk in concert with strategy and/or operational performance (21 percent)
- Heightened the need to implement effective risk management (20 percent)
- More frequent discussion of risks at board meetings (18 percent)

Protiviti Commentary

The SEC proxy enhancements require greater transparency into how the board operates to provide oversight with respect to the organization's risk management. Because risk oversight is not a robust process at the present time for most organizations and there is a lack of authoritative guidance as to best risk oversight practices, the risk oversight playbook is likely to evolve over time. The SEC proxy enhancements are prompting more interest on the part of directors and executives regarding the enterprise's risks and risk management processes, and may even be part of the reason why public companies show more progress than private companies and not-for-profit organizations.

Protiviti's Recommendations to Improve Board Risk Oversight Effectiveness

As the results of this study demonstrate, there are opportunities to improve the maturity of the board risk oversight process in many organizations today so that it can become more systematic, robust and repeatable. For example, boards may want to consider the following in view of the nature and complexity of their organization's operations and risks and the current state of their risk oversight process:

- Implement a more structured process for monitoring and reporting critical enterprise risks and emerging risks to the board.
- Look for opportunities to enhance the risk reporting process to make it more effective and efficient and increase the regularity of reporting according to the nature of the organization's operations and risk profile.
- Come to an agreement with management on the risk-related matters that need to be escalated to the board, addressing the what, when and why.
- Encourage employment of techniques that foster out-of-box, big-picture thinking focused on the critical assumptions underlying the corporate strategy to assess the strategic risks and uncertainties the enterprise faces.
- At least annually, focus on whether development in the business environment has resulted in changes in the critical assumptions and inherent risks underlying the organization's strategy and the effect of such changes on the organization's business model.
- Implement a more defined and rigorous process supporting the risk appetite dialogue between the board and management, and ensure the results of this dialogue are driven down into the organization in an appropriate manner.
- Incorporate appropriate questions relating to risk oversight in the board's periodic evaluation of board performance effectiveness.

The above practices can be applied to most organizations, irrespective of how the board chooses to organize itself for risk oversight.

About COSO

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a voluntary private-sector organization comprised of the following organizations dedicated to guiding executive management and governance participants towards the establishment of more effective, efficient, and ethical business operations on a global basis. It sponsors and disseminates frameworks and guidance based on in-depth research, analysis, and best practices.

COSO, 2010

American Accounting Association | AICPA | fei | ima | IIA

About Protiviti

Protiviti (www.protiviti.com) is a global business consulting and internal audit firm composed of experts specializing in risk, advisory and transaction services. The firm helps solve problems in finance and transactions, operations, technology, litigation, governance, risk, and compliance. Protiviti's highly trained, results-oriented professionals provide a unique perspective on a wide range of critical business issues for clients in the Americas, Asia-Pacific, Europe and the Middle East.

Protiviti has more than 60 locations worldwide and is a wholly owned subsidiary of Robert Half International Inc. (NYSE symbol: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

protiviti®
Risk & Business Consulting.
Internal Audit.

COSO

Committee of Sponsoring Organizations
of the Treadway Commission

www.coso.org

BOARD RISK OVERSIGHT

A PROGRESS REPORT

Where Boards of Directors Currently Stand in Executing Their Risk Oversight Responsibilities

COSO

Committee of Sponsoring Organizations of the Treadway Commission

www.coso.org