

# 2015 Report on the Current State of Enterprise Risk Oversight:

Update on Trends and Opportunities

---



6<sup>th</sup> Edition  
February 2015

**Mark Beasley**  
Deloitte Professor of ERM  
Director, ERM Initiative

**Bruce Branson**  
Associate Director,  
ERM Initiative

**Bonnie Hancock**  
Executive Director,  
ERM Initiative

[www.erm.ncsu.edu](http://www.erm.ncsu.edu)

Research Conducted by the ERM Initiative at North Carolina State University on behalf of the American Institute of CPAs Business, Industry & Government Team



**NC STATE** Poole College of Management  
Enterprise Risk Management Initiative



## Overview of Study

The rapid pace of change and unanticipated disruptions in the global marketplace trigger a seemingly endless barrage of risks that can erode, or even destroy, an organization's business model and brand. Boards of directors and executives face a tremendous challenge in identifying, assessing, and managing risks that may affect – both positively and negatively – the organization's strategic success.

Over the past decade, there have been escalating demands on organizations to strengthen their enterprise-wide risk oversight processes. To obtain an understanding of the current state of enterprise risk oversight among entities of all types and sizes, we have partnered over the past six years with the American Institute of Certified Public Accountants' (AICPA) Business, Industry, and Government Team to survey business leaders about a number of characteristics related to their current enterprise-wide risk management efforts. This is the sixth report that we have published summarizing our research in partnership with the AICPA.

Data was collected during the fall of 2014 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 1,093 completed surveys. This report summarizes our findings and provides a resource for benchmarking an organization's approach to risk oversight against current practices.

This year we observe that the maturity of enterprise-wide risk oversight processes appears to have leveled off with large organizations, public companies, and financial services organizations significantly more mature than other organizations in their enterprise-risk oversight processes. Most notably, organizations continue to struggle to integrate their risk oversight efforts with their strategic planning processes. We believe that significant opportunities remain for organizations to continue to strengthen their approaches to identifying and assessing key risks facing the entity especially as it relates to coordinating these efforts with strategic planning activities.

The following Executive Summary highlights some of the key findings from this research. The remainder of the report provides more detailed 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*

*The ERM Initiative in the Poole College of Management at North Carolina State University provides thought leadership on enterprise risk management (ERM) and its integration with strategic planning and corporate governance, with a focus on helping boards of directors and senior executives gain strategic advantage by strengthening their oversight of all types of risks affecting the enterprise.*

[www.erm.ncsu.edu](http://www.erm.ncsu.edu)



## Key Findings

### State of the Risk Environment

**59%** believe that the volume and complexity of risks have changed “extensively” or “mostly” in the last five years. This holds true for organizations of all sizes and types.

- **65%** admit they were caught off guard by an operational surprise “somewhat” to “extensively” in the last five years. This percentage was even higher for large organizations and public companies.

### State of ERM Maturity

**25%** believe their organization has a “complete formal enterprise-risk management process in place,” and that finding does not differ from the prior year, suggesting that no significant strides in risk oversight maturity were made over the prior year.

- Larger companies, public companies, and financial services organizations are more likely to describe their ERM at that level – about **45%**

**23%** describe their organization’s level of risk management maturity as “Mature” or “Robust.”

- About **one-third** of the larger companies, public companies, and financial services organizations describe their ERM maturity at that level.

**52%** indicate that their organization’s risk management process is “not at all” or “minimally” viewed as a proprietary strategic tool that provides unique competitive advantage, suggesting that many organizations continue to struggle to integrate ERM and strategic planning.

### Calls for Improved Enterprise-Wide Risk Oversight

**68%** indicate that the board of directors is asking “somewhat” to “extensively” for increased senior executive involvement in risk oversight. That is even higher for large companies (**86%**) and public companies (**88%**).

- **65%** of organizations experience “somewhat” to “extensive” pressure from external parties to provide more information about risks.
- Financial services organizations are especially experiencing these external pressures with **79%** experiencing them “somewhat” to “extensively.” These demands are most notably coming from regulators.

### Risk Oversight Leadership

**32%** have designated an individual to serve as the chief risk officer or equivalent.

- Financial services organizations are most likely to designate an individual as CRO or equivalent, with such appointments occurring in **56%** of the firms surveyed.

**45%** have a management-level risk committee

- For most organizations with a risk management committee, the committee meets at least quarterly.



## Risk Identification Techniques

**58%** or more of large companies, public companies, and financial services organizations have formal policy statements regarding enterprise-wide risk management.

**33%** of organizations maintain risk inventories at the enterprise level.

- The largest organizations and public companies are much more likely to maintain inventories of risks at the enterprise level, with **53%** and **57%** doing so, respectively.

**34%** of organizations update their risk inventories annually while an additional **25%** update the inventories semi-annually or quarterly.

**48%** of the largest organizations provide explicit guidelines (e.g., scales) for management to assess an individual risk's probability and impact. That is similar to public companies and financial services organizations. However, only **28%** of the full sample provides that kind of guidance.

## Risk Reporting

**30%** describe their ERM process as systematic, robust, and repeatable with regular reporting of top risks to the board.

- That percentage is higher (**55%**) for large organizations and public companies (**59%**).

**71%** of the largest organizations use written reports to communicate risks information to senior executives (**73%** of public companies). That was true for only **39%** of the full sample.

**27%** use scheduled agenda discussion time at management meetings to communicate key risks to senior executives. That percentage ranges between **35%** and **37%** for large organizations, public companies, and financial services organizations.

- **59%** of the organizations report risks to senior executives via ad hoc discussions at management meetings.

**41%** admit to not being "at all satisfied" or "minimally" satisfied with the nature and extent of the reporting of key risk indicators to senior executives.

## Board of Director Involvement in Enterprise Risk Oversight

**70%** of the boards of directors of the largest organizations and public companies have formally assigned risk oversight responsibilities to a board committee.

- **56%** of large organizations that have assigned oversight responsibility to a board committee delegate responsibility to the audit committee while **29%** delegate to a risk committee.
- **60%** of boards of financial services organizations delegate risk oversight to a board committee and when they do so **41%** delegate to a risk committee and **38%** delegate to an audit committee.

**77%** of large organizations and **84%** of public companies formally report top risk exposures to the board of directors or one of its committees at least annually.

- About **65%** of the largest organizations and public companies report between 5 and 19 risks to the board.



## Integration of Risk Oversight and Strategic Planning

**48%** believe that existing risk exposures are considered “mostly” or “extensively” when evaluating new strategic initiatives. But, **36%** do no formal assessments of emerging strategic, market, or industry risks.

**27%** of the organizations have boards that “mostly” or “extensively” review the top risk exposures facing the organization when the board discusses the organization’s strategic plan.

- This percentage was higher (**45%**) for the largest organizations and financial services organizations (**43%**), although still noticeably low. This seems surprisingly low given the relationship between risk and return.

**33%** of the organizations have “mostly” or “extensively” articulated its appetite for or tolerance of risks in the context of strategic planning.

## Barriers to Progress

**42%** believe that a “barrier” or “significant barrier” to ERM is that it is seen as a “competing priority” to other initiatives at the organization. A similar percentage believes that there are insufficient resources allocated for ERM.

**60%** have not provided or only minimally provided training and guidance on risk management.

The following page identifies a number of high-level insights we gleaned from the analysis of these findings. The detailed findings from this study follow that.



