Board of Trustees Audit, ERM, Compliance, and Ethics Committee Meeting
April 19, 2018
Agenda

I.	Approval of February 15, 2018 Minutes	Action
II.	Office of Internal Audit - Mr. Wayne Poole	
	A. Internal Audit Dashboard	Information
	B. Staffing Update	Information
	C. Hotline/Investigative Audit Activity	Information
	D. Proposed Audit Plan Changes	Action
	E. Internal Audit Operating Budget	Information
III.	Research Compliance - Dr. Mike Van Scott	
	A. Export Controls Officer Introduction	Information
IV.	Enterprise Risk Management - Mr. Tim Wiseman	
	A. Update of ERM Activities	Information
V.	Information Security - Mr. Don Sweet (CIO)	Information
VI.	Closed Session	
VII.	Other Business	

Board of Trustees

Audit, ERM, Compliance, and Ethics Committee Meeting

April 19, 2018

Agenda Item:	I. Approval of February 15, 2018 Minutes
Responsible Person:	Kel Normann, Chair
Action Requested:	Approval
Notes:	N/A

Back To Agenda

DRAFT

Minutes from ECU BOT Audit, Enterprise Risk Management, Compliance, and Ethics Committee
February 15, 2018
Coastal Studies Institute* – Wanchese, NC

The Audit, Enterprise Risk Management, Compliance, and Ethics Committee of the ECU Board of Trustees met at the UNC Coastal Studies Institute in Wanchese, NC on February 15, 2018.

Committee members present included Kel Normann (Chair), Bob Plybon (Vice Chair), Mark Copeland, Max Joyner, Jason Poole, Vince Smith, and LaQuon Rogers

Other board members present included Kieran Shanahan (Board Chair), Edwin Clark, Vern Davenport, Deborah Davis, Leigh Fanning, Fielding Miller

Others present* included Chancellor Cecil Staton, James Hopf, Donna Payne, Nick Benson, Michelle Evans*, Rick Niswander, Dee Bowling*, Alton Daniels, Megan Ayers, Josh Brown*, Tim Wiseman*, Stacie Tronto*, Amanda Danielson*, Sarah von Stein*, and Wayne Poole*.

* *These people joined the meeting via video conference from Spilman 105 on the campus of ECU.*

Kel Normann, Chair of the Committee, convened the meeting at 11:40AM. Mr. Normann read the conflict of interest provisions as required by the State Government Ethics Act. Mr. Normann asked if anyone would like to declare or report an actual or perceived conflict of interest. None were reported.

Mr. Normann asked for the approval of the minutes of the November 9, 2017 audit committee meeting.

Action Item: The minutes of the November 9, 2017 audit committee meeting were approved with no changes.

Mr. Tim Wiseman provided the **Enterprise Risk Management** (**ERM)** update.
Mr. Wiseman briefed the committee on the ERM office's recent activities and initiatives. He advised the committee that he has been assisting the UNC System Office with the risk assessment at Elizabeth City State University. Mr. Wiseman also advised the committee that the UNC System Office is in the process of exploring how to establish an ERM framework for the entire system. ECU is already on the leading edge in this area and will likely be counted on to provide advice and assistance.

Mr. Wiseman provided an update on the development of risk management plans related to the University's "Top 10" risks that were identified during the annual risk prioritization exercise.

Mr. Wiseman advised the committee that the ERM office recently led a discussion on the events at Michigan State, and coordinated a meeting with administrators from Athletics, University Counsel, Internal Audit, Student Affairs, and Title IX Compliance to discuss the case, the implications for ECU, and lessons to be learned.

Mr. Wayne Poole provided the **Internal Audit** update.
Mr. Poole advised the committee that Chief Audit Officer Stacie Tronto was selected by the state's Council of Internal Audit as the 2017 recipient of the North Carolina Internal Audit Award of Excellence. This is the second time that Ms. Tronto or the ECU Internal Audit team has received this honor. The ECU Office of Internal Audit won the award in 2012.

Mr. Poole presented the Internal Audit dashboard as of January 31, 2018. As of January 31, 2018, 41% of the annual audit plan is complete, with another 48% in progress. The direct productivity rate for the Audit staff was 72%. Management had made satisfactory progress towards resolving 100% of the audit recommendations that Internal Audit has followed up on so far this fiscal year.

