ERM INITIATIVE AT NC STATE UNIVERSITY

Report on the Current State of Enterprise Risk Oversight

Management Accounting Research Conducted on Behalf of the American Institute of CPAs

Mark Beasley, Bruce Branson, Bonnie Hancock

2009

Report on the Current State of Enterprise Risk Oversight

Research Conducted By Faculty

in the ERM Initiative at North Carolina State University

Mark S. Beasley
Deloitte Professor of Enterprise Risk Management
and Director of the ERM Initiative

Bruce C. Branson
Associate Director of the ERM Initiative
and Professor of Accounting

Bonnie V. Hancock
Executive Director of the ERM Initiative
and Executive Lecturer

www.erm.ncsu.edu

March 2009

Current State of Enterprise Risk Oversight

The recent financial crisis is calling into question the robustness of risk oversight processes in all types of organizations, including for-profit, not-for-profit and governmental entities. Boards of directors and senior executives are increasingly being criticized for their failure to effectively manage risks and preserve stakeholder value for the organizations they serve. Expectations are increasing rapidly for boards and senior executives to strengthen their risk oversight processes to preserve and enhance enterprise value.

Calls for strengthening risk oversight have been occurring on an increasing basis over the last several years. For example, the New York Stock Exchange in 2004 adopted governance rules that require audit committees of listed firms to oversee management's risk oversight processes. More recently rating agencies, such as Standard & Poor's, have begun to explicitly evaluate an entity's ERM processes as an input into their credit ratings analysis. Greater expectations also exist among regulators, such as the Federal Reserve (see Appendix for details).

Some organizations are responding to these shifts in expectations by implementing an enterprise-wide approach to risk management frequently referred to as "enterprise risk management" or "ERM." Despite the growing trends towards adopting a more holistic approach to risk oversight, not all organizations are modifying their procedures for identifying, assessing, managing, and communicating risk information to key stakeholders. To better understand the state of ERM practices across a wide range of organizations, we surveyed over 700 entities and asked a series of questions designed to illuminate their enterprise risk oversight process.

This report contains insights on how boards and senior management teams are responding to the challenges of risk oversight in light of the current environment. We explore numerous factors that help shed light upon the current level of risk oversight sophistication, many of the current drivers within organizations that are leading to changes in their risk oversight processes, and some of the impediments to further ERM evolution.

The next page summarizes some of the key findings from this research. The remainder of the report provides additional information about other key findings and related implications for risk oversight.

Key Findings

Below are some of the key findings contained in this report:

- Over 60% of respondents believe that the volume and complexity of risks have changed "Extensively" or "A Great Deal" in the last five years.

- Just over a third of respondents (36%) note that they were caught off guard by an operational surprise "Extensively" or "A Great Deal" in the last five years.

- Over 50% indicate that their risk culture is one that is either "strongly risk averse" or "risk averse."

- Despite these findings, 44% of respondents have no enterprise-wide risk management process in place and have no plans to implement one. An additional 18% without ERM processes in place indicate that they are currently investigating the concept, but have made no decisions about implementing ERM.

- Forty-three percent do not have their business functions establishing or updating assessments of risk exposures on any formal basis. Over 75% indicate that key risks are being communicated merely on an ad hoc basis at management meetings.

- Almost half (47%) admit that they are "Not at All Satisfied" or are "Minimally" satisfied with the nature and extent of reporting of key risk indicators to senior executives regarding the entity's top risk exposures.

- Expectations for improvements in risk oversight may be on the rise. For almost half (45%) of the organizations represented, the board of directors is asking senior executives to increase their involvement in risk oversight.

- Much of the board's focus on strengthening risk oversight is being funneled through the audit committee. For those with audit committees, 12% are asking executives to increase their risk oversight "A Great Deal" and an additional 46% are asking for increased oversight "Extensively."

- For those audit committees formally monitoring risks for the board, 19% only monitor financial risks, 63% monitor operational and compliance risks in addition to financial risks. Only 18% monitor all entity risks, including strategic risks.

- Despite strong interest in improving senior executive leadership in risk oversight, very few organizations (18%) have created a chief risk officer (CRO) position to lead and coordinate the organization's risk oversight processes.

The remainder of this report provides more detailed analysis of other key findings.

Overview of Research Approach

This study was conducted by research faculty who lead the Enterprise Risk Management Initiative (the ERM Initiative) in the College of Management at North Carolina State University (for more information about the ERM Initiative please see http://www.erm.ncsu.edu). The research was conducted as a part of the Management Accounting Research series sponsored by the American Institute of Certified Public Accountants. Data was collected during the fall of 2008 through an online survey instrument electronically sent to members of the AICPA's Business and Industry group who serve in chief financial officer or equivalent positions. In total, we received 701 partially or fully completed surveys.[1] This report summarizes our findings.