## Key Insights & Considerations

In light of these findings, here are the critical takeaways for board and executive management consideration:

- There appears to be a disconnect between the recognition of today's high risk business environment and the decision to invest more in structured risk oversight.
  - Risk environments are changing rapidly and organizations are being surprised by unexpected risks; however, few organizations have "complete," "mature/robust," or "repeatable" ERM processes in place, even for the largest organizations and public companies.
- Executives indicate that they are receiving increased calls for greater engagement by executives in risk oversight. But, those pressures do not appear to be leading to significant year-over-year change in risk management approaches. Are the pressures sufficient to warrant real change?
- Organizations appear to be using management-level risk committees to lead the risk oversight effort. Most organizations, except for financial services firms, are not creating new management level risk leadership positions, such as chief risk officer or equivalent.
- Most organizations indicate they use written reports to communicate risk information to senior executives and most prepare a formal report of top risk exposures to the board at least annually. However, only about half of them (at best) maintain risk inventories at the enterprise level, which begs the question about the nature of the sources of risk information used to generate the written reports.
- About a third of the organizations update their understanding of risks annually while an additional 24% update that understanding semi-annually or quarterly. More importantly, almost half of the organizations have no formal updating process. Given the nature of the ever-changing business environment, key stakeholders may wonder if the frequency of risk updates is sufficient.
- Most organizations do not provide any guidelines or scales for management to assess risk probabilities or impacts. Thus, the process used to prioritize risks is mostly *ad hoc* and subject to the biases of an individual's personal risk tolerances. Are those potential biases skewing the list of top risks?
- Organizations appear to be struggling to integrate their risk oversight with their strategy development and execution.
  - A majority indicate that their risk management activities are not important strategic tools.
  - Only about one-half of the organizations believe that existing risk exposures are considered when evaluating new strategic initiatives.
  - Boards are not extensively reviewing the top risk exposures when discussing the organization's strategic plan.
  - Most have not articulated the amount of risk they are willing to take in the pursuit of objectives.
  - Executives see risk management as a "competing priority" despite the realities of the risk/return relationship.
- While most view the risk landscape as increasing in complexity over time, the majority of organizations have provided no formal training or guidance on risk management for employees.

As organizations peer into the future, the challenge question for the board of directors, senior executives, and other key stakeholders is *"how confident are we in our organization's ability to effectively identify and navigate the unfolding uncertainties surrounding our current business model and new strategic initiatives?"* Based on key findings in this report, what opportunities exist to enhance the organization's risk management thinking so that both sides of the risk and return relationship are sufficiently and effectively managed?



## Overview of Research Approach

This is the sixth year we have conducted this study to identify trends across a number of organizations related to their enterprise risk management (ERM) processes. This study was conducted by research faculty who lead the Enterprise Risk Management Initiative (the ERM Initiative) in the Poole 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, Industry, and Government Team. Data was collected during the fall of 2014 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 1093 partially or fully completed surveys.<sup>1</sup> This report summarizes our findings.

### Description of Respondents

Respondents completed an online survey consisting of over 40 questions that sought information about various aspects of risk oversight within their organizations. Most of those questions were included in our five previous editions of the surveys conducted each year from 2009 - 2013. This approach provides us an opportunity to observe any shifts in trends in light of more recent developments surrounding 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 bias exists. 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, we believe the results reported herein provide useful insights 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.



Results are based on responses from 1093 executives, mostly serving in financial leadership roles, representing a variety of industries and firm sizes.

A variety of executives serving in financial roles responded to our survey, with 28%<sup>2</sup> having the title of chief financial officer (CFO), 18% serving as controller, and 9% leading internal audit. Other respondents included the chief risk officer (4%) and treasurer (2%), with the remainder representing numerous other executive positions.

### Nature of Organizations Represented

A broad range of industries are represented by the respondents. Consistent with our 2013 survey, the four most common industries responding to the 2014 survey were finance, insurance, and real estate (25%), followed by not-

<sup>1</sup> Not all questions were completed by all 1093 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.

<sup>2</sup> Throughout this report we have rounded the reported percentages to the nearest full percent for ease of discussion.



for-profit (25%), services (19%), and manufacturing (14%). The mix of industries is generally consistent with the mix in all of our previous reports.

Industry (SIC Codes)	Percentage of Respondents
<b>For-Profit Entities:</b>	
Finance, Insurance, Real Estate (SIC 60-67)	25%
Services (SIC 70-89)	19%
Manufacturing (SIC 20-39)	14%
Wholesale/Distribution (SIC 50-51)	4%
Construction (SIC 15-17)	4%
Retail (SIC 52-59)	4%
Transportation (SIC 40-49)	3%
Mining (SIC 10-14)	2%
<b>Not-for-Profit (SIC N/A)</b>	<b>25%</b>

A variety of sizes of organizations are represented by the respondents to the survey. As shown in the table below, two-thirds (66%) of companies that provided data about their financial performance generated revenues up to \$500 million in their most recent fiscal year. An additional 10% generated revenues between \$500 million and \$1 billion while 24% organizations providing revenue data earned revenues in excess of \$1 billion. Almost all (89%) of the organizations are based in the United States.

Range of Revenues in Most Recent Fiscal Year	Percentage of Respondents
\$0 < x ≤ \$10 million	20%
\$10 million < x ≤ \$100 million	30%
\$100 million < x ≤ \$500 million	16%
\$500 million < x ≤ \$1 billion	10%
\$1 billion < x ≤ \$2 billion	6%
\$2 billion < x ≤ \$10 billion	9%
x > \$10 billion	9%

Throughout this report, we highlight selected findings that are notably different for the 243 largest organizations in our sample, which represent those with revenues greater than \$1 billion. Additionally, we also provide selected findings for the 259 publicly-traded companies, 268 financial services entities, and 276 not-for-profit organizations included in our sample.





## State of Risk Environment

Many argue that the volume and complexity of risks faced by organizations today continue to evolve at a rapid pace, creating huge challenges for management and boards in their oversight of the most important risks. To get a sense for the extent of risks faced by organizations represented by our respondents, we asked them to describe how the volume and complexity of risks have increased in the last five years. Twenty-one percent noted that the volume and complexity of risks have increased “extensively” over the past five years, with an additional 38% responding that the volume and complexity of risks have increased “mostly.” Thus, on a combined basis, 59% of respondents indicate that the volume and complexity of risks have changed “mostly” or “extensively” in the last five years, which is in line with what participants in prior years noted: 57% in the 2013 report, 62% in the 2012 report, 55% in the 2011 report, 64% in the 2010 report and 62% in the 2009 report). Only 2% responded that the volume and complexity of risks have not changed at all.

The majority of respondents believe the volume and complexity of risks have increased “mostly” or “extensively” in the past five years, and that finding is consistent across various types of organizations.

We separately analyzed responses to this question for various subgroups of respondents. The percentage of respondents from the largest organizations (those with revenues in excess of \$1 billion) who believe the volume and complexity had increased “extensively” or “mostly” was higher (at 71%) than the full sample. Similarly, public company respondents also believe the volume and complexity has increased notably with 30% responding with “extensively” and 42% responding “mostly” for a combined percentage of 72%. Similar results were noted for financial services entities where 68% described the change in volume and complexity of risks as “mostly” or “extensively.” In summary, most leaders, regardless of type of organization, continue to believe the risks they face are complex and numerous.

Question	Description of Response (Full Sample)				
	Not at All	Minimally	Somewhat	Mostly	Extensively
To what extent has the volume and complexity of risks increased over the past five years?	2%	7%	32%	38%	21%

Some risks have actually translated into significant operational surprises for the organizations represented in our survey. About 9% noted that they have been affected by an operational surprise “extensively” within the last five years and an additional 23% of respondents noted that they have been affected “mostly” in that same time period. An additional 33% responded “somewhat” to this question. Collectively, this data indicates that the majority of organizations (65%) are being affected by real risk events that have emerged, consistent with what we found in our prior studies. The rate is even higher for large organizations and publicly-traded entities, with three-fourths of those responding as “somewhat,” “mostly,” or “extensively.” The reality is that all organizations are dealing with unexpected risks. Just over two-thirds of the financial services entities and not-for-profit organizations in our sample responded with “somewhat” or higher to this question.



Question	Description of Response (Full Sample)				
	Not at All	Minimally	Somewhat	Mostly	Extensively
To what extent has your organization faced an operational surprise in the last five years?	6%	29%	33%	23%	9%

Relative to our earlier studies, we do not observe a notable reduction in the rate of operational surprises affecting organizations “mostly” or “extensively.” The responses to questions about the nature and extent of risks organizations face indicate that executives are experiencing a noticeably high volume of risks that are also growing in complexity, which ultimately results in significant unanticipated operational issues. The reality that unexpected risks and uncertainties occur and continue to “surprise” organizational leaders suggests that opportunities to improve risk management techniques still exist for most organizations.