Mr. Poole updated the committee on Internal Audit staffing changes (1 recent and two pending retirements) and the implementation of the electronic audit workpapers software. ECU Internal Audit has been asked to demonstrate how they are using the new software for the audit teams at the other UNC system schools.

Back To Agenda

Mr. Poole updated the committee on the volume of hotline and investigative audit activity so far this fiscal year. So far this year, (just over halfway through the year), Internal Audit has received 21 hotline calls (In FY 2017, there were 10 for the entire year). So far this year, 22 investigative audits/special reviews have been begun or completed (compared to 16 total for FY 2017). Internal Audit budgeted 2200 hours for this category, but will likely need 3000 or more hours for investigative audits and special reviews. The high volume of investigative work will lead to some necessary changes in the annual audit plan, which will be presented to the committee at the April meeting.

Mr. Poole updated the committee on several information security-related topics. One key recent change was the approval of a new UNC system-wide policy which requires one individual at each institution be assigned responsibility for Information Security. That individual is also required to report to the Audit Committee to provide periodic updates and information. Mr. Poole stated that Chancellor Staton and Vice Chancellor Niswander have assigned this responsibility to Chief Information Officer Don Sweet. Mr. Sweet will be briefing the committee at the April meeting.

Closed Session
At 12:00 PM, a committee member made a motion that the committee go into closed session in order to discuss items that are protected according to state statutes governing personnel information, internal audit working papers, sensitive security information, and/or otherwise not considered a public record within the meaning of Chapter 132 of the North Carolina General Statutes. The motion was seconded and unanimously approved.

Return to Open Session
The Committee returned to open session and continued work on the agenda at 12:19 PM.

Other Business
Dr. Nick Benson, Associate Vice Chancellor for Health Sciences Regulatory Affairs, advised the committee that Dr. Ken Deville will be stepping down from his role as the Director of the Office of Institutional Integrity to return to a faculty role. Ms. Michelle Evans will serve as the Director on an interim basis.

There being no further business, the Audit Committee meeting was adjourned at 12:21 PM.

_____

Respectfully submitted,
Wayne Poole
ECU Office of Internal Audit and Management Advisory Services

Back To Agenda

Board of Trustees

Audit, ERM, Compliance, and Ethics Committee Meeting

April 19, 2018

Agenda Item:	II.A. Internal Audit Dashboard
Responsible Person:	Wayne Poole
Action Requested:	None - Information
Notes:	N/A

Back To Agenda

Internal Audit Dashboard - as of March 31, 2018

Completion of Audit Plan: Completed vs. Planned Audits

Status of Audit Plan	Number of Engagements	Percent of Total Plan
Completed	28	50%
Reporting Phase	4	7%
In Process	19	34%
Pending	5	9%
Total	**56**	**100%**

Goal = 80%

Staff Utilization: Direct vs. Indirect Hours

	With UPS	Without UPS
Direct Hours	68%	74%
Indirect Hours	32%	26%

Goal = 75%

Consultations

	Number	% of Audit Plan
Consultations	89	10%

Should not exceed 20%

Management's Corrective Actions

Observations by Division:	Completed	Outstanding	% Complete	% Outstanding	Pending
Academic Affairs	0	0	0%	0%	6
Administration and Finance	0	0	0%	0%	31
Athletics	0	0	0%	0%	0
Chancellor	0	0	0%	0%	3
Health Sciences	5	0	100%	0%	4
Research and Graduate Studies	0	0	0%	0%	3
Student Affairs	0	0	0%	0%	0
University Advancement	0	0	0%	0%	0
Total Observations	**5**	**0**			47
Total Percentages	**100%**	**0%**			

Goal = 95%

Back To Agenda

Board of Trustees

Audit, ERM, Compliance, and Ethics Committee Meeting

April 19, 2018

Agenda Item:	II.B. Staffing Update
Responsible Person:	Wayne Poole
Action Requested:	None - Information
Notes:	N/A

Back To Agenda

Board of Trustees

Audit, ERM, Compliance, and Ethics Committee Meeting

April 19, 2018

Agenda Item:	II.C. Hotline/Investigative Audit Activity
Responsible Person:	Wayne Poole
Action Requested:	None - Information
Notes:	N/A

Back To Agenda

Board of Trustees

Audit, ERM, Compliance, and Ethics Committee Meeting

April 19, 2018

Agenda Item:	II.D. Proposed Audit Plan Changes
Responsible Person:	Wayne Poole
Action Requested:	Approval
Notes:	N/A