Description of Respondents

Respondents completed an online survey with questions that address many of the factors and conditions related to the organization for which the individual is a member of management. They were asked over 40 questions that sought information about various aspects of risk oversight within their organizations.

Because the completion of the survey was voluntary, there is some potential for bias if those choosing to respond differ significantly from those who did not respond. Our study's results may be limited to the extent that such a possibility exists. Also, some respondents provided an answer to selected questions while they omitted others.

A majority of those responding (55%[2]) have the title of chief financial officer (CFO) and an additional 21% bear the title of controller. Others respondents included the head of internal audit (3%), treasurer (2%), and chief risk officer (1%). The remainder represented individuals in various other positions within organizations they serve.

A broad range of industries are represented by the respondents. The most common industry was manufacturing (22%), followed by services (21%), finance, insurance, and real estate (19%), not-for-profit (14%), and wholesale/distribution (9%).

[1] Not all questions were completed by all 701 respondents. In some cases, the questions were not applicable based on their responses to other questions. In other cases, the respondents chose to skip a particular question.
[2] All percentages reported have been rounded to the nearest whole number.

Industry (SIC Codes)	Percentage of Respondents
Manufacturing (SIC 20-39)	22%
Services (SIC 70-89)	21%
Finance, Insurance, Real Estate (SIC 60-67)	19%
Not-for-Profit (SIC N/A)	14%
Wholesale/Distribution (SIC 50-51)	9%
Construction (SIC 15-17)	5%
Retail (SIC 52-59)	5%
Transportation (SIC 40-49)	2%
Agriculture, Forestry, Fishing (SIC 01-09)	2%
Mining (SIC 10-14)	1%

A broad range of organization sizes is included in our survey. Total revenues ranged from $14,950 to $115 billion, with median revenues for the sample of $50 million.

Summary Description of Responses

Many of our questions asked respondents to provide an assessment of various risk management factors and characteristics using an 11-point Likert scale where a score of 1 represents a response reflecting "Not at all" and a score of 11 represents a response reflecting "A Great Deal" or a similar response depending on the nature of the question. [3]

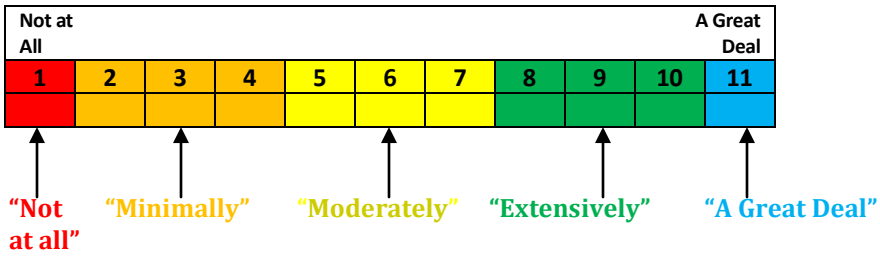
Respondents were asked to *"Place an "X" in one column below"* to reflect their response to many of our questions.

Not at All										A Great Deal
1	2	3	4	5	6	7	8	9	10	11

For purposes of our analysis, we converted responses to one of these five descriptive categories that are mapped to the 11-point Likert scale as follows:

Likert Scale Score	Description of Responses
1	"Not at All"
2, 3, or 4	"Minimally"
5, 6, or 7	"Moderately"
8, 9, or 10	"Extensively"
11	"A Great Deal" unless otherwise described

[3] In some cases, the 11th point response was worded differently from "A Great Deal" given the nature of the question. In those cases, the responses were "Very Mature/Robust," "Very Satisfied," or "Very Closely." We note when those differences occurred as we report the responses in this report.



We use the above descriptive categories in this report to explain responses to specific questions about the state of risk oversight in organizations they serve.

Volume and Complexity of Risks

Many argue that the volume and complexity of risks faced by organizations today are at all-time highs. To get a sense for the extent of risks faced by organizations represented by our respondents, we asked them to describe the extent to which the volume and complexity of risks have increased in the last five years. Sixteen percent noted that the volume and complexity of risks had increased "A Great Deal" over the past five years. An additional 46% responded that the volume and complexity of risks have increased "Extensively" (a Likert score of 8, 9, or 10). Thus, on a combined basis 62% of respondents indicate that the volume and complexity of risks have changed "Extensively" or "A Great Deal" in the last five years. Only 2% responded that the volume and complexity of risks have not changed at all.