## State of ERM Maturity

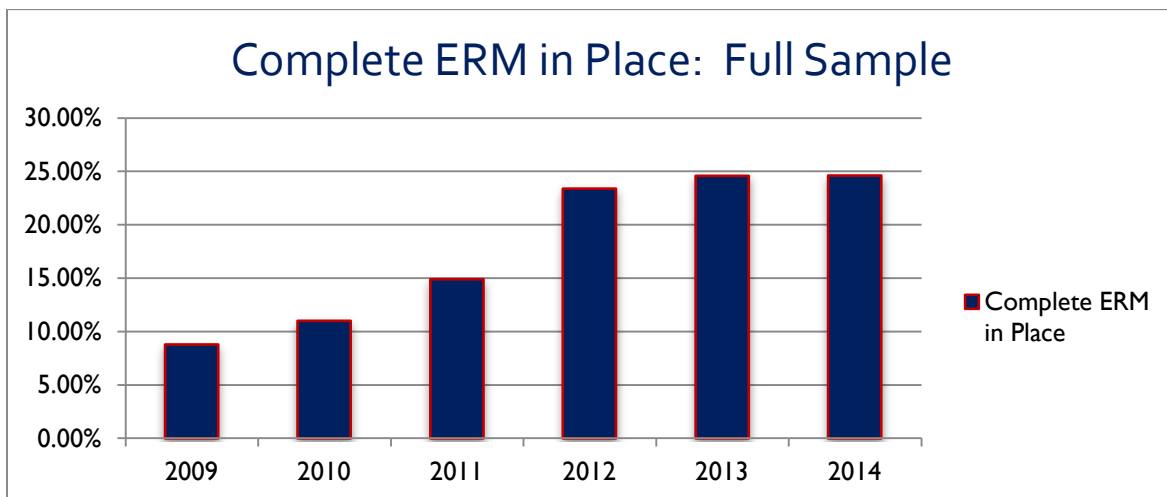
There have been growing calls for more effective enterprise risk oversight at the board and senior management levels in recent years. Many corporate governance reform experts have called for the adoption of a holistic approach to risk management widely known as “enterprise risk management” or “ERM.” ERM is different from traditional approaches that focus on risk oversight by managing silos or distinct pockets of risks. ERM emphasizes a top-down, enterprise-wide view of the inventory of key risk exposures potentially affecting an entity’s ability to achieve its objectives. See Appendix A for more information about the concept of ERM.

### Current State of ERM

To obtain a sense for the current state of ERM maturity, we asked survey participants to respond to a number of questions to help us get a sense for the current level of risk oversight in organizations surveyed. One of the questions asked them to select from the following the best description of the state of their ERM currently in place:

- No enterprise-wide process in place
- Currently investigation concept of enterprise-wide risk management, but have made no decisions yet
- No formal enterprise-wide risk management process in place, but have plans to implement one
- Partial enterprise-wide risk management process in place (i.e., some, but not all, risk areas addressed)
- Complete formal enterprise-wide risk management process in place

One of the more notable observations is that there appears to be a leveling off of the percentage of organizations in the full sample that believe they have a “complete formal enterprise-wide risk management process in place.” As illustrated by the chart below, there does not appear to be an increase over time in the number of organizations that believe their ERM is complete.



The above chart shows an increase from 2009 through 2012 with a leveling off in 2013 and 2014 in the percentage of organizations that claim they have a “complete formal enterprise-wide risk management process in place.” In our 2009 report, only 9% of organizations claimed to have complete ERM processes in place; however, in 2014 the percentage is just below 25% for the full sample. That suggests that there continues to be significant opportunity



for improvement in most organizations, given that three-fourths of organizations surveyed cannot yet claim they have “complete ERM in place.” The adoption of ERM is greatest for larger companies and public companies.

Description of the State of ERM Currently in Place	Percentage of Respondents				
	Full Sample	Largest Organizations (Revenues >\$1B)	Public Companies	Financial Services	Not-For-Profit Organizations
No enterprise-wide management process in place	24%	7%	7%	13%	26%
Currently investigating concept of enterprise-wide risk management, but have made no decisions yet	11%	5%	5%	7%	12%
No formal enterprise-wide risk management process in place, but have plans to implement one	10%	5%	3%	5%	13%
Partial enterprise-wide risk management process in place (i.e., some, but not all, risk areas addressed)	30%	39%	37%	33%	30%
Complete formal enterprise-wide risk management process in place	25%	44%	48%	42%	19%

As seen in the last row of the chart above, 44% of the largest companies in our sample and 48% of public companies in our sample claim to have complete formal enterprise-wide risk management processes in place. This is slightly lower than in 2013 when 56% of the largest organizations and 52% of public companies reported they have complete, formal ERM processes in place. These findings suggest that ERM is of greater significance and importance, especially in the largest organizations and those that are public companies.

There continues to be noticeable room for improvement. For the full sample, we found that just under one-fourth (24%) of the respondents have no enterprise-wide risk management process in place. An additional 11% 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, 35% of respondents have no formal enterprise-wide approach to risk oversight and are currently making no plans to consider this form of risk oversight.

The variation in results highlights that the level of ERM maturity can differ greatly across organizations of various sizes and types. While variations exist, the results also reveal that there are a substantial number of firms in all categories that have no ERM processes or are just beginning to investigate the need for those processes.





## State of ERM Maturity

We also asked respondents to provide their assessment of the overall level of their organization’s risk management maturity using a scale that ranges from “very immature” to “robust.” We found that the level of sophistication of underlying risk management processes still remains fairly immature for most responding to our survey. When asked to describe the level of maturity of their organization’s approach to risk oversight, we found that 19% described their organization’s level of functioning ERM processes as “very immature” and an additional 23% described their risk oversight as “developing.” So, on a combined basis 42% self-describe the sophistication of their risk oversight as immature to developing (this is even slightly lower than the 45% reported in our 2013 study). Only 4% responded that their organization’s risk oversight was “robust,” consistent with responses noted in all five of our prior reports.

What is the level of maturity of your organization’s risk management oversight?	Very Immature	Developing	Evolving	Mature	Robust
Full Sample	19%	23%	35%	19%	4%
Largest Organizations	8%	15%	41%	25%	11%
Public Companies	8%	14%	39%	30%	9%
Financial Services	6%	20%	40%	25%	9%
Not-for-Profit Organizations	24%	25%	34%	15%	2%

In general, the largest organizations, public companies, and financial services entities believe their approach to ERM is more mature relative to the full sample. As shown in the table above, 23% of the full sample respondents describe their organization’s approach to ERM as either “mature” or “robust.” In contrast, 36% of the largest organizations, 39% of the public companies, and 34% of financial services entities indicate their ERM approaches are either “mature” or “robust.” In contrast, only 17% of not-for-profit organizations believe their level of risk management oversight is “mature” or “robust.”

While the level of risk oversight maturity is higher for these subsets of organizations than the full sample and the numbers improved compared to previous years’ results, it is important to note that a significant percentage of these subsets of organizations still do not describe their approaches to ERM as being “mature” or “robust.” When you consider the results concerning the changing complexity and volume of risks facing most organizations, along with growing expectations for improved risk oversight, opportunities remain for all types of organizations to increase the level of their enterprise-wide risk management maturity.

Most organizations describe the level of ERM maturity as very immature to evolving. Few describe their processes as robust.

## ERM as Strategic Tool

Responses to the question about the extent respondents believe the organization’s risk management process is a proprietary strategic tool that provides unique competitive advantage provide insight about how risk management is viewed in those organizations. Just over half (52%) responded to that question by indicating “not



at all” or “minimally.” Interestingly, the assessment of the strategic value of the organization’s risk management process was relatively low and not significantly different for the largest organizations, public companies, and financial services organizations. Thus, there may be a lack of understanding of how an effective ERM process can be informative to management as they execute their strategic plan, and/or the organization has not developed its process well enough to consider it a proprietary strategic tool.