Back To Agenda

East Carolina University
Office of Internal Audit
Annual Engagement Plan
By Type
FY 2017-2018

Description	Budget Status	Budgeted Hours	Revised Hours	%age of Total	Revised % of total	Risk Ranking
Integrated/Operational Audits:						
Teaching Overload Payments	CYP	300	800	2%		Med
SoDM CSLCs	CYP	420	0	3%		High
Greek Life	CYP	400	0	2%		High
Athletics Imprest Fund	CYP	200	200	1%		High
Security Cameras	CYP	400	20	2%		High
Export Controls	CYP	400	400	2%		High
Governance and Ethics	CYP	400	400	2%		High
Total Operational Audit Hours		**2520**	**1820**	**15%**	**11%**	
Compliance Audits:						
University Youth Programs	CYP	400	400	2%		High
Student Academic Appellate Process	CYP	400	344	2%		High
Conflict of Interest/Management Plans	WIP	20	20	0%		HIgh
Total Compliance Audit Hours		**820**	**764**	**5%**	**5%**	
Information Technology Audits:						
Mobile Device Policies and Controls	CYP	300	300	2%		High
Change Control Practices	CYP	300	340	2%		High
IT Disaster Recovery	WIP	200	150	1%		High
Total Information Technology Audit Hours		**800**	**790**	**5%**	**5%**	
Special Reviews:						
Special Reviews - Pending	CYP	1500	2700	9%		NA
Special Reviews in Progress	WIP	700	700	4%		NA
Total Special Review Audit Hours		**2200**	**3400**	**13%**	**20%**	
Follow-Up Reviews:						
3rd-Parking and Transportation Services (A15014)	CYP	20	20	0%		Med
2nd-Academic Integrity (A16019)	CYP	40	40	0%		High
Undergraduate Admissions Waivers (A17028)	CYP	40	40	0%		High
Title IX (A17027)	CYP	100	70	1%		High
Telemedicine (A16050)	CYP	120	75	1%		High
Incident Detection (A17009)	CYP	100	100	1%		High
Kronos/Payroll (A16038)	CYP	150	150	1%		High
Organizational Continuity (A16044)	CYP	40	0	0%		High
User Account On and Off-Boarding (A17008)	CYP	100	100	1%		High
One Card Access (A17004)	CYP	60	60	0%		High
Total Follow-Up Review Audit Hours		**770**	**655**	**5%**	**4%**	

Budget Status:
BF = Brought Forward From Previous Year's Plan
AYP = Added to Current Year Plan
CYP = Current Year Plan
CYP-B = Current Year Plan (Budgeted under Special Reviews - Pending)
WIP = Work-In-Progress

Back To Agenda

East Carolina University
Office of Internal Audit
Annual Engagement Plan
By Type
FY 2017-2018

Description	Budget Status	Budgeted Hours	Revised Hours	%age of Total	Revised % of total	Risk Ranking
Other/Special Projects:						
Consultations	CYP	2900	2900	17%		NA
Committees/Other Routine Tasks (ie. SBI Reports, Assist State Auditor)	CYP	500	500	3%		NA
Audit Management Software Implementation	CYP	500	600	3%		High
Data Analytics	CYP	600	600	4%		High
Anti-Fraud Guide	CYP	200	200	1%		High
Student Intern	CYP	200	200	1%		NA
Self-Assessment of Internal Audit	CYP	100	0	1%		High
Risk Assessment/Audit Planning 2018-2019	CYP	40	40	0%		High
Risk Assessment/Audit Planning 2017-2018	WIP	20	20	0%		High
Total Other/Special Project Hours		**5060**	**5060**	**30%**	**30%**	
Total Direct Audit Hours		**12170**	**12489**	**73%**	**74%**	
Administration	CYP	1350	1350	8%		NA
Leave	CYP	2500	2500	15%		NA
Professional Development	CYP	620	620	4%		NA
Total Indirect Audit Hours:		**4470**	**4470**	**27%**	**26%**	
Grand Total Audit Hours		**16640**	**16959**	**100%**	**100%**	

=Delete from Audit Plan/Postpone
=Add to Audit Plan
=Material Change in Budget

Chancellor/Date

ECU BOT Audit Committee Chair/Date

Budget Status:
BF = Brought Forward From Previous Year's Plan
AYP = Added to Current Year Plan
CYP = Current Year Plan
CYP-B = Current Year Plan (Budgeted under Special Reviews - Pending)
WIP = Work-In-Progress