	Description of Response				
Question	Not at All	Minimally	Moderately	Extensively	A Great Deal
To what extent has the volume and complexity of risks increased over the past five years?	2%	7%	29%	46%	16%
To what extent has your organization faced an operational surprise in the last five years?	5%	26%	33%	30%	6%

The increased volume and complexity of risks has actually impacted organizations we surveyed in significant ways in the last five years. Just over six percent noted that they have been impacted by an operational surprise by "A Great Deal" in the last five years and an additional 30% of respondents noted that they have been impacted "Extensively" in the last five years. Even though the number of organizations who were caught off-guard by a significant operational surprise in the last five years were less than the number of respondents noting that their risks are changing in volume and complexity, still over one-third of the respondents were impacted "Extensively" or "A Great Deal" by an operational issue. An additional 33% of respondents noted that they were impacted "Moderately" by an operational surprise in the last five years.

Taken together, the above responses indicate that organizations are facing an increasing volume of risks that are also growing in complexity. And for many, the risks are creating significant operational issues not anticipated by management.

Consideration of an Enterprise-Wide Approach to Risk Oversight

While organizations have managed risks for centuries, most have traditionally tackled risk oversight by managing silos or pockets of risks. 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 these silos of risk management come together to share risk oversight information. Unfortunately, for many organizations, risks continue to be managed in isolation with no one obtaining an enterprise view of the portfolio of risks facing an organization.

In recent years there has been an increasing focus on the need for organizations to embrace an enterprise-wide approach to risk management widely known as "enterprise risk management" or "ERM." 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. Boards and senior executives seek to obtain knowledge of these risks with the goal of preserving and enhancing stakeholder value.

To learn more about factors related to the embrace of ERM in organizations we surveyed, we asked a series of questions about the status of ERM implementation in their organizations. Because the term "ERM" is used often, but not necessarily consistently understood, we provided respondents the following definition of enterprise risk management, which is the definition included in the Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) ***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."*
>
> COSO's ***Enterprise Risk Management – Integrated Framework*** (2004)

We also emphasized to respondents key aspects of this definition by noting that ERM is a formal process; that it is enterprise-wide; and that it addresses risks in a portfolio manner, where interactions among risks are considered.

We asked respondents to consider the COSO definition of ERM as they responded to a series of additional questions about the state of ERM in their organizations. We found that

44% of the respondents have no enterprise-wide risk management process in place and 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 have made no decisions to implement an ERM approach to risk oversight at this time. Thus, on a combined basis over 60% of our respondents have no formal enterprise-wide approach to risk oversight. Only a small number (9%) of respondents believe they have a complete formal enterprise-wide risk management process in place. An additional 22% noted that they have partially implemented an ERM process, but not all risk areas are currently being addressed by that process.

Description of the State of ERM in Place	Percentage of Respondents
No enterprise-wide management process in place	44%
Currently investigating concept of enterprise-wide risk management, but have made no decisions yet	18%
No formal enterprise-wide risk management process in place, but have plans to implement one	7%
Partial enterprise-wide risk management process in place (i.e., some, but not all, risk areas addressed)	22%
Complete formal enterprise-wide risk management process in place	9%

In addition, in 74% of the organizations responding to our 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 enterprise-wide risk oversight sophistication in the organizations we surveyed is fairly immature and not based on a top-down, holistic approach to risk management.

Barriers to Enterprise-Wide Risk Oversight

To help us understand potential impediments that organizations face in considering the implementation of an enterprise-wide risk management process, we asked respondents whose organizations have not yet implemented an enterprise-wide risk management process to provide some perspective on that decision. While respondents could indicate more than one impediment, the most common response (in over 53% of the cases) was that they believe risks are monitored in other ways besides ERM. The next most common responses were *"no requests to change our risk management approach"* have been made (29% of respondents with no ERM process in place) and "*too many pressing needs"* keep them from launching an ERM process (noted by 24% of respondents without any existing ERM processes). Eighteen percent of those same respondents also noted a belief that they *"do not see benefits exceeding the costs."*

Respondents provided more depth about some of the primary barriers. Below is a summary of those that the respondents described as "Extensive" and "Very Significant Barriers." Competing priorities and a lack of sufficient resources appear to be the most common barriers to embracing an ERM approach to risk oversight. A lack of perceived value and a lack of visible ERM leadership among boards and senior executives also impact ERM implementation decisions.

