

2010

*Report on the Current State of
Enterprise Risk Oversight: 2nd Edition*



**Research Conducted in Conjunction with the
American Institute of Certified Public Accountants (AICPA)
Business, Industry, & Government Team
and the
ERM Initiative at North Carolina State University**



Authors:

**Mark Beasley,
Bruce Branson, and
Bonnie Hancock**

ERM Initiative at NC State

www.erm.ncsu.edu

Report on the Current State of Enterprise Risk Oversight – 2nd Edition

**Research Conducted in Conjunction with the
American Institute of Certified Public Accountants (AICPA)
Business, Industry & Government Team
and 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

February 2010

2010 Report on the Current State of Enterprise Risk Oversight

The intense focus on board oversight of risk management processes continues in 2010. The volatile economic environment that persists is generating greater scrutiny of the role of boards and senior executives in the oversight of the multitude of risks their organizations face.

The Securities and Exchange Commission (SEC) announced in December 2009 new proxy disclosure rules that require U.S. publicly traded companies to include in their annual proxy statements information about the board's involvement in risk oversight. In October 2009, the Blue Ribbon Commission of the National Association of Corporate Directors (NACD) issued its report, *Risk Governance: Balancing Risk and Reward*, providing suggestions and practical advice for directors on risk oversight. Similarly, COSO issued in fall 2009 two thought papers, *Effective Enterprise Risk Management: The Role of the Board of Directors* and *Strengthening Enterprise Risk Management for Strategic Advantage*, that highlight the key roles of the board of directors and senior executives in enterprise risk management. Furthermore, legislation has been proposed in Congress that would require boards of public companies to create separate risk committees among other matters.

These recent developments continue the emphasis on strengthening risk oversight that has been building over the last several years. In 2004, the New York Stock Exchange adopted governance rules that require audit committees of listed firms to oversee management's risk oversight processes. In 2008, rating agencies, such as Standard & Poor's, began to explicitly evaluate an entity's ERM processes as an input to their credit ratings analysis. Greater expectations also exist among regulators, such as the Federal Reserve.

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 top-down approach to risk oversight, not all organizations have taken steps to modify their procedures for identifying, assessing, managing, and communicating risk information to key stakeholders.

In March 2009, we issued, in conjunction with the AICPA Business, Industry, & Government Team, our first *Report on the Current State of Enterprise Risk Management*, to provide insight about the current state of enterprise risk management based on fall 2008 survey results from over 700 senior executives representing organizations of various sizes and industries. That report found that while organizations face a significant volume of complex risks, the state of enterprise-wide risk management was relatively immature in late 2008.

Given the continued amount of attention and focus throughout 2009 and early 2010 on the need to strengthen risk oversight from organizations such as the SEC, NACD, COSO, Congress, the Federal Reserve, and the financial press, we partnered again with the AICPA Business, Industry, and Government Team to update our understanding about the current state of enterprise risk management. We surveyed senior executives in December 2009 to ask them a series of questions similar to those we asked in 2008 designed to illuminate their enterprise risk oversight process.

This *2010 Report on the Current State of Enterprise Risk Management – 2nd Edition*, updates our 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 sophistication of risk oversight, 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 two pages summarize 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.