Back To Agenda

Board of Trustees

Audit, ERM, Compliance, and Ethics Committee Meeting

April 19, 2018

Agenda Item:	II.E. Internal Audit Operating Budget
Responsible Person:	Wayne Poole
Action Requested:	None - Information
Notes:	N/A

Back To Agenda

Board of Trustees

Audit, ERM, Compliance, and Ethics Committee Meeting

April 19, 2018

Agenda Item:	III.A. Export Controls Officer Introduction
Responsible Person:	Mike Van Scott
Action Requested:	None - Information
Notes:	N/A

Back To Agenda

Board of Trustees

Audit, ERM, Compliance, and Ethics Committee Meeting

April 19, 2018

Agenda Item:	IV.A. Update of ERM Activities
Responsible Person:	Tim Wiseman
Action Requested:	None - Information
Notes:	N/A

Back To Agenda

4/2/2018

INFORMATION PAPER

SUBJECT: Enterprise Risk Management (ERM) Update for the BOT-Audit, Risk Management, Compliance and Ethics Committee April 2018 Meeting

1. Purpose. To advise BOT-ARMCE committee members of significant ERM activities from the past two months and those planned or anticipated for the next two months.

2. Action Recapitulation:

a. Significant ERM/CRO Activities from the Past Two Months:

- ERM Consultation and Assistance to UNC-Support Office and ECSU – Ongoing
  - Completed Risk Assessment Report – Presented to ECSU BOT
  - UNC ERM in Higher Ed Workshop – Facilitated (Agenda Attached FYI)
- Quarterly ERM Committee Meeting – (Feb)
- ECU Emergency Operations Plan Working Group
- Youth Programs Annual Workshop – Insurance and Risk Mgmt Input
- UAS/Drone Flight Requests Screening - Multiple
- SACS Accreditation Review Input – Risk Management Narrative
- University Admissions Safety and University Employee and Student Behavior Concern Teams Meetings and Actions
- ERM and Military Programs Orientation for New VCAF (Ms. Thorndike)
- ERM Consultations/Research/Inquiries – Various Departments
  - ECU Siblings Weekend - Student Affairs
  - Privatized Sports Camps Issues Review – Athletics & Internal Audit
  - Document Security and Storage Working Group – Various

b. Significant ERM/CRO Activities Next Two Months:

- ERM Consultation and Assistance to UNC-Support Office – Ongoing
- University Admissions Safety and University Employee and Student Behavior Concern Teams Meetings and Actions
- ECU Risk Management Program Framework Reference and Philosophy Statement
- Present ERM in Higher Ed Webinar for Arizona School Risk Retention Trust (ASRRT)
- Prepare for Summer/Fall Top Risk Survey and Risk Management Plans Review
- ERM Consultations/Research/Inquiries – Various Departments

3. Other:

- 2018 The State of Risk Oversight, 9th Edition, March 2018 – Attached/Included FYI

ACTION OFFICER: Tim Wiseman
Assistant Vice Chancellor for ERM & Military Programs
Spilman Bldg., Room 214, 252-737-2803

Back To Agenda

PRIMA 2018 ERM Training Itinerary				
DAY 1	**8:00 am**	**Attendee Check- In**		**Outside of Sterling 6**
	8:30 am	**Breakfast**		**Sterling 6**
Module 1: Workshop & Agenda Overview	**9:00 am**	**All Attendees – Sterling 6**		**Program Outline**
Module 1: Implementing ERM Using ISO 31000	**9:30 am**	**All Attendees – Sterling 6**		**Introductions** **1. Reasons** **2. Learning objectives**
	10:30 am	**Break – Sterling 6**		
Module 2: Understanding ISO 31000 and Your Organization	**10:45 am**	**All Attendees – Sterling 6**		**1. ID people** **2. ID key principles** **3. Brainstorm evidence**
Lunch – Sterling 6				
Module 3: Building a Sustainable Framework	**1:00 pm**	**Higher Ed Sterling 3**	**Public Sector Sterling 1**	**1. Note taking** **2. Context** **3. Stakeholders**
	2:15 pm	**Break – Sterling 6**		
Module 4: RM Process (Part 1)	**2:30 pm**	**Higher Ed Sterling 3**	**Public Sector Sterling 1**	**1. Context & risk assess** **2. Open discussion**
	6:00 pm -7:00 pm	**Welcome Reception**		**Sterling 6**
DAY 2	**8:30 am**	**Breakfast**		**Sterling 6**
Module 5: RM Process (Part 2) – Risk Assessment Techniques	**9:00 am**	**Higher Ed Sterling 3**	**Public Sector Sterling 1**	**1. Risk treatment**
	10:30 am	**Break – Sterling 6**		
Module 6: Building Your Plan	**10:45 am**	**Higher Ed Sterling 3**	**Public Sector Sterling 1**	**1. Building your plan**
Lunch – Sterling 6				
Module 7: Continuing Improving & Sustaining the Work	**1:00 pm**	**Higher Ed Sterling 3**	**Public Sector Sterling 1**	**1. Framework Design Elements – Monitor & review**
	2:00 pm	**Break – Sterling 6**		
Module 8: Summary, Review and Next Steps	**2:30 pm**	**Higher Ed Sterling 3**	**Public Sector Sterling 1**	**1. Potential problem areas** **2. Takeaways & learning objectives**