	Percentage Believing Barrier is		
Description of Barrier	**"Extensive"**	**"Very Significant"**	**Combined Percentage**
Competing priorities	40%	21%	61%
Insufficient resources	43%	17%	60%
Lack of perceived value	34%	14%	48%
Lack of board or senior executive ERM leadership	28%	10%	38%
Perception ERM adds bureaucracy	26%	11%	37%
Legal or regulatory barriers	4%	1%	5%

General State of Risk Oversight

Ironically, a majority of the respondents indicated that their organization's risk culture is one that is either "strongly risk averse" (10%) or "risk averse" (41%). An additional 35% of our respondents indicated that they are in an organizational culture that is "risk neutral."

Despite growing complexities in the risk environments for organizations in our survey and despite the fact that a majority of the entities are self-described as being "risk averse," the level of risk management sophistication still remains fairly immature for most responding to our survey. When asked to describe the level of maturity of their organization's approach to enterprise risk management process, we found that 32% described their organization's level of functioning ERM processes as "very immature." An additional 35% described their risk culture as "minimally mature." Only 1% responded that their organization's risk culture was "very mature."

	Very Immature	Minimally Mature	Moderately Mature	Extensively Mature	Very Mature/Robust
What is the level of maturity of your organization's approach to a fully functioning ERM process?	32%	35%	24%	8%	1%

The changing complexity and volume of risks facing most organizations, along with growing expectations for improved risk oversight are most likely creating tensions for management teams who overwhelmingly indicate that they have a risk aversion mindset. It is interesting to observe that those tensions are failing to motivate management and boards of those organizations to modify their approach to risk oversight.

Most organizations appear to lack some of the most fundamental methodologies that would allow them to develop a consistent and reliable view of risk. Out of the organizations surveyed, 78% have not formally defined the term "risk" for employees to use as they identify and assess key risks. Forty-three percent of the respondents do not have their business functions establishing or updating assessments of risk exposures on any formal basis. For those that do require business units to establish or update key risk exposures, those assessments are generally only happening on an annual basis (in 29% of the organizations surveyed).

Frequency of Establishing and Updating Key Risk Exposures	Percentage
Not at all	43%
Annually	29%
Semi-annually	5%
Quarterly	12%
Monthly	6%
Weekly	2%
Daily	3%

Most of the risk oversight occurring within organizations we surveyed is fairly unstructured. Over 75% of respondents indicated that key risks are being communicated merely on an *ad hoc* basis at management meetings. In only 29% of the organizations surveyed is management scheduling agenda time to discuss key risks at management meetings and only 10% of the organizations require written risk reports to be submitted annually to management.

Organizations may be beginning to realize the limitations of their current approaches to risk oversight. Almost half (47%) of our respondents admitted that they were "Not at All

Satisfied" or were "Minimally" satisfied with the nature and extent of the reporting of key risk indicators to senior executives regarding the entity's top risk exposures.

Emerging Calls for Enterprise-Wide Risk Oversight

In spite of these findings, our survey results indicate that expectations for improving risk oversight in these organizations are on the rise. Respondents noted that for 9% of the organizations surveyed, the board of directors is asking senior executives to increase their involvement in risk oversight "A Great Deal" and another 36% are asking for increased oversight "Extensively." About 30% indicated "Moderate" board interest in increasing senior executive risk oversight.

These expectations are possibly being prompted by external pressures now being placed on boards, such as those arising from the NYSE governance rules and credit rating agency reviews. In general, boards and audit committees are now 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 the board's interest in strengthening risk oversight is being funneled through the audit committee. For respondents in organizations that have an audit committee function in place, 12% of the audit committees are asking executives to increase their risk oversight "A Great Deal" and an additional 46% are asking for increased oversight "Extensively." Another 28% 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 75% of the full boards and 86% of audit committees are making "Moderate" to "Extensive" to "A Great Deal" of requests for more senior management involvement in risk oversight. Internal audit also appears to be placing additional expectations on executive involvement in risk oversight. For those entities with an internal audit function, 83% of the respondents indicated that internal audit is making "Moderate" to "Extensive" to "A Great Deal" of requests for more senior management involvement in risk oversight. Thus, pressures on senior executives to strengthen risk oversight appear to be significantly emerging among the organizations represented by our survey.

	Percentages		
Extent of Requests for Increased Senior Executive Involvement in Risk Oversight Coming from:	**"Moderate"**	**"Extensive"**	**"A Great Deal"**
Boards of Directors	30%	36%	9%
Audit Committee	28%	46%	12%
Internal Audit	30%	43%	10%

We also asked respondents to describe to what extent external factors (e.g., investors, rating agencies, emerging best practices) are applying pressure on senior executives to provide more information about risks affecting their organizations. While a small percentage (5%) of respondents described "A Great Deal" of external pressure, an additional 27% indicated that external pressures to do so were "Extensive" while another 33% described that pressure as "Moderate." Thus, on a combined basis almost two-thirds of our respondents believe the external pressure to be more transparent about their risk exposures is "Moderate" to "A Great Deal."