Mark Beasley
Deloitte Professor of ERM
ERM Initiative

Bruce Branson
Associate Director
ERM Initiative

Bonnie Hancock
Executive Director
ERM Initiative

Key Findings

- Over 63% of respondents believe that the volume and complexity of risks have changed “Extensively” or “A Great Deal” in the last five years. This is relatively unchanged from the 62.2% who responded similarly in the 2009 report. Thus, most believe the world of risk is rapidly evolving in complex ways.
- Organizations continue to experience significant operational surprises. Thirty-nine percent of respondents admit they were caught off guard by an operational surprise “Extensively” or “A Great Deal” in the last five years. Another 35% noted that they had been “Moderately” affected by an operational surprise. Together, these findings suggest that weaknesses in existing risk identification and monitoring processes may exist, given that unexpected risk events have significantly affected many organizations.
- About half (47.5%) of respondents self describe the organization’s risk culture as one that is either “strongly risk averse” or “risk averse.” Given their admission of a highly complex and voluminous risk environment and the risk averse nature of the organization’s culture, one might expect these organizations to be moving rapidly towards more robust risk oversight processes.
- Ironically, 48.7% of respondents describe the sophistication of their risk oversight processes as immature to minimally mature. Forty-seven percent do not have their business functions establishing or updating assessments of risk exposures on any formal basis. Almost 70% noted that management does not report the entity’s top risk exposures to the board of directors. These trends are relatively unchanged from those noted in the 2009 report.
- Almost 57% of our respondents have no formal enterprise-wide approach to risk oversight, as compared to 61.8% in our 2009 report with no formal ERM processes in place. Only a small number (11%) of respondents believe they have a complete formal enterprise-wide risk management process in place as compared to 9% in the 2009 report. Thus, there has been only a slight movement towards an ERM approach since our 2009 report.
- Almost half (48%) admit that they are “Not at All Satisfied” or are “Minimally” satisfied with the nature and extent of reporting to senior executives of key risk indicators.

- Very few (15.5%) organizations provide explicit guidelines or measures to business unit leaders on how to assess the probability or potential impact of a risk event. Despite this, 60.5% indicate that they believe risks are being effectively assessed and monitored in other ways besides ERM. This raises the potential for those organizations to have widely varying levels of risk acceptance across business units, and an increased potential for the acceptance of risks beyond an organization's appetite for risk taking.
- Almost half (47.6%) have provided senior executives or key business unit leaders formal training or guidance on risk management in the past two years, with an additional 30.5% providing minimal training or guidance.
- There has been some movement towards delegating senior management leadership over risk oversight. Twenty-three percent have created a chief risk officer position, up from 17.8% in the 2009 report, and 30% have an internal risk committee that formally discusses enterprise level risks, up from 22% noted in the 2009 report.
- Just over half (53%) of organizations surveyed currently do no formal assessments of strategic, market, or industry risks, and 51% noted that they do not maintain any risk inventories on a formal basis. Thus, almost half have no processes for assessing strategic risks. Despite that, about 43% of our respondents believe that existing risk exposures are considered "Extensively" or "A Great Deal" when evaluating possible new strategic initiatives. This raises the question of whether some organizations may be overconfident of their informal processes.
- When boards of directors delegate risk oversight to a board level committee, most (65%) are assigning that task to the audit committee, which is somewhat higher than the 55% of boards assigning risk oversight to the audit committee noted in our 2009 report.
- When risk oversight is assigned to the audit committee, 64% of those audit committees are focusing on financial, operational, or compliance related risks. Only 36% indicate that they also track strategic and/or emerging risks; however, this is up from the 18% in the 2009 report who said the audit committee monitors all entity risks, including strategic risks.
- 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.

The remainder of this report provides more detailed analysis of these and 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 in conjunction with the American Institute of Certified Public Accountants' (AICPA) Business and Industry Group. Data was collected during December 2009 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 senior executive positions. In total, we received 331 partially or fully completed surveys.¹ This report summarizes our findings.

Results are based on responses from 331 executives, mostly including CFOs, representing a variety of industries and firm sizes.

Description of Respondents

Respondents completed an online survey with questions that address many of the factors and conditions related to the entity 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. Most of those questions were included in our first survey that served as the basis for the 2009 report. This approach provides us an opportunity to observe whether we are seeing any shifts in trends in light of more recent developments surrounding the board and senior executive's roles in risk oversight.

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. Furthermore, there is a high concentration of respondents representing financial reporting roles. Possibly there are others leading the risk management effort within their organizations whose views are not captured in the responses we received. Despite these limitations, the results reported herein provide needed insight about the current level of risk oversight maturity and sophistication and highlight many challenges associated with strengthening risk oversight in many different types of organizations.

¹ Not all questions were completed by all 331 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.

A majority of those responding (64.9%) have the title of chief financial officer (CFO) and an additional 18.2% bear the title of controller. Other respondents included the head of internal audit (1.7%), treasurer (1.3%), and chief risk officer (.9%), with the remainder representing numerous other executive positions. The mix of respondents in this year's update is relatively similar to those analyzed in our 2009 report, where 55.1% of the responses were from CFOs, 20.9% were from controllers, while no other title represented more than 3% of our respondents.