	Not at All	Minimally	Somewhat	Mostly	Extensively
To what extent do you believe the organization’s risk management process is a proprietary strategic tool that provides unique competitive advantage?	30%	22%	28%	15%	5%



## Calls for Improved Enterprise-Wide Risk Oversight

A majority of the respondents in the full sample indicated that their organization's risk culture is one that is either "strongly risk averse" (12%) or "risk averse" (45%). An additional 31% of our respondents indicated that they are in an organizational culture that is "risk neutral." Thus, it is somewhat surprising to see the overall lack of ERM maturity for the full sample given their description of organizational appetite for risk-taking.

Sixty percent of the largest organizations, public companies, and financial services companies indicated their risk culture is "strongly risk averse" or "risk averse." Perhaps the relatively lower appetite for risk taking in those organizations is one of the drivers for more advanced ERM processes as compared to the full sample.

Ironically, 62% of not-for-profit organizations express their risk culture as "strongly risk averse" or "risk averse;" however, those organizations appear to be the least mature in their enterprise-wide risk oversight processes.

Our survey results indicate that board of director expectations for improving risk oversight in these organizations is strong, especially for the largest organizations, public companies, and financial services entities. Respondents noted that for 14% of the organizations surveyed, the board of directors is asking senior executives to increase their involvement in risk oversight "extensively," another 27% of the organizations report "mostly," and an additional 27% have boards that are asking for increased oversight "somewhat." Board expectations for increased senior executive involvement in risk oversight is most dramatic for the largest organizations, public companies, and financial services organizations, as shown in the table below. Requests from the board of directors for increased risk oversight are a little less frequent for not-for-profit organizations.

Extent to which the board of directors is asking for increased senior executive involvement in risk oversight	Percentage of Respondents				
	Full Sample	Largest Organizations (Revenues >\$1B)	Public Companies	Financial Services	Not-for-Profit Organizations
"Extensively"	14%	26%	25%	19%	11%
"Mostly"	27%	34%	40%	29%	24%
"Somewhat"	27%	26%	23%	27%	33%
Combined	68%	86%	88%	75%	68%

These expectations are possibly being prompted by increasing external pressures that continue to be placed on boards. In response to these expectations, boards and audit committees may be challenging senior executives about existing approaches to risk oversight and demanding more information about the organization's top risk exposures.

In addition, and perhaps due to the board's interest in strengthened risk oversight, the chief executive officer (CEO) is also calling for increased senior executive involvement in risk oversight. Over 40% of the respondents indicated that the CEO has asked "mostly" or "extensively" for increased management involvement in risk oversight, which is almost identical to what we saw in our 2013 and 2012 reports. An additional 28% of our respondents indicated that the CEO has expressed "somewhat" of a request for increased senior management oversight of risks.



We also asked respondents to describe to what extent external factors (e.g., investors, ratings agencies, emerging best practices) are creating pressures on senior executives to provide more information about risks affecting their organizations. As illustrated in the table below, while a small percentage (13%) of respondents described external pressures as “extensive,” an additional 22% indicated that external pressures were “mostly” and another 30% described that pressure as “somewhat.” Thus, on a combined basis well over half (65%) of our respondents believe the external pressure to be more transparent about their risk exposures is “somewhat” to “extensive.” That result is up somewhat from the similar combined percentage of 58% noted in our 2013 report.

Most executives note there is “somewhat” to “extensive” external pressure to provide more information about risks.

External pressures are notably stronger for financial services entities, likely from regulators who are becoming more vocal proponents of ERM in banks. These organizations perceived the external pressures to provide more information about risks facing the organization to be much greater than the overall sample of firms.

Percentage of Respondents					
Extent that external parties are applying pressure on senior executives to provide more information about risks affecting the organization	Full Sample	Largest Organizations (Revenues >\$1B)	Public Companies	Financial Services	Not-for-Profit Organizations
“Extensively”	13%	21%	21%	25%	11%
“Mostly”	22%	27%	30%	28%	17%
“Somewhat”	30%	28%	28%	25%	37%
Combined	65%	76%	79%	78%	65%

Several other factors are prompting senior executives to consider changes in how they identify, assess, and manage risks. For the overall sample, respondents noted that regulator demands, emerging corporate governance requirements and a desire to better anticipate unexpected risk events are the three most frequently cited factors for increasing senior executive involvement. However, as illustrated by the table on the next page, regulator demands seem to be putting even greater pressure on senior executives in financial services organizations. In contrast, the strongest factor for increased risk oversight in the largest organizations and public companies is coming from the board of directors and the related emerging corporate governance requirements. Not-for-profit organizations are also experiencing pressure to increase senior executive focus on risk management activities, although to a lesser extent than other organizations.





Percentage of Respondents  
Selecting “Mostly” or “Extensively”

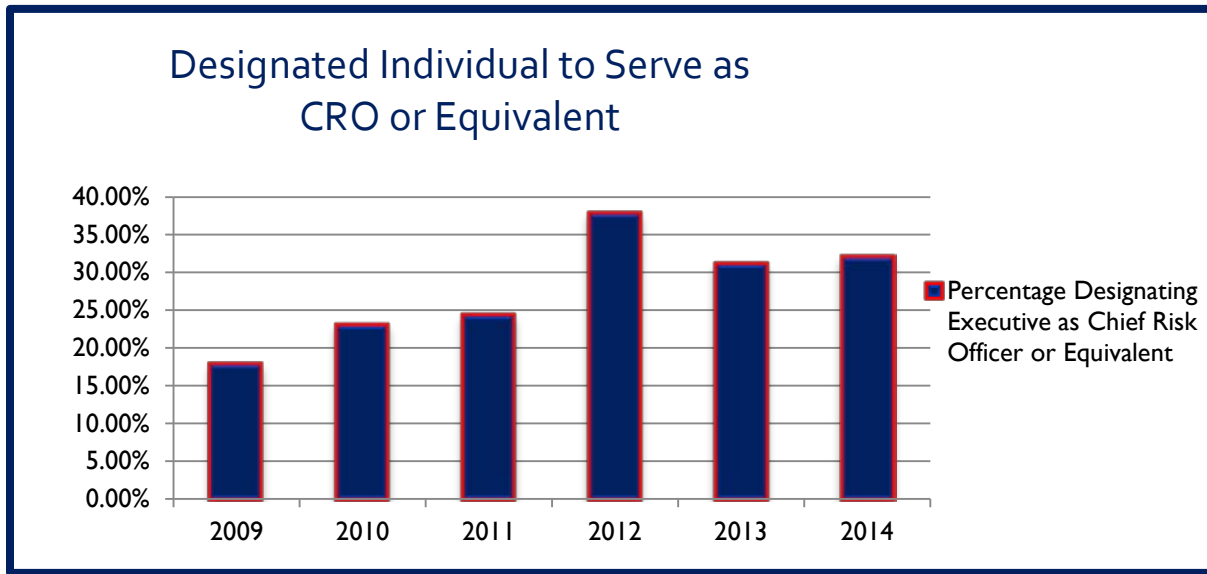
Factors “Mostly” or “Extensively” Leading to Increased Senior Executive Focus on Risk Management Activities	Full Sample	Largest Organizations (Revenues >\$1B)	Public Companies	Financial Services	Not-for-Profit Organizations
Regulator Demands	33%	47%	49%	63%	25%
Unanticipated risk events affecting organization	32%	45%	44%	35%	30%
Emerging best practice expectations	33%	39%	39%	50%	34%
Emerging corporate governance requirements	32%	49%	50%	51%	25%
Board of Director requests	31%	51%	48%	31%	26%

Corporate governance trends, regulatory demands, and board of directors are all placing pressure on executives to engage more in risk oversight.



## Risk Oversight Leadership

While in the initial years of our surveys, we found an increasing percentage of firms formally designating an individual to serve as the Chief Risk Officer (CRO) or equivalent senior risk executive, it appears that the trend has stalled. As illustrated by the bar chart below, 32% of organizations responding indicated that they have made that kind of designation, compared to the 31% reported in 2013, 38% reported in 2012, 24% reported in 2011, 23% reported in 2010, and 18% reported in 2009.



Financial services organizations are more likely to have designated an individual to serve as CRO or equivalent, with more than half of those organizations doing so. A good number of the largest organizations and public companies have also pinpointed individuals to serve in those capacities.