Back To Agenda

2018

THE STATE OF RISK OVERSIGHT

AN OVERVIEW OF ENTEPRISE RISK MANAGEMENT PRACTICES

9TH EDITION | MARCH 2018

Mark Beasley
Deloitte Professor of ERM
Director, ERM Initiative

Bruce Branson
Associate Director, ERM Initiative

Bonnie Hancock
Executive Director, ERM Initiative

AICPA

NC STATE Poole College of Management
Enterprise Risk Management Initiative

Back To Agenda

OVERVIEW OF STUDY

The highly dynamic global business environment, combined with geopolitical shifts, rapidly emerging technologies, cyber threats, economic and financial market volatilities, tax reform and other emerging developments create tremendous opportunities for organizations as they pursue growth and the advancement of their core mission. As business leaders manage the ever-changing economic, political, and technological landscape they face an exponentially increasing range of uncertainty that creates a highly complex portfolio of potential risks that, if unmanaged, can cripple, if not destroy, an organization's business model and brand.

Some business leaders and other key stakeholders are recognizing the increasing complexities and real-time challenges of navigating potentially emerging risks as they seek to achieve key strategic goals and objectives. Many are investing more in how they proactively manage potentially emerging risks by strengthening their organizations' processes surrounding the identification, assessment, management, and monitoring of those risks most likely to impact – both positively and negatively – the entity's strategic success. A number of organizations have embraced the concept of enterprise risk management (ERM), which is designed to provide an organization's board and senior leaders a top-down, strategic perspective of risks on the horizon so that those risks can be managed proactively to increase the likelihood the organization will achieve its core objectives.

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 nine years with the American Institute of Certified Public Accountants' (AICPA) Management Accounting - Business, Industry, and Government Team to survey business leaders regarding a number of characteristics related to their current enterprise-wide risk management efforts. This is the ninth report that we have published summarizing our research in partnership with the AICPA.

Data was collected during the fall of 2017 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 474 fully completed surveys from individuals representing different sizes and types of organizations (see **Appendix A** for details about respondents). This report summarizes our findings and provides a resource for benchmarking an organization's approach to risk oversight against current practices. In addition to highlighting key findings for the full sample of **474 respondents**, we also separately report many of the key findings for the following subgroups of respondents:

- 130 large organizations (those with revenues greater than $1 billion)
- 138 publicly-traded companies
- 137 financial services entities
- 103 not-for-profit organizations

The following page 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 S. Beasley
Deloitte Professor of ERM
ERM Initiative

Bruce C. Branson
Associate Director
ERM Initiative

Bonnie V. Hancock
Executive Director
ERM Initiative

Back To Agenda

SUMMARY OF KEY OBSERVATIONS

1 **Managing risks in today's environment isn't getting easier.** Most respondents (60%) believe the volume and complexity of risks is increasing extensively over time. And, 65% of organizations indicate they have recently experienced an operational surprise due to a risk they did not adequately anticipate.

2 **Demands for greater management focus on risks are increasing.** Most boards of directors (68%) are putting pressure on senior executives to increase management involvement in risk oversight. Strong risk management practices are becoming an expected best practice. These pressures are getting harder and harder for senior executives to ignore.

3 **Risk management practices in most organizations remain relatively immature.** Twenty-two percent of respondents describe their risk management as "mature" or "robust" with the perceived level of maturity declining over the past two years. Thirty-one percent of organizations (48% of the largest organizations) have complete ERM processes in place.