A broad range of industries are represented by the respondents. The most common industry was finance, insurance, and real estate (24.6%), followed by not-for-profit (19.3%), manufacturing (18.4%), services (15.8%), and construction (6.1%). The mix of industries is generally consistent with the mix in our 2009 report.

| Industry (SIC Codes) | Percentage of Respondents |
|---|---------------------------|
| Finance, Insurance, Real Estate (SIC 60-67) | 24.6% |
| Not-for-Profit (SIC N/A) | 19.3% |
| Manufacturing (SIC 20-39) | 18.4% |
| Services (SIC 70-89) | 15.8% |
| Construction (SIC 15-17) | 6.1% |
| Wholesale/Distribution (SIC 50-51) | 5.3% |
| Retail (SIC 52-59) | 3.5% |
| Agriculture, Forestry, Fishing (SIC 01-09) | 1.8% |
| Transportation (SIC 40-49) | 1.3% |
| Mining (SIC 10-14) | 1.3% |

A broad range of organization size is included in our survey. Total revenues ranged from a start-up company with no revenues to a company with \$45 billion in revenues, with median revenues for the sample of \$50 million (our sample for the 2009 report also had median revenues of \$50 million).

Summary Description of Responses

Consistent with our first study, 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.²

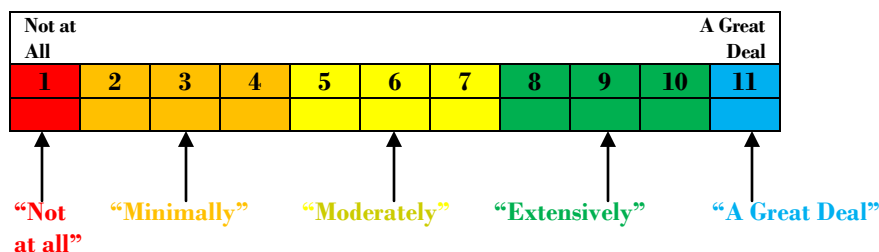
² In some cases, the 11th point response was worded differently from "A Great Deal" given the nature of the question. In those cases, the responses were "Very Mature/Robust," "Very Satisfied," or "Very Closely." We note when those differences occurred as we report the responses in this report.

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, consistent with our treatment in the 2009 report, as follows:

| <u>Likert Scale Score</u> | <u>Description of Responses</u> |
|---------------------------|---|
| 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 |



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

Perceptions about the Nature and Extent of Risks Organizations Face

With the volatile state of the global economy, 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. Almost 17% noted that the volume and complexity of risks had increased “A Great Deal” over the past five years. An additional 47.1% responded that the volume and complexity of risks have increased “Extensively” (a Likert score of 8, 9, or 10). Thus, on a combined basis about 64% of respondents indicate that the volume and complexity of risks have changed “Extensively” or “A Great Deal” in the last five years, which is almost identical to the 62.2% who responded in that manner in the 2009 report. Only 1% responded that the volume and

complexity of risks have not changed at all. Thus, organizational leaders today continue to believe the risks they face are complex and numerous.

Organizational leaders continue to believe the risks they face are complex and numerous, with many translating into actual operational surprises.

Some of those risks have actually translated into significant operational surprises for the organizations represented in our survey. Just over 8% percent noted that they have been impacted by an operational surprise by “A Great Deal” in the last five years and an additional 30.8% of respondents noted that they have been impacted “Extensively” in the last five years. An additional 34.7% of respondents noted that they were impacted “Moderately” by an operational surprise in the last five years. Collectively, this data indicates that the majority of organizations are being impacted by real

risk events that emerged at levels they did not expect, consistent with what we found in our 2009 study.

| Question | Description of Response | | | | |
|--|-------------------------|-----------|------------|-------------|--------------|
| | 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? | 1.0% | 4.8% | 30.5% | 47.1% | 16.6% |
| To what extent has your organization faced an operational surprise in the last five years? | 3.3% | 23.0% | 34.7% | 30.8% | 8.2% |

Relative to our 2009 study, we do not observe a reduction in the rate of operational surprises impacting the organization “Extensively” or “A Great Deal.” These responses indicate that organizations continue to face an increasing volume of risks that are also growing in complexity and that can ultimately create significant operational issues not anticipated by management.