That pressure is also reflected by the extent that Chief Executive Officers (CEOs) are asking for increased senior management risk oversight. About 8% of the respondents indicated that the CEO is asking other senior executives to increase their risk oversight "A Great Deal" and another 38% are asking for increases "Extensively." Another 29% are asking at "Moderate" levels for increases in senior executive engagement in ERM.

In addition to board of director engagement in the need to strengthen enterprise-wide risk oversight, other factors are prompting senior executives to consider changes in how they identify, measure, assess, and manage risks. We found that several factors are affecting senior executive focus on risk management activities. First, a desire to better manage unexpected risk events affecting their organizations is providing the strongest incentive for senior executives to focus on risk management activities. Respondents in 28% of the organizations rated that factor as "Extensive" while another 4% rated that as "A Great Deal." Additionally, the question of whether an ERM approach to risk management is becoming an expected "best practice" was rated as "Extensive" for 23% of the respondents while 3% rated that as "A Great Deal." Observing unanticipated risk events affecting competitors was noted as "Extensive" by 16% and as "A Great Deal" by 3% of respondents.

	Percentages		
Incentives for Senior Executives to Increase Focus on Risk Management Activities	**"Extensive"**	**"A Great Deal"**	**Combined**
Unanticipated risk events that have affected organization	28%	4%	32%
Expectation that ERM is "Best Practice"	23%	3%	26%
Unanticipated risk events affecting competitors	16%	3%	19%

It will be interesting to monitor future changes in risk oversight practices given these emerging expectations for improved risk management in organizations today.

Risk Oversight Leadership

Despite strong interest in improving senior executive leadership in risk oversight, very few organizations (18%) have created a chief risk officer (CRO) position to lead and coordinate the organization's risk oversight processes. For the small minority of firms with a chief risk officer position, the individual to whom the CRO most often reports is the CEO (55% of the instances). Interestingly, for 19% of the organizations with a CRO position, the individual reports directly to the board of directors or its audit committee.

Highest Level of Required Reporting by Chief Risk Officer is to the…	Percentage Among Organizations with CROs
Board of Directors or Audit Committee	19%
Chief Executive Officer	55%
Chief Financial Officer	11%
Chief Operating Officer	7%
Other Management Positions	8%

Some organizations choose to coordinate risk oversight using a management committee structure, rather than appointing a chief risk officer. We found that only 22% of the organizations have an internal risk committee (or equivalent) that formally discusses enterprise level risks.

Thus, when combining the 18% of organizations with a chief risk officer position with the 22% of organizations with a risk committee, the majority of the organizations represented by our survey do not appear to have formally designated an individual or executive committee with explicit responsibility for overseeing enterprise-wide risks.

For the relatively few organizations with a formal executive risk oversight committee, those committees met most often (45% of the time) on a quarterly basis, with an additional 25% of the risk committees meeting monthly. The officer most likely to serve on the executive risk committee is the chief financial officer (CFO) who serves on 81% of the risk committees that exist among organizations represented in our survey. The CEO/President serves on 67% of the risk committees while the chief operating officer serves on 51% of the risk committees that exist in organizations we surveyed. In about a third of the organizations surveyed, the general counsel, chief risk officer, and/or the internal audit officer also serve on the risk committee.

Other Senior Executive Involvement in Risk Oversight

Despite the lack of formal designated risk oversight leadership that we observed in the organizations represented by our survey, we recognize that risk oversight leadership may occur even when that leadership has not been formally assigned. To gain a sense for senior executive involvement in risk oversight activities, we asked a series of questions about the nature of their involvement. In 32% of the organizations, our respondents indicated that senior executives are involved "Extensively" or "A Great Deal" in providing ERM leadership in their organizations.

The most common involvement for senior executives was in developing risk responses (i.e., deciding how to respond to identified risks) where 28% of the respondents indicated that senior executives were involved "Extensively" or "A Great Deal" in these activities. Similarly 26% of the respondents indicated that senior executives are also involved "Extensively" or "A Great Deal" in suggesting control activities to ensure risk responses are in place. Twenty-four percent of senior executives are involved "Extensively" or "A Great Deal" in risk identification and about 21% are similarly involved in performing risk assessments in ERM whereby both likelihood and impact of possible risk events are considered. Just over 20 percent are involved in coordinating ERM efforts among various business functions.

While the data reflect some involvement of senior executive leadership in risk oversight, the level of senior executive involvement in ERM leadership is fairly detached in a vast majority of the organizations surveyed. Interestingly, 26% of the respondents noted that there is "No involvement" by senior executives in providing ERM leadership in their organizations.