4 **Organizations are formalizing their risk management leadership structures.** The percentage of organizations designating an individual to serve as chief risk officer (or equivalent) has increased over time, with 67% of large organizations and 63% of public companies doing so. Most of those organizations (>80%) have management risk committees.

5 **Most struggle to integrate risk management with strategy.** Less than 20% of organizations view their risk management process as providing important strategic advantage. Only 29% of the organizations' board of directors substantively discuss top risk exposures in a formal manner when they discuss the organization's strategic plan.

6 **Organizations have some elements of risk management processes.** About one-half (45%) of the organizations have a risk management policy statement, with 43% maintaining risk inventories at an enterprise level. About 40% have guidelines for assessing risk probabilities and impact. Most (75%) update risk inventories at least annually.

7 **Boards receive written reports annually about top risks, but the underlying process may not be robust.** Most boards of large organizations (82%) or public companies (89%) discuss written reports about top risks at least annually; however, just 60% of those describe the underlying risk management process as systematic or repeatable.

8 **Opportunities exist for improvement in the nature of risk information being reported to senior management.** Forty-one percent (41%) of the respondents admit they are "not at all" or only "minimally" satisfied with the nature and extent of internal reporting of key risk indicators that might be useful for monitoring emerging risks by senior executives.

9 **Few organizations are linking risk management responsibilities to incentive compensation.** The lack of risk management maturity may be tied to the challenges of providing sufficient incentives for them to engage in risk management activities. Most (66%) have not included explicit components of risk management activities in compensation plans.

10 **Different barriers exist that limit progress in how organizations manage risks.** Respondents of organizations that have not yet implemented an enterprise-wide risk management process indicate that one impediment is the belief that the benefits of risk management do not exceed the costs or there are too many other pressing needs.

While there is some indication that management efforts related to enterprise-wide risk oversight are increasing over time, there continues to be noticeable room for improving how organizations identify, manage, and keep their eyes on risks that may emerge and significantly impact their ability to achieve strategic goals. This report puts a spotlight on a number of risk management practices that organizations may want to consider as they seek to strengthen their ability to proactively and strategically navigate rapidly emerging risks.

Back To Agenda

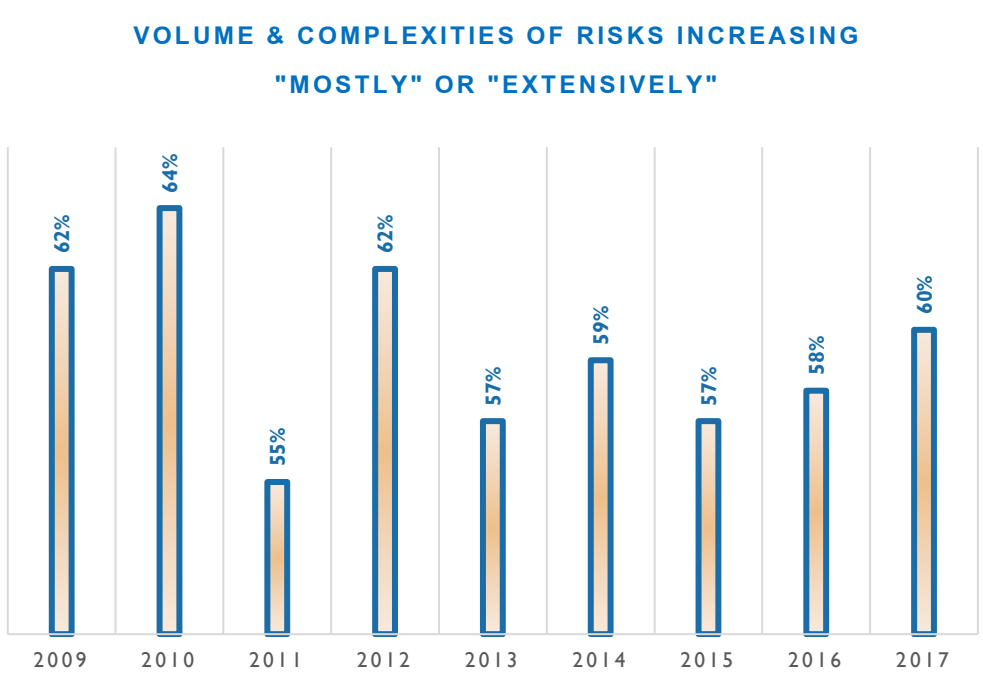
CHALLENGING RISK ENVIRONMENT

- ***The volume and complexities of risks in the global business environment are increasing.***
- ***Risks are triggering significant operational surprises.***
- ***The management of risks is not getting easier.***