Consideration of an Enterprise-Wide Approach to Risk Oversight

There have been growing calls for more effective enterprise risk oversight at the board and senior management levels in recent years. Many corporate governance reform experts have called for the embrace of an enterprise-wide approach to risk management widely known as “enterprise risk management” or “ERM.” ERM is different from traditional approaches that focus on risk oversight by managing silos or pockets of risks, such as chief technology officers managing the information technology infrastructure while general counsels manage legal and

regulatory risks, absent the additional step of obtaining an enterprise view of the portfolio of risks facing an organization.

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 (as we did for the 2009 report) 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 40.1% of the respondents have no enterprise-wide risk management process in place and have no plans to implement one. An additional 16.7% 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 almost 57% of our respondents have no formal enterprise-wide approach to risk oversight, as compared to 61.8% in our 2009 report with no formal ERM processes in place. Only a small number (11%) of respondents believe they have a



Almost 57% have no formal enterprise-wide approach to risk oversight, as compared to 61.8% in the 2009 report.

complete formal enterprise-wide risk management process in place as compared to 9% in the 2009 report. So, there has been only a slight movement towards an ERM approach since our 2009 report. 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 Currently in Place | Percentage of Respondents |
|--|---------------------------|
| No enterprise-wide management process in place | 40.1% |
| Currently investigating concept of enterprise-wide risk management, but have made no decisions yet | 16.7% |
| No formal enterprise-wide risk management process in place, but have plans to implement one | 10.2% |
| Partial enterprise-wide risk management process in place (i.e., some, but not all, risk areas addressed) | 22.0% |
| Complete formal enterprise-wide risk management process in place | 11.0% |

Ironically, close to a majority of the respondents indicated that their organization’s risk culture is one that is either “strongly risk averse” (7.6%) or “risk averse” (39.9%). An additional 37.6% of our respondents indicated that they are in an organizational culture that is “risk neutral.” These responses indicate that the level of enterprise-wide risk oversight sophistication in the organizations we surveyed continues to be fairly immature and not based on a top-down, holistic approach to risk management.

State of Risk Oversight Maturity

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 13.0% described their organization’s level of functioning ERM processes as “very immature” and an additional 35.7% described their risk culture as “minimally mature.” So, on a combined basis 48.7% self-describe the sophistication of their risk oversight as immature to minimally mature. Only 1.5% responded that their organization’s risk culture was “very mature,” consistent with the 1.6% responding that way in our 2009 report.

The level of enterprise-wide risk oversight sophistication in organizations surveyed continues to be fairly immature, despite the fact that almost half are in a risk culture described as risk averse or strongly risk averse

| | 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? | 13.0% | 35.7% | 35.7% | 14.1% | 1.5% |

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 are risk averse. It is interesting to observe that those tensions do not appear to have motivated 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. For 68.5% 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. Forty-seven percent of the respondents do not have their business functions establishing or updating assessments of risk exposures on any formal basis and 78% have not formally defined the term “risk” for employees to use as they

identify and assess key risks. And, very few (15.5%) organizations provide explicit guidelines or measures to business unit leaders on how to assess the probability or impact of a risk event. Almost half (47.6%) have provided senior executives or key business unit leaders formal training or guidance on risk management in the past two years, with an additional 30.5% providing minimal training or guidance.

For 68.5% of the organizations surveyed, management does not provide a report to the board of directors describing the entity’s top risk exposures.

Most of the risk oversight occurring within organizations we surveyed appears to be fairly unstructured. Over 76% of respondents indicated that key risks are being communicated merely on an *ad hoc* basis at management meetings. Only 29% of the organizations surveyed scheduled agenda time to discuss key risks at management meetings and only 14% of the organizations require written risk reports to be submitted annually to management. These findings are virtually the same as what we found in our 2009 report. 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 26% of the organizations surveyed). These findings are also almost identical to our 2009 report findings.

| Frequency of Establishing and Updating Key Risk Exposures | Percentage |
|---|------------|
| Not at all | 47% |
| Annually | 26% |
| Semi-annually | 7% |
| Quarterly | 13% |
| Monthly | 3% |
| Weekly | 3% |
| Daily | 1% |

Almost half (48%) 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. A similar level of dissatisfaction (47.1%) was observed in our 2009 report.