Board of Director Involvement in Enterprise Risk Oversight

While boards of directors are placing greater expectations on management to improve their risk oversight processes, only 31% of the respondents indicated that their boards have formally assigned risk oversight responsibility to a board committee. For those

boards that have assigned formal risk oversight to a committee, most (55%) are assigning that task to the audit committee. Others are assigning risk oversight to the board's Executive Committee (21%) or to separate Risk Committees (18%). Only a small number (7%) of boards are assigning risk oversight to the Corporate Governance Committee. Of those boards that are delegating risk oversight formally to a committee, 53% have added explicit responsibilities for risk oversight in the respective committee's charter.

We asked respondents to describe the nature of the types of risks formally monitored at the assigned committee level by having respondents indicate which of the following categories of risk are monitored by the committee: Strategic Risks, Financial Risks, Operational Risks, and/or Compliance Risks. Of those organizations that formally assign risk oversight responsibilities to the audit committee, respondents noted that the audit committee was monitoring Financial Risks only in 19% of the cases. Most audit committees with formal risk oversight (63%) also track either Compliance or Operational Risks in addition to Financial Risks. However, only 18% of the respondents at organizations where the audit committee is responsible for formally overseeing risks indicated that those audit committees are formally tracking *all* types of risks, including Strategic Risks. Thus, broad oversight of all types of risks affecting an enterprise does not appear to be a widespread practice among audit committees at this time.

Nature of Risks Monitored by Audit Committees	Percentage of Audit Committees Overseeing These Risks
Financial Risks only	19%
Operational and Compliance Risks in addition to Financial Risks	63%
All Entity Risks, including Strategic, Operational, Compliance, and Financial Risks	18%

Interestingly, while only 21% of the organizations have formally designated risk oversight to the Executive Committee, the focus on Strategic Risks or all entity risks was explicitly noted for 76% of those Executive Committees. For those 18% of organizations that formally delegate risk oversight to a Risk Committee, the risk focus appears to be limited to monitoring Compliance or Operational Risks for most (61%) Risk Committees. Thus, while there may be a growing desire for enterprise-wide risk oversight at the board level, there are differences in focus when the board formally delegates risk oversight to one of its existing committees. Audit Committees tend to focus mostly on Financial Risks, Compliance Risks, or Operational Risks. Risk Committees tend to focus on Compliance and

Operational Risks. Strategic Risks are most likely monitored at the committee level only when risk oversight is delegated to board Executive Committees.

In light of these formal committee assignments for oversight of the enterprise's risk management processes, there is variation as to the frequency of explicit discussion at the full board level about the top risk exposures facing the enterprise. About a quarter of the boards (22%) are explicitly discussing the organization's top risk exposures on an annual basis while another 28% discuss the top risk exposures quarterly. Twelve percent discuss the entity's top risk exposures more than quarterly. Interestingly, 20% of the boards do not formally discuss the organization's top risk exposures. The remaining 18% of the respondents were unsure as to the frequency of board discussions of top risk exposures.

Frequency of Board Discussions about Risk Exposures	Percentages
No Explicit Risk Discussions Occur	20%
Annual basis only	22%
Quarterly basis	28%
More than Quarterly basis	12%
Unsure about extent of board discussions	18%

Impact of Risk Oversight on Strategic Planning and Execution

Many regulators are now calling for meaningful improvements in board-level risk oversight, especially as it relates to strategic risk management. For example:

"…boards of directors and senior management, who bear the responsibility to set strategy and develop and maintain risk management practices, must not only address current difficulties, but must also establish a framework for the inevitable uncertainty that lies ahead."[4]

Randall S. Kroszner, Federal Reserve Governor, October 20, 2008

The current economic crisis has highlighted the increasing importance of embedding ERM processes into strategic planning and execution for all types of organizations. We asked several questions to obtain information about the intersection of risk management and strategy in the organizations we surveyed.

We found that 44% of organizations in our survey currently do no formal assessments of strategic, market, or industry risks and over fifty percent (55%) noted that they do not maintain any risk inventories on a formal basis. Thus, almost half have no processes for

[4] See speech by Federal Reserve Governor Randall S. Kroszner, "Strategic Risk Management in an Interconnected World," October 20, 2008, Baltimore, Maryland (www.federalreserve.gov).

assessing strategic risks. Eighty percent noted that they do not have a standardized process or template for identifying and assessing risks.