	Percentage of Respondents				
	Full Sample	Largest Organizations (Revenues >\$1B)	Public Companies	Financial Services	Not-For-Profit Organizations
Percentage designating individual to serve as CRO or equivalent	32%	49%	50%	56%	22%

For firms with a chief risk officer position, the individual to whom the CRO most often reports is the CEO or President (46% of the instances for the full sample). Interestingly, for 32% of the organizations with a CRO position, the individual reports formally to the board of directors or its audit committee while an additional 13% report to the chief financial officer. These lines of reporting are similar to what we noted in our prior year reports.

When you examine the largest organizations, public companies, and financial services entities separately, there are some notable differences

Financial services entities are more likely to appoint individuals to serve as Chief Risk Officer (CRO) or equivalent than other organizations.



as shown in the table below. Direct reporting to the CEO and/or President is most common for financial services firms and not-for-profit organizations.

To Whom Does the CRO Formally Report?	Percentage of Respondents				
	Full Sample	Largest Organizations (Revenues >\$1B)	Public Companies	Financial Services	Not-for-Profit Organizations
Board of Directors or Committee of the Board	32%	28%	34%	32%	18%
Chief Executive Officer or President	46%	44%	45%	52%	43%
Chief Financial Officer	13%	18%	13%	10%	21%

Similar to our observation that about one-third (32%) of organizations are designating an executive to lead the risk oversight function (either as CRO or equivalent) in 2014, we also observed that a number of organizations have a management-level risk committee or equivalent. For 2014, 45% of the full sample has a risk committee as compared to 43% in 2013, 49% in 2012, 35% in 2011, 30% in 2010, and 22% in 2009.



The presence of an internal risk committee was noticeably more likely to be present in the largest organizations, public companies, and financial services entities where 68%, 70%, and 66%, respectively, of those organizations had an internal risk committee. These findings are, again, about the same as what we observed in our 2013 report where 70% of the largest organizations, 63% of public companies, and 63% of financial services organizations had management-level risk committees.



For the organizations with a formal executive risk oversight committee, those committees met most often (43% of the time) on a quarterly basis, with an additional 37% of the risk committees meeting monthly. These results did not differ notably for the subsets of largest organizations, public companies, or financial services entities.

The officer most likely to serve on the executive risk committee is the chief financial officer (CFO) who serves on 78% of the risk committees that exist among organizations represented in our survey. The CEO/President serves on 64% of the risk committees while the chief operating officer serves on 54% of the risk committees. In about 40% of the organizations surveyed, the general counsel and the internal audit officer also sit on the risk committee along with other executives from different positions.

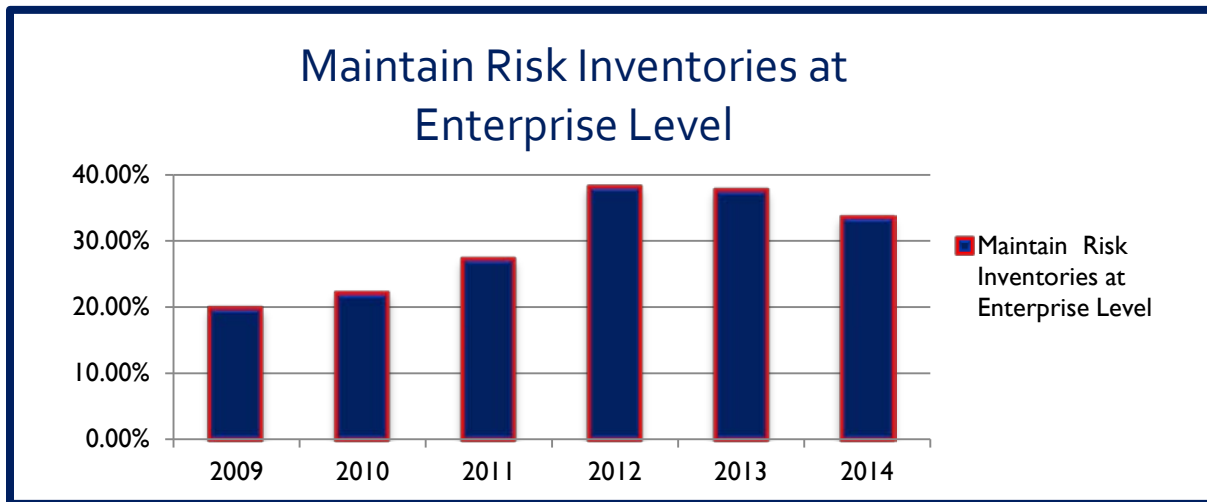


## Risk Identification Techniques

More than half of the organizations in the full sample (65%) do not have a formal policy statement regarding its enterprise-wide approach to risk management. The presence of a formal policy is more common in the largest organizations (58%), public companies (60%), and financial services entities (60%). Not-for-profit organizations are least likely to have a formal policy in place.

	Percentage of Respondents				
	Full Sample	Largest Organizations (Revenues >\$1B)	Public Companies	Financial Services	Not-For-Profit Organizations
Has formal policy statement regarding enterprise-wide approach to risk management	35%	58%	60%	60%	22%

The number of organizations that maintain inventories of risks at the enterprise level remained practically the same over the last year, as illustrated by the bar graph below. Despite that, the percentage has increased significantly when looking at the last five years. While only 20% of organizations did so in 2009, by 2014 one-third of organizations claim to be maintaining an inventory of risks at the enterprise level.



A greater percentage of large organizations, public companies, and financial services firms maintain risk inventories at the enterprise level as shown on the next page. Fewer not-for-profit organizations do so.



	Percentage of Respondents				
	Full Sample	Largest Organizations (Revenues >\$1B)	Public Companies	Financial Services	Not-For-Profit Organizations
Percentage that maintain risk inventories at enterprise level	33%	53%	57%	47%	25%

Just over one-third of the full sample has formally defined the meaning of the term “risk” for employees to use as they identify and assess key risks. When they do so, about a third focus their definition on “downside” risks (threats to the organization) and about one-fourth focus on both the “upside” and “downside” of risk.

A large majority of the full sample *do not* provide explicit guidelines or measures to business unit leaders on how to assess the probability and impact of a risk event (72% and 71%, respectively). We found similar results for not-for-profit organizations. However, consistent with 2013 about half of the largest organizations and public companies provide explicit guidelines or measures to business unit leaders for them to use when assessing risk probabilities and impact. The largest organizations are the most likely to provide this guidance. In 2014, 48% and 49% provide guidelines for assessing risk probabilities and impact, respectively.

	Percentage of Respondents				
	Full Sample	Largest Organizations (Revenues >\$1B)	Public Companies	Financial Services	Not-For-Profit Organizations
Provide explicit guidelines to assess risk					
- Probability	28%	48%	46%	43%	19%
- Impact	29%	49%	47%	42%	17%

We also asked whether organizations go through a dedicated process to update their key risk inventories. As shown in the table below, there is substantial variation as to whether they go through an update process. But, when they do update their risk inventories, it is generally done annually, although a noticeable percentage of organizations update their risk inventories quarterly. Not-for-profit organizations are less likely to be going through a process to update their risk inventories.



Frequency of Going Through Process to Update Key Risk Inventories	Percentage of Respondents				
	Full Sample	Largest Organizations (Revenues >\$1B)	Public Companies	Financial Services	Not-for-Profit Organizations
Not at all	33%	12%	10%	18%	43%
Annually	34%	39%	36%	38%	36%
Semi-Annually	10%	12%	14%	10%	9%
Quarterly	15%	25%	29%	22%	6%
Monthly, Weekly, or Daily	8%	12%	11%	12%	6%

Over two-thirds of the large organizations (68%) and public companies (69%) have a standardized process or template for identifying and assessing risks, while 62% of the financial services organizations have those kinds of procedures in place. In contrast, only 33% of not-for-profit organizations structure their risk identification and assessment processes in that manner.



## Risk Reporting

We asked respondents about their current stage of risk management processes and reporting procedures. Just under half (43%) either have no structured process for identifying and reporting top risk exposures to the board or they track risks by silos with minimal reporting of aggregate risk exposures to the board. An additional 27% describe their risk management processes as informal and unstructured with *ad hoc* reporting of aggregate risk exposures to the board.