Impediments to Embracing Enterprise-Wide Risk Oversight

Ironically, the self-described lack of risk management maturity and the observation that many respondents have experienced actual operational surprises in the last five years do not appear to be significant motivators for organizations to make changes in risk management practices. There appear to be several perceived impediments that prevent management from taking action to strengthen their approach to risk oversight.

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 60.5% of the cases) was that they believe “*risks are monitored in other ways besides ERM.*” This strikes us as interesting and paradoxical, given the lack of risk oversight infrastructure highlighted by the data discussed in the prior pages of this report.

The next most common responses were “*no requests to change our risk management approach*” have been made (29.5% of respondents with no ERM process in place) and “*too many pressing needs*” keep them from launching an ERM process (noted by 28.4% of respondents without any existing ERM processes). Just over

There appears to be a strong confidence that existing risk management processes are adequate to address the risks that may arise, even though a large portion of the respondents indicated an overall dissatisfaction with their current approach to managing top risk exposures.

21% of those same respondents also noted a belief that they “do not see benefits exceeding the costs.”

These responses are very much in line with responses noted in our 2009 report. So, there has been little change in what appears to be a barrier to embracing an ERM approach to risk oversight. Instead, there appears to be a strong confidence that existing risk management processes are adequate to address the risks that may arise, even though a large portion of our respondents indicated an overall dissatisfaction with their current approach to managing top risk exposures.

Respondents provided more depth about some of the primary barriers. The table below contains 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. The ordering of these most common barriers is consistent with the ordering of results reported in our 2009 report.


| Description of Barrier | Percentage Believing Barrier is | | |
|--|---------------------------------|--------------------|---------------------|
| | “Extensive” | “Very Significant” | Combined Percentage |
| Competing priorities | 36.8% | 19.2% | 56.0% |
| Insufficient resources | 31.9% | 19.7% | 51.6% |
| Lack of perceived value | 27.7% | 16.4% | 44.1% |
| Perception ERM adds bureaucracy | 25.2% | 13.4% | 38.6% |
| Lack of board or senior executive ERM leadership | 24.0% | 11.8% | 35.8% |
| Legal or regulatory barriers | 2.9% | .4% | 3.3% |

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 may be 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 27% indicated “Moderate” board interest in increasing senior executive risk oversight.

These expectations are possibly being prompted by increasing external pressures now being placed on boards. 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 risk oversight is channeled through the audit committee.

Much of the board’s interest in strengthening risk oversight is being channeled through the audit committee. For respondents in organizations that have an audit committee function in place, 14% of the audit committees are asking executives to increase their risk oversight “A Great Deal” and an additional 44% are asking for increased oversight “Extensively.” Another 26% 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 72% of the full boards and 84% of audit committees are making “Moderate” to “Extensive” to “A Great Deal” of requests for more senior management involvement in risk oversight. These trends are slightly lower, but generally consistent with, what we reported in our 2009 report where 75% of the full board and 92% of the audit committees were making similar requests.

In addition, and perhaps due to the board and audit committee’s interest in strengthened risk oversight, the chief executive officer (CEO) is also calling for increased senior executive involvement in risk oversight. Almost half (43%) of the respondents indicated that the CEO has asked “Extensively” or “A Great Deal” for increased management involvement in risk oversight, which is consistent with what we saw in our 2009 report. An additional, 29% of our respondents indicated that the CEO has expressed “Moderate” levels of requests for increased senior management oversight of risks.