Of those that do attempt to assess strategic risks, most do so in a predominantly qualitative (26%) manner or using a blend of qualitative and quantitative assessment tools (20%). Similarly, 45% of those surveyed also fail to conduct any formal assessments of operational/supply chain related risks and 45% fail to formally assess reputational and political risks. If they do identify and maintain risk inventories, over half (55%) have no regular process to update its understanding of key risk exposures.

Frequency of Board Discussions about Risk Exposures	Percentages
Conduct formal assessments of strategic, market, or industry risks	44%
Do not maintain risk inventories on a formal basis	55%
No regular process to update understanding of key risk exposures	55%

The risk areas with greater frequencies of formal assessment appear to be those related to financing/investing/financial reporting risks, information technology risks, and legal/regulatory risks. For financing/investing/financial reporting risks, 65% of respondents indicated that they do some form of assessment, with 34% indicating that their assessments of those risks are mostly quantitative. While the percentages of respondents who formally assess information technology risks and legal/regulatory risks are much higher than the percentage of respondents assessing strategic, operational/supply chain, and reputational/political risks, the assessments of the latter risks tend to be mostly qualitative assessments, not quantitative assessments.

Ironically, while the majority of organizations appear to be fairly unstructured, casual, and somewhat *ad hoc* in how they identify, assess, and monitor key risk exposures, responses to several questions suggest a higher level of confidence that risks are being strategically managed in an effective manner. We asked several questions to gain a sense for how risk exposures are integrated into an organization's strategic planning and execution. Almost half of our respondents believe that existing risk exposures are considered "Extensively" or "A Great Deal" when evaluating possible new strategic initiatives. About a quarter of the respondents believe that their organization has articulated its appetite for or tolerance of risks in the context of strategic planning "Extensively" or "A Great Deal." And, about one-third of the respondents indicate that risk exposures are considered "Extensively" or "A Great Deal" when making capital allocations to functional units.

	Percentages		
Extent that	**"Extensively"**	**"A Great Deal"**	**Combined**
Existing risk exposures are considered when evaluating possible new strategic initiatives	36%	12%	48%
Organization has articulated its appetite for or tolerance of risks in the context of strategic planning	21%	4%	25%
Risk exposures are considered when making capital allocations to functional units	26%	7%	33%

What is uncertain is how respondents arrive at that level of confidence when a majority of their organizations fail to maintain any risk inventories on a formal basis and almost half do no formal assessments of risks, including strategic risks.

Linkage of Risk Oversight and Compensation

The linkage between executive compensation and risk oversight is receiving more attention. The U.S. Treasury Department announced on January 16, 2009 a new certification requirement for the CEOs of financial institutions that receive federal funding under the Troubled Asset Relief Program's (TARP) Capital Purchase Program. For those entities, the CEO must certify within 120 days of receiving the TARP funding that the board's compensation committee has reviewed the senior executive's incentive compensation arrangements with the senior risk officers to ensure that these arrangements do not encourage senior executives to "*take unnecessary and excessive risks that could threaten the value of the financial institution*."

While most organizations will not be directly subject to this certification requirement, there is an emerging expectation that similar discussions should be ongoing in all organizations, not just those in financial services. Shareholder activism and negative media attention are likely to lead to more pressure for boards of directors to consider how existing compensation arrangements might lead to excessive risk-taking on the part of management.

Emerging best practices are attempting to identify ways in which boards can more explicitly embed risk oversight into management's compensation structure in order to provide such incentives. Ultimately, the goal is to link risk oversight capabilities to individual performance assessments to make the relationship of risk and return more

explicit. For enterprise-wide risk oversight to be sustainable for the long term, members of the management team must be incented to embrace this holistic approach to risk oversight. These incentives should be designed to encourage proactive management of risks under their areas of responsibility.

We asked respondents about the extent to which risk management activities are an explicit component of determining management performance compensation. We found that in 37% of the organizations surveyed, risk management is "Not at All" a component of the performance compensation and for another 26% the component is only "Minimally" considered. This may represent an opportunity for significant improvement for many organizations, especially if expectations continue to demand greater linkages of compensation and risk oversight.

Risk Disclosures

While 62% of respondents indicated their belief that the volume and complexity of risks have increased "Extensively" or "A Great Deal" in the past five years and 36% admitted that they have faced a significant operational surprise "Extensively" or "A Great Deal" in the past five years, the extent of external disclosures about risk events has changed very little in that same time period. Sixty-six percent of the organizations responding to our survey noted that the nature of the organization's public disclosure of risks in their financial filings have changed "Not at All." Another 7% have changed their risk disclosures "Minimally" while 13% have made "Moderate" changes. Thus, while organizations admit to being significantly impacted by changes in risk events, very little has been done to change the nature of public disclosures of those risks for key stakeholders.