Interestingly, however, just under one-third (30%) of the full sample believe their enterprise risk oversight processes are systematic, robust, and repeatable with regular reporting of top risk exposures to the board. This percentage is slightly higher than the results reported in our 2013 report (26%).

Percentage who describe their ERM implementation as	Percentage of Respondents				
	Full Sample	Largest Organizations (Revenues >\$1B)	Public Companies	Financial Services	Not-For-Profit Organizations
"Our process is systematic, robust, and repeatable with regular reporting of top risk exposures to the board."	30%	55%	59%	49%	22%

Thus, while a noticeable majority of organizations do not claim to have systematic, robust, and repeatable ERM processes with regular reporting to the board, the trends suggest that more organizations are moving in that direction over time. As demonstrated by the data in the table above, a noticeably higher percentage of large organizations, public companies, and financial services organizations believe they have a systematic, robust, and repeatable ERM process.

There is notable variation across organizations of different sizes and types in how key risks are communicated by business unit leaders to senior executives. According to the data in the table on the next page, the majority (59%) of organizations communicate key risks merely on an *ad hoc* basis at management meetings. Only 27% of the organizations surveyed scheduled agenda time to discuss key risks at management meetings. The percentage of organizations scheduling agenda discussions about risks at management meetings has been relatively flat over the last five years we have tracked this data point (34% in 2013, 33% in 2012, 33% in 2011, 29% in 2010 and 2009). The communication of key risks is more likely to be scheduled for discussion at management meetings for the largest organizations or financial services organizations, as shown on the next page. Written reports prepared on a monthly, quarterly, or annual basis are most likely to be prepared by the largest organizations, public companies, and financial services organizations. The largest organizations are more likely to enter risk data into a risk management database at least quarterly.

The majority of organizations communicate risk information to senior executives on an *ad hoc* basis.



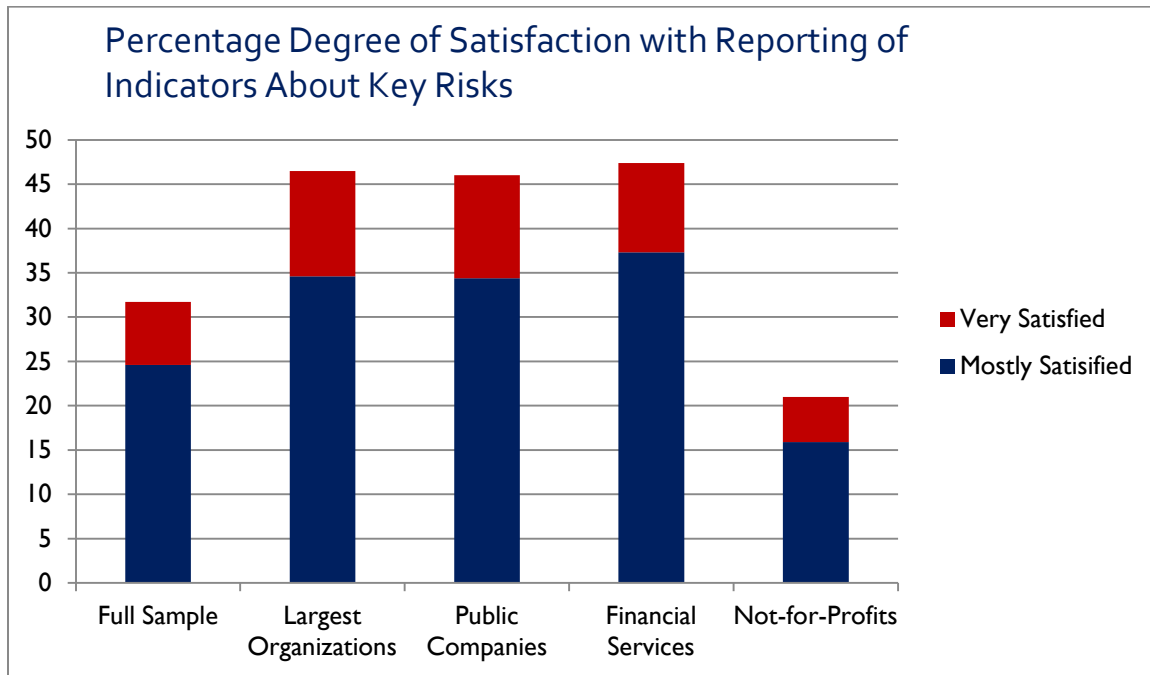


Percentage of Respondents

How are risks communicated from business unit leaders to senior executives?	Full Sample	Largest Organizations (Revenues >\$1B)	Public Companies	Financial Services	Not-for-Profit Organizations
<b>Ad hoc</b> discussions at management meetings	59%	43%	39%	47%	69%
Scheduled agenda discussion at management meetings	27%	37%	35%	37%	21%
Written reports prepared either monthly, quarterly, or annually	39%	71%	73%	62%	30%

Note: Respondents could select more than one choice. Thus, the sum of the percentages exceeds 100%.

Overall, there seems to be room for improvement in the nature of risk information being reported to senior executives. Almost half (41%) 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. Similar levels of dissatisfaction, 44% and 43%, were observed in our 2013 and 2012 reports, respectively. In contrast, only 32% are “mostly satisfied” or “very satisfied” with the nature and extent of reporting of key risk indicators to senior executives.



Results are very different, however, for the largest organizations where almost half (47%) of the respondents are mostly satisfied or very satisfied with the nature and extent of reporting of key risk indicators to senior executives regarding the entity’s top risk exposures. About half of public companies (46%) and financial services (47%) organizations report those levels of satisfaction with this type of reporting. Levels of satisfaction are lowest for



not-for-profits where 54% are not-at-all or only minimally satisfied with the nature and extent of their reporting of key risk indicators.

For the subset of publicly traded companies, we asked about the extent to which the organization's public disclosures of risks in their Form 10-K filing had increased in the past five years. We found that about one-fourth (26%) believed their disclosures had changed "mostly" while an additional 19% believed their disclosures had changed "extensively." We find these rates of change in disclosure noteworthy given that those same organizations indicated that the extent to which the volume and complexity of risks had increased over the past five years was "mostly" for 42% and "extensively" for 30%. Thus, the realization that the organization's risk profile has changed is also affecting its risk disclosures in the Form 10-K.



## Board of Director Involvement in Enterprise Risk Oversight

Regulators and other corporate governance proponents have placed a number of expectations on boards for effective risk oversight. The New York Stock Exchange (NYSE) Governance Rules place responsibility for risk oversight on the audit committee, while credit rating agencies, such as Standard & Poor's, evaluate the engagement of the board in risk oversight as part of their credit rating assessments. The SEC requires boards of public companies to disclose in proxy statements to shareholders the board's role in risk oversight, and the Dodd-Frank legislation imposes requirements for boards of the largest financial institutions to create board-level risk committees. While many of these are targeted explicitly to public companies, expectations are gradually being recognized as best practices for board governance causing a trickle-down effect on all types of organizations, including not-for-profits.

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 46% of the respondents in the full sample indicated that their boards have formally assigned risk oversight responsibility to a board committee. This is noticeably different from the largest organizations, public companies, and financial services organizations where 70%, 70%, and 60% respectively, of those organizations' boards have assigned to a board committee formal responsibility for overseeing management's risk assessment and risk management processes. For those boards that have assigned formal risk oversight to a committee, half (50%) are assigning that task to the audit committee. About a quarter of firms assign oversight to a risk committee. The largest organizations and public companies are most likely to assign formal risk oversight to the audit committee.

For about half of the organizations, the board has delegated risk oversight to a committee, with most delegating to the audit committee.