Internal audit also appears to be placing additional expectations on executives regarding risk oversight. For those entities with an internal audit function, 86% 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, as compared to 82.6% reported in our 2009 report. Thus, pressures on senior executives to strengthen risk oversight continue to be present among the organizations represented by our survey.

| Extent of Requests for Increased Senior Executive Involvement in Risk Oversight <u>Coming from:</u> | Percentages | | |
|---|-------------|-------------|----------------|
| | “Moderate” | “Extensive” | “A Great Deal” |
| Boards of Directors | 27% | 36% | 9% |
| Audit Committee | 26% | 44% | 14% |
| Chief Executive Officer | 29% | 38% | 5% |
| Internal Audit | 31% | 47% | 8% |

We also asked respondents to describe to what extent external factors (e.g., investors, rating agencies, emerging best practices) are creating pressure on senior executives to provide more information about risks affecting their organizations. While a small percentage (7%) of respondents described “A Great Deal” of external pressure, an additional 27% indicated that external pressures were “Extensive” and another 31% 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.” This is virtually the same finding as that reported in our 2009 report.

In addition to board engagement in strengthening enterprise-wide risk oversight, several other factors are prompting senior executives to consider changes in how they identify, measure, assess, and manage risks. 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 27% of the organizations rated that factor as “Extensive” while another 5% 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 24% of the respondents while 3% rated that as “A Great Deal.” Observing unanticipated risk events affecting competitors was noted as “Extensive” by 13% and as “A Great Deal” by 2% of respondents. While these incentives exist, our respondents apparently do not sense that these incentives are unduly strong or convincing, given that less than a third of the respondents suggest any of these incentives are “Extensive” or “A Great Deal.” These findings are consistent with our findings in the 2009 report.

| Incentives for Senior Executives to Increase Focus on Risk Management Activities | Percentages | | |
|--|-------------|----------------|----------|
| | “Extensive” | “A Great Deal” | Combined |
| Unanticipated risk events that have affected organization | 27% | 5% | 32% |
| Expectation that ERM is “Best Practice” | 24% | 3% | 27% |
| Unanticipated risk events affecting competitors | 13% | 2% | 15% |

We find the lack of any notable shift from 2009 to 2010 in factors driving senior management focus on strengthening risk oversight to be intriguing, given the current dialogue and focus on calls coming from groups such as the SEC, Federal Reserve, NACD, COSO, and Congress for greater board and executive risk oversight. It will be interesting to monitor future developments in risk oversight practices in light of 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 (23%) have created a chief risk officer (CRO) position to lead and coordinate the organization’s risk oversight processes. This is somewhat higher than the 17.8% of respondents in our 2009 report who indicated their organization has a CRO position. For the minority of firms with a chief risk officer position, the individual to whom the CRO most often reports is the CEO or President (55% of the instances). Interestingly, for 24% of the organizations with a CRO position, the individual reports directly to the board of directors or its audit committee. These lines of reporting are similar to what we noted in our 2009 report.

There has been a slight increase in the percentage of organizations creating a chief risk officer or equivalent position.

| Highest Level of Required Reporting by Chief Risk Officer is to the... | Percentage Among Organizations with CROs |
|--|--|
| Board of Directors or Audit Committee | 24% |
| Chief Executive Officer or President | 55% |
| Chief Financial Officer | 19% |
| Chief Operating Officer | 5% |
| Other Management Positions | 5% |

Some organizations choose to coordinate risk oversight using a management committee structure, rather than appointing a chief risk officer. We found that 30% of the organizations have an internal risk committee (or equivalent) that formally discusses enterprise level risks. This is up from the 22% we reported in 2009.

Thus, when combining the 23% of organizations with a chief risk officer position with the 30% of organizations with a risk committee, about half of the organizations represented by our survey 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 (41% of the time) on a quarterly basis, with an additional 27% 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 85% of the risk committees that exist among organizations represented in our survey. The CEO/President serves on 71% of the risk committees while the chief operating officer serves on 45% of the risk committees. In about a third of the organizations surveyed, the general counsel, chief risk officer, and/or the internal audit officer also sit on the risk committee.

Board of Director Involvement in Enterprise Risk Oversight


Many regulators are now calling for meaningful improvements in board-level risk oversight, especially as it relates to strategic risk management. In fact, the SEC's new proxy disclosure rules focus explicitly on the need for greater disclosure about the board's role in risk oversight. Specifically, effective February 28, 2010, public companies will have to provide information in proxy statements that discusses how the company perceives the role of its board and the relationship of the board and senior management in managing the material risks facing the company. The SEC rules suggest that companies may want to address whether individuals who supervise the day-to-day risk management responsibilities report directly to the board as a whole or to a board committee and/or how the board or committee receives information from such individuals. In addition, legislation has been proposed in

Congress that would require public company boards to create separate risk committees. So, the debate concerning how boards should delegate responsibilities, if at all, continues.