Summary

Despite the growing pressures for more effective risk oversight that are emerging from the recent financial crisis, the level of enterprise-wide risk oversight across a wide spectrum of organizations appears to be fairly immature. Most organizations have not fully embraced the need for a top-down, enterprise-wide 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.

However, there are emerging trends that 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 focusing on risk issues. When boards are explicitly focusing on risk issues, 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 level of interest in trying to create a more structured approach to risk oversight. Some are responding by creating 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.

Our report highlights several areas that offer opportunities for improvements in risk oversight and the potential danger of an apparent overconfidence in the effectiveness of less formal or *ad hoc* approaches to risk management. Organizations may need to begin with some basic risk management fundamentals to ensure that senior management is explicitly charged with identifying and assessing key risk exposures and that there is a disciplined, structured process that leads to consistent risk identifications and measurements at the top of the organization. As expectations for more effective enterprise-wide risk oversight unfold, it will be interesting to track changes in risk oversight procedures over time.

Appendix - Governance Expectations for Board Risk Oversight

1. Excerpt from the NYSE's *2004 Final Corporate Governance Rules*[5]

Among numerous other responsibilities, duties and responsibilities of the audit committee include:

"(D.) discuss policies with respect to risk assessment and risk management;

Commentary: While it is the job of the CEO and senior management to assess and manage the company's exposure to risk, the audit committee must discuss guidelines and policies to govern the process by which this is handled. The audit committee should discuss the company's major financial risk exposures and the steps management has taken to monitor and control such exposures. The audit committee is not required to be the sole body responsible for risk assessment and management, but, as stated above, the committee must discuss guidelines and policies to govern the process by which risk assessment and management is undertaken. Many companies, particularly financial companies, manage and assess their risk through mechanisms other than the audit committee. The processes these companies have in place should be reviewed in a general manner by the audit committee, but they need not be replaced by the audit committee."

2. Excerpt from Standard & Poor's "Enterprise Risk Management: Standard & Poor's To Apply Enterprise Risk Analysis to Corporate Ratings" [6]

In May 2008, Standard & Poor's issued a document titled, *Standard & Poor's To Apply Enterprise Risk Analysis to Corporate Ratings,* that announces S&P's plan to expand its analysis of ERM processes as part of its credit rating assessments into 17 different industries involving non-financial companies. S&P's goal is to *"... enhance transparency by providing investors and issuers our views of a management team's ability to understand, articulate, and successfully manage risks."* They will include commentary about ERM in their credit assessment reports and those assessments will largely focus on risk-management culture and strategic risk management.

3. Excerpt from Speech by Federal Reserve Governor Randall S. Kroszner – October 20, 2008

"...It is absolutely clear that many financial institutions need to undertake a fundamental review of risk management. They now realize that ignoring risk management in any aspect of the banking business usually creates problems later on. Risk management shortcomings need to be addressed not only to improve the health and viability of individual institutions, but also to maintain stability for the financial system as a whole."[7]

[5] See New York Stock Exchange, *Final Corporate Governance Rules*, 2004 (www.nyse.com).
[6] See Standard & Poor's, *Enterprise Risk Management: Standard & Poor's To Apply Enterprise Risk Analysis to Corporate Ratings*, May 2008, www.standardandpoors.com, New York, NY.
[7] See speech by Federal Reserve Governor Randall S. Kroszner, "Strategic Risk Management in an Interconnected World," October 20, 2008, Baltimore, Maryland (www.federalreserve.gov).

Author Bios

All three authors serve in leadership positions within the Enterprise Risk Management (ERM) Initiative at NC State University (http://www.erm.ncsu.edu) The ERM Initiative provides thought leadership about ERM practices and their integration with strategy and corporate governance. Faculty in the ERM Initiative frequently work with boards of directors and senior management teams helping them link ERM to strategy and governance.

Mark S. Beasley is the Deloitte Professor of Enterprise Risk Management and the Director of the Enterprise Risk Management Initiative in the College of Management at NC State University in Raleigh, North Carolina. He currently serves on the board of the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Bruce C. Branson is a Professor of Accounting and Associate Director of the ERM Initiative at NC State. He teaches financial risk management topics in both the College's undergraduate and graduate programs, where he has received numerous teaching awards.

Bonnie V. Hancock is and Executive Lecturer and Executive Director of the ERM Initiative**.** She came to NC State from Progress Energy, an NYSE listed firm in the utility industry and a Fortune 250 company, where she served as President, Progress Fuels. Prior to that she held the following executive positions at Progress Energy: Senior Vice President, Finance and Information Technology; Vice President, Strategic Planning; Vice President, Accounting and Controller; and Tax Manager.