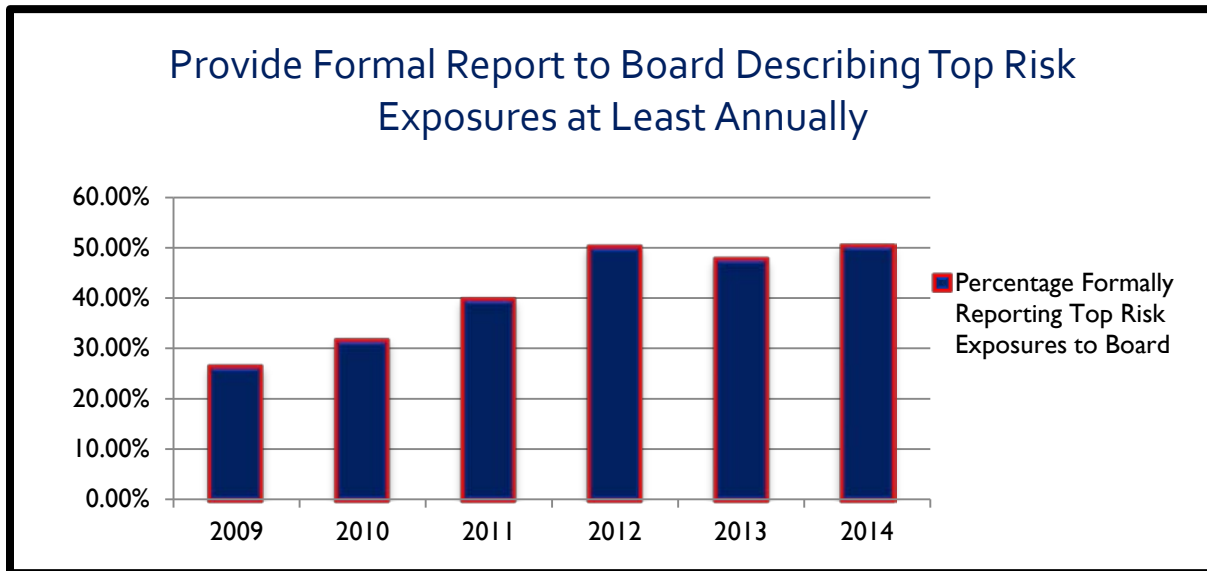
If board delegates formal responsibility of risk oversight to a subcommittee, which committee is responsible?	Percentage of Respondents				
	Full Sample	Largest Organizations (Revenues >\$1B)	Public Companies	Financial Services	Not-for-Profit Organizations
Audit committee	50%	56%	53%	38%	58%
Risk committee	24%	29%	31%	41%	7%
Executive committee	14%	4%	4%	9%	15%

In light of these formal committee assignments for oversight of the enterprise's risk management processes, we asked to what extent the full board reviews and discusses in a specific meeting the top risk exposures facing the organizations. Surprisingly, just over half (55%) of those in the full sample indicate that the full board has those discussions on a formal basis. However, as shown by the table below, boards of the largest organizations, public companies and financial services organizations are much more likely to discuss in a specific meeting the top risk exposures facing the organization.



Percentage of organizations where the	Percentage of Respondents				
	Full Sample	Largest Organizations (Revenues >\$1B)	Public Companies	Financial Services	Not-for-Profit Organizations
<i>Board of Directors reviews and discusses in a specific meeting the top risk exposures facing the organization</i>	<b>55%</b>	<b>74%</b>	<b>80%</b>	<b>69%</b>	<b>39%</b>

As illustrated by the graph below, about half (50%) of the organizations provide a formal report at least annually to the board of directors or one of its committees describing the entity’s top risk exposures. However, this number still represents a significant increase over the last six years. In 2009, we found that 26% of organizations provided that kind of information to the board at least annually. By 2014, that had risen to 50% of organizations surveyed.



As illustrated by the chart below, an overwhelming percentage (77%) of large organizations and public companies (84%) formally report top risk exposures to the board of directors or one of its committees at least annually. This is in line with what we found in our 2013 study where 85% of large organizations and 85% of public companies provided those reports to the board. In 2014, just over two-thirds of financial services organizations formally report top risk exposures to the board; however just 40% of not-for-profit organizations do so.

Percentage that formally report top risk exposures to the board at least annually	Percentage of Respondents				
	Full Sample	Largest Organizations (Revenues >\$1B)	Public Companies	Financial Services	Not-For-Profit Organizations
	<b>50%</b>	<b>77%</b>	<b>84%</b>	<b>68%</b>	<b>40%</b>



We also asked about the number of risk exposures that are typically presented to the board or one of its committees. As illustrated in the table below, just over half of the full sample and not-for-profit organizations report less than 5 risk exposures to the board. However, about two-thirds of the large organizations, public companies, and financial services organizations formally report between 5 and 19 risks to the board.

Percentage of organizations reporting the following number of risk exposures to the board of directors or one of its committees:	Percentage of Respondents				
	Full Sample	Largest Organizations (Revenues >\$1B)	Public Companies	Financial Services	Not-for-Profit Organizations
Less than 5 risks	51%	22%	20%	34%	58%
Between 5 and 9 risks	23%	28%	31%	26%	20%
Between 10 and 19 risks	18%	36%	34%	26%	15%
More than 20 risks	8%	14%	15%	14%	7%



## Integration of Risk Oversight and Strategic Planning

The increasingly competitive business landscape highlights the importance of having a more explicit focus on the interrelationship of risk-taking and strategy development and execution. We asked several questions to obtain information about the intersection of risk management and strategy in the organizations we surveyed.

We found that 36% of organizations in our full sample currently do no formal assessments of emerging strategic, market, or industry risks. The lack of these emerging risk assessments is greatest for not-for-profit organizations where we found that 41% of those organizations have no formal assessments of those types of risks. The largest organizations, public companies, and financial services organizations are much more likely to consider emerging strategic, market, and industry risks, where only 14%, 12%, and 18% of those organizations, respectively, have no formal assessments of these kinds of emerging risks.

Of those in the full sample that do attempt to assess strategic risks, most do so in a predominantly qualitative (14%) manner or by using a blend of qualitative and quantitative assessment tools (48%). This dominance of a qualitative approach holds true for the subgroups (largest organizations, public companies, and financial services firms) 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 strategy execution. Almost half (48%) of our respondents believe that existing risk exposures are considered "mostly" or "extensively" when evaluating possible new strategic initiatives and about one-third (33%) of the respondents believe that their organization has articulated its appetite for or tolerance of risks in the context of strategic planning "mostly" or "extensively." In addition, 36% of the respondents indicate that risk exposures are considered "mostly" or "extensively" when making capital allocations to functional units.

Over one-third of organizations in our survey do no formal assessments of strategic, market, or industry risks.

Extent that	Percentages		
	"Mostly"	"Extensively"	Combined
Existing risk exposures are considered when evaluating possible new strategic initiatives	34%	14%	48%
Organization has articulated its appetite for or tolerance of risks in the context of strategic planning	24%	9%	33%
Risk exposures are considered when making capital allocations to functional units	26%	10%	36%

These results suggest that there is still opportunity for improvement in better integrating risk oversight with strategic planning. Given the importance of considering the relationship of risk and return, it would seem that all organizations should "extensively" consider existing risk exposures in the context of strategic planning. Similarly, about one-third of organizations in our full sample have not articulated an appetite for risk-taking in the context



of strategic planning. Without doing so, how do boards and senior executives know whether the extent of risk-taking in the pursuit of strategic objectives is within the bounds of acceptability for key stakeholders?

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 only 27% indicated those discussions about top risk exposures in the context of strategic planning are “mostly” or “extensively.” When we separately analyzed this for the largest organizations, public companies, and financial services firms, we did find that those boards were somewhat more likely to integrate their discussions of the top risk exposures as part of their discussion of the organization’s strategic plan as documented in the table below.

Extent to which top risk exposures are formally discussed by the Board of Directors when they discuss the organization’s strategic plan	Percentage of Respondents				
	Full Sample	Largest Organizations (Revenues >\$1B)	Public Companies	Financial Services	Not-for-Profit Organizations
“Extensively”	10%	20%	16%	15%	6%
“Mostly”	17%	25%	27%	28%	11%
Combined	27%	45%	43%	43%	17%

Despite the higher percentages of boards that discuss risk exposures in the context of strategic planning for the largest organizations and public companies, the fact that more than half of those organizations are not having these kinds of discussions suggests that there is still room for marked improvement in how risk oversight efforts and strategic planning are integrated. Given the fundamental relationship between risk and return, it would seem that these kinds of discussions should occur in all organizations. Thus, there appears to be a continued disconnect between the oversight of risks and the design and execution of the organization’s strategic plan.