To shed some insight into current practices, we asked respondents to provide information about how their organization's board of directors has delegated risk oversight to board level committees. We found that only 33% of the respondents indicated that their boards have formally assigned risk oversight responsibility to a board committee. The vast majority of our respondents indicate that such delegation has not been formalized by their boards.

For those boards that have assigned formal risk oversight to a committee, most (65%) are assigning that task to the audit committee, which is somewhat higher than the 55% of boards assigning risk oversight to the audit committee noted in our 2009 report. Others are assigning risk oversight to the board's Executive Committee (17%) or to separate Risk Committees (15%). Only a small number (9%) of boards are assigning risk oversight to the Corporate Governance Committee. Of those boards that are delegating risk oversight formally to a committee, 52% have delineated explicit responsibilities for risk oversight in the respective committee's charter.

We asked respondents to describe 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 13% of the cases. Most audit committees with formal risk oversight (51%) also track either Compliance and/or Operational Risks. Interestingly, we found that an additional 36% 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. This is notably higher than what we reported in our 2009 report of 17.9% of audit committees formally tracking all types of risk. Thus, we are seeing a greater percentage of audit committees formally overseeing all types of risks affecting an enterprise than what we observed in 2009; however, a majority of audit committees charged with risk oversight still do not appear to focus on all types of risks, with strategic risks the common omission.



While boards often delegate risk oversight to the audit committee, only a third of those audit committees focus on all types of risks, including strategic risks.

| Nature of Risks Monitored by Audit Committees | Percentage of Audit Committees Overseeing These Risks |
|---|---|
| Financial Risks only | 13% |
| Operational and Compliance Risks in addition to Financial Risks | 51% |
| All Entity Risks, including Strategic, Operational, Compliance, and Financial Risks | 36% |

Interestingly, while only 17% 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 80% of those Executive Committees. For those 15% of organizations that formally delegate risk oversight to a Risk Committee, their focus appears to include all types of risks, including strategic risks for a majority of those committees (55%). The remaining Risk Committees focus only on Operational or Compliance risks or narrower risk silos, such as IT risks or medical risks. Thus, while there may be a growing desire for enterprise-wide risk oversight at the board level, there are substantial 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. Strategic Risks are most likely monitored by either Risk Committees or Executive Committees.


In light of these formal committee assignments for oversight of the enterprise’s risk management processes, we wanted to determine to what extent the full board reviews and discusses in a specific meeting the top risk exposures facing the organizations. Surprisingly, less than half (48.6%) of those responding indicate that the full board has those discussions on a formal basis. In a separate question, we asked about the extent that the board formally discusses the top risk exposures facing the organization when the board discusses the organization’s strategic plan. We found that 10% of the boards do not discuss top risk exposures at all when discussing the organization’s strategy, while another 51% only discuss top risk exposures “Minimally” or “Moderately.” Only 39% indicated those discussions about top risk exposures in the context of strategic planning are “Extensive” or “A Great Deal.”

| | Not at All | Minimally | Moderately | Extensively | A Great Deal |
|--|------------|-----------|------------|-------------|--------------|
| To what extent are the top risk exposures facing the organization formally discussed when the board discusses the organization’s strategic plan? | 10% | 25% | 26% | 28% | 11% |

Impact of Risk Oversight on Strategic Planning and Execution

The current economic crisis has highlighted the increasing importance of more explicit focus on the interrelationship of risk taking and strategy execution. We asked several questions to obtain information about the intersection of risk management and strategy in the organizations we surveyed.

We found that 53% of organizations in our survey currently do no formal assessments of strategic, market, or industry risks and over fifty percent (51%) noted that they do not maintain any risk inventories on a formal basis. Thus, just over half have no processes for assessing strategic risks. Seventy-one percent noted that they do not have a standardized process or template for identifying and assessing risks. These results are consistent with what we found in the 2009 report.



A majority of organizations surveyed do no formal assessments of strategic, market, or industry risks and they do not maintain any risk inventories on a formal basis.

Of those that do attempt to assess strategic risks, most do so in a predominantly qualitative (25%) manner or using a blend of qualitative and quantitative assessment tools (22%). Similarly, 52% of those surveyed also fail to conduct any formal assessments of operational/supply chain

related risks and 50% fail to formally assess reputational and political risks. If they do identify and maintain risk inventories, just under half (48%) have no regular process to update its understanding of key risk exposures.

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, 63% 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. This is what we found in our 2009 report as well.

Even though 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 indicate a high 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. About 43%

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, 30% of the respondents indicate that risk exposures are considered “Extensively” or “A Great Deal” when making capital allocations to functional units.

| Extent that | Percentages | | |
|---|----------------------|-----------------------|-----------------|
| | “Extensively” | “A Great Deal” | Combined |
| Existing risk exposures are considered when evaluating possible new strategic initiatives | 35% | 8% | 43% |
| Organization has articulated its appetite for or tolerance of risks in the context of strategic planning | 21% | 5% | 27% |
| Risk exposures are considered when making capital allocations to functional units | 26% | 4% | 30% |

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, almost half do no formal assessments of risks, including strategic risks, and very few (15.5%) provide any guidance on how business unit leaders should assess risk probabilities or impact.

Linkage of Risk Oversight and Compensation

The linkage between executive compensation and risk oversight is also receiving more attention. In fact, the SEC’s newly issued proxy disclosure rules require public companies to provide information about the relation between compensation policies and risk management and risk-taking incentives that can affect the company’s risks, if those compensation policies and practices create risks that are reasonably likely to have a material adverse effect on the company. Shareholder activism and negative media attention are also creating more pressure for boards of directors to consider how existing compensation arrangements might contribute to excessive risk-taking on the part of management.

Emerging best practices are identifying ways in which boards can more explicitly embed risk oversight into management compensation structures. Ultimately, the goal is to link risk management capabilities to individual performance assessments so that the relationship between risk and return is 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 as well as to enhance timely and transparent sharing of risk knowledge.

We asked respondents about the extent to which risk management activities are an explicit component of determining management performance compensation. We found that in 32% of the organizations surveyed, risk management is “Not at All” a component of the performance compensation and for another 33% the component is only “Minimally” considered. Thus, in almost two-thirds of the organizations surveyed, the extent that risk management activities are an explicit component in determining management performance compensation is non-existent or minimal. The increasing focus on compensation and risk-taking should lead more organizations to consider modifications to their compensation policies and procedures.

Risk Disclosures

While 63.7% 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 39% admitted that they have faced a significant operational surprise “Extensively” or “A Great Deal” over that same time frame, the extent of external disclosures about risk events has changed very little. Sixty-five 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 4.9% have changed their risk disclosures “Minimally” while 14.4% 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.

The extent of external disclosures about risk events have changed very little, despite most believing the volume and complexity of risks have changed “Extensively” or “A Great Deal.”

Summary

Despite the growing demand for more effective risk oversight that has emerged from the recent financial crisis, including new SEC disclosure requirements, the level of enterprise-wide risk oversight across a wide spectrum of organizations remains fairly immature. Most organizations have still not fully embraced the need for a top-down, enterprise-wide perspective of risk oversight. In some organizations ongoing economic challenges have likely occupied management's attention to ensure the organization's survival through the crisis, with less time focused on efforts to strengthen processes to anticipate emerging strategic risks. In others, however, the need for more robust systematic processes surrounding risk oversight may not yet be recognized by management or the board.

Results from this second survey suggest that the approach to risk oversight in some organizations continues to be *ad hoc* and informal, with little recognized need for strengthened approaches to tracking and monitoring key risk exposures, especially emerging risks related to strategy. The results from the survey suggest there may be an urgent need for some entities 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.

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 certain 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 challenge of top-down risk oversight. Management is also demonstrating renewed interest in creating a more structured approach to risk oversight. Some are responding by establishing senior executive risk leadership positions in their organizations. When they do, those positions are reporting directly to the top of the organization, either the CEO or directly to the board.

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 continue to unfold, it will be interesting to track changes in risk oversight procedures over time.

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 an 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. She currently serves on the board of AgFirst Farm Credit Bank.