## Linkage of Risk Oversight and Compensation

The linkage between executive compensation and risk oversight is also receiving more attention. In fact, the SEC’s 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.

Most organizations do not include risk management activities as an explicit component in determining management compensation.

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 28% of the organizations surveyed, risk management is “not at all” a component of the performance compensation and for another 28% the component is only “minimally” considered. Thus, in a little over half of the organizations surveyed (56%), the extent that risk management activities are an explicit component in determining management compensation is non-existent or minimal. The outcomes shown in the following table actually represent a noticeable increase in some of the organization categories compared to the results from the 2013 survey where almost two-thirds said “not-at-all” or “minimally.” Many organizations are now less likely to consider risk management activities as a determinant for performance compensation.

Percentage of Respondents  
Selecting “Not-at-All” or “Minimally”

To what extent are risk management activities an explicit component in determining management performance compensation?	Full Sample	Largest Organizations (Revenues >\$1B)	Public Companies	Financial Services	Not-for-Profit Organizations
Not at All	28%	17%	15%	18%	38%
Minimally	28%	24%	23%	22%	31%
Combined	56%	41%	38%	40%	69%

While the largest organizations, public companies, and financial services firms are more likely to factor risk management activities into performance compensation, roughly four in ten firms within those subsets in our sample are “not at all” or only “minimally” doing so as illustrated by the table above. The increasing focus on compensation and risk-taking should lead more organizations over time to consider modifications to their compensation policies and procedures.





## Barriers to Progress

While our analysis suggests that organizations have made real advancements in how they identify, assess, and manage key risks, there is still plenty of room for improvement. In some ways it is encouraging to see the progress; however, given the significant global financial, economic, and political challenges that have been in play in recent years, it is discouraging not to see more organizations making progress in developing robust, systematic processes to oversee an entity's most significant risk exposures. There appear to be several perceived impediments that prevent management from taking the necessary actions 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 47% 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. It begs the question, *"so what processes are in place to help management and the board keep its eyes on emerging, strategic risks?"*

The next most common responses were "no requests to change our risk management approach" and "do not see benefits exceeding costs," noted by 36% and 20%, respectively, of respondents in the full sample. Thirty-two percent of those same respondents also noted that there are "too many pressing needs" while 24% reported a belief that they had "no one to lead the effort."

These findings are similar to those reported in our earlier reports. So, there has been little change in the nature of barriers 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 42% of the full sample describe their risk oversight processes as very immature or minimally mature, and a large proportion of our respondents indicated an overall dissatisfaction with their current approach to the reporting of information to senior executives about top risk exposures.

Respondents provided more depth about some of the primary barriers. The table on the next page contains a summary of those that the respondents described as a "barrier" or "significant barrier." Competing priorities and a lack of sufficient resources appear to be the most common barriers to adopting an ERM approach to risk oversight. A lack of perceived value and a lack of visible ERM leadership among boards and senior executives also affect ERM implementation decisions. The ordering of these most common barriers is consistent with the ordering of results provided in all our prior years' reports. The results are also very similar for each of the subsets we examined (largest organizations, public companies only, and financial services firms). A higher percentage of not-for-profits (42%) related to the full sample noted that competing priorities are the primary barrier to their embrace of ERM.



Description of Barrier	Percentage Believing Barrier is		
	"Barrier"	"Significant Barrier"	Combined Percentage
Competing priorities	25%	17%	42%
Insufficient resources	26%	16%	42%
Lack of perceived value	21%	12%	33%
Perception ERM adds bureaucracy	17%	11%	28%
Lack of board or senior executive ERM leadership	14%	11%	25%
Legal or regulatory barriers	6%	2%	8%

Most organizations (60%) have not provided or only minimally provided training and guidance on risk management in the past two years for senior executives or key business unit leaders. This is similar for the largest organizations (42%), public companies (39%), and financial services (41%). Training is least likely to be provided in not-for-profit organizations (70% provided no or only minimal training and guidance). Thus, while improvements have been made in the manner in which organizations oversee their enterprise-wide risks, the lack of robustness in general may be due to a lack of understanding of the key components of an effective enterprise-wide approach to risk oversight that some basic training and education might provide.



## Summary

While we do notice a trend towards more advanced enterprise-wide risk oversight from 2009 through 2014, there continue to be significant opportunities for improvement in the robustness of those processes. Organizations agree that the volume and complexity of risks they face continue to increase over time and they often encounter significant operational surprises. What we do observe is that the largest organizations, public companies, and financial services firms are more advanced in their risk oversight processes than the full sample of organizations. Thus, enterprise-wide risk management maturity does vary across different sizes and types of firms.

Results from all six years of our surveys continue to find that the approach to risk oversight in many 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. Even the large organizations, public companies, and financial services organizations admit that their risk management oversight processes are less than mature. The results from the survey suggest there may be a 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.

There may be opportunities to better connect risk oversight and strategic planning efforts. Four of ten sample firms (41%) admitted that they were “not at all” or “minimally” satisfied with the nature and extent of reporting of key risk indicators to senior executives regarding top risk exposures.

There are a number of resources available to executives and boards to help them understand their responsibilities for risk oversight and effective tools and techniques to help them in those activities (see for example, the NC State ERM Initiative’s Web site – <http://www.erm.ncsu.edu>). As expectations for more effective enterprise-wide risk oversight continue to unfold, it will be interesting to continue to track changes in risk oversight procedures over time.



## Appendix A: Description of Enterprise Risk Management (ERM)

An enterprise risk management (ERM) approach emphasizes a top-down 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.

Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) ***Enterprise Risk Management – Integrated Framework*** defines ERM as follows:

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

COSO's ***Enterprise Risk Management – Integrated Framework*** (2004)

ERM is a formal process that is enterprise-wide and addresses risks in a portfolio manner, where interactions among risks are considered.

Because the term "ERM" is used often, but not necessarily consistently understood, we provided respondents (as we did for the 2009 - 2013 reports) COSO's definition of enterprise risk management.



## 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, CPA, Ph.D.**, is the Deloitte Professor of Enterprise Risk Management and Director of the ERM Initiative at NC State University. He specializes in the study of enterprise risk management, corporate governance, financial statement fraud, and the financial reporting process. He completed over seven years of service as a board member of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and has served on other national-level task forces related to risk management issues. He advises boards and senior executive teams on risk governance issues, is a frequent speaker at national and international levels, and has published over 90 articles, research monographs, books, and other thought-related publications. He earned his Ph.D. at Michigan State University.

**Bruce C. Branson, Ph.D.**, is Professor of Accounting and Associate Director of the ERM Initiative in the Poole College of Management at NC State University. His teaching and research is focused on enterprise risk management and financial reporting, and includes an interest in the use of derivative securities and other hedging strategies for risk reduction/risk sharing. He also has examined the use of various forecasting and simulation tools to form expectations used in financial statement audits and in earnings forecasting research. He earned his Ph.D. at Florida State University.

**Bonnie V. Hancock, M.S.**, is the Executive Director of the ERM Initiative at NC State University where she also teaches graduate and undergraduate courses in the Poole College of Management. Her background includes various executive positions at Progress Energy where she has served as president of Progress Fuels (a Progress Energy subsidiary with more than \$1 billion in assets), senior vice president of finance and information technology, vice president of strategy and vice president of accounting and controller. She currently serves on the following corporate boards: AgFirst Farm Credit Bank where she chairs the risk policy committee, Office of Mortgage Settlement Oversight where she chairs the audit committee, and Powell Industries, a publicly traded company based in Houston, Texas, where she serves on both the compensation and audit committees.

Contact us at: [erm\\_initiative@ncsu.edu](mailto:erm_initiative@ncsu.edu) or 919.513.0901.

**NC STATE** Poole College of Management  
Enterprise Risk Management Initiative