Growth in equity markets, tax reform, rapid pace of innovation, cyber breaches, evolving geo-political shifts in leadership, terrorism, and significant natural disasters, among numerous other issues, represent examples of challenges management and boards face in navigating an organization's risk landscape. These developments are increasing the volume and complexity of risks faced by organizations today, creating huge challenges for management and boards in their oversight of the most important risks.

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.

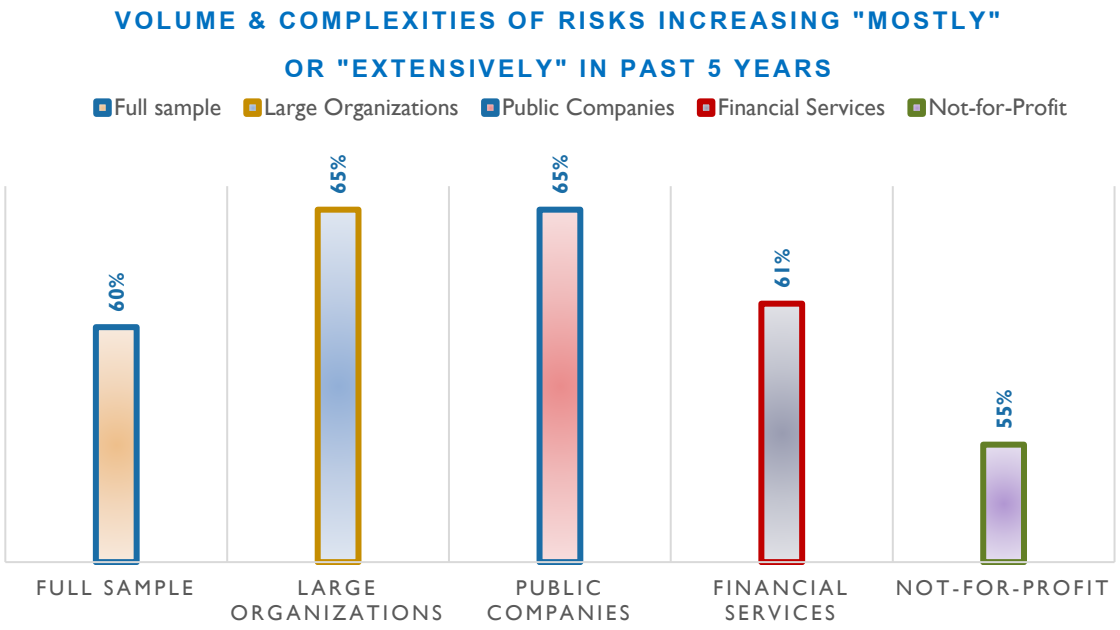
To get a sense for the extent of risks faced by organizations represented by our respondents, we asked them to describe how the volume and complexity of risks have increased in the last five years. Twenty-one percent noted that the volume and complexity of risks have increased "extensively" over the past five years, with an additional 39% responding that the volume and complexity of risks have increased "mostly." Thus, on a combined basis, 60% 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 noted in the most recent prior years. Less than 2% responded that the volume and complexity of risks have not changed at all. While the higher percentages in 2009-2010 were likely due to concerns related to the "Great Recession", the higher percentages in 2016-2017 may be due to increased concerns related to geopolitical shifts, cyber threats, terrorism, and the rapid deployment of new technology-based innovations, among other risk drivers.



Back To Agenda

	Percentage of Respondents				
Question	Not at All	Minimally	Somewhat	Mostly	Extensively
To what extent has the volume and complexity of risks increased over the past five years?	1%	6%	32%	39%	21%

We separately analyzed responses to this question for various subgroups of respondents. As shown below, the percentage of respondents indicating an increase in the volume and complexity of risks is even higher for large organizations and public companies. Not-for-profit organizations are not immune to this either. While the percentages shown in the chart below were closer to 70% last year for the larger organizations and those in financial services, the current year findings, while somewhat lower, continue to indicate that the overall business environment is perceived as relatively risky across all types of entities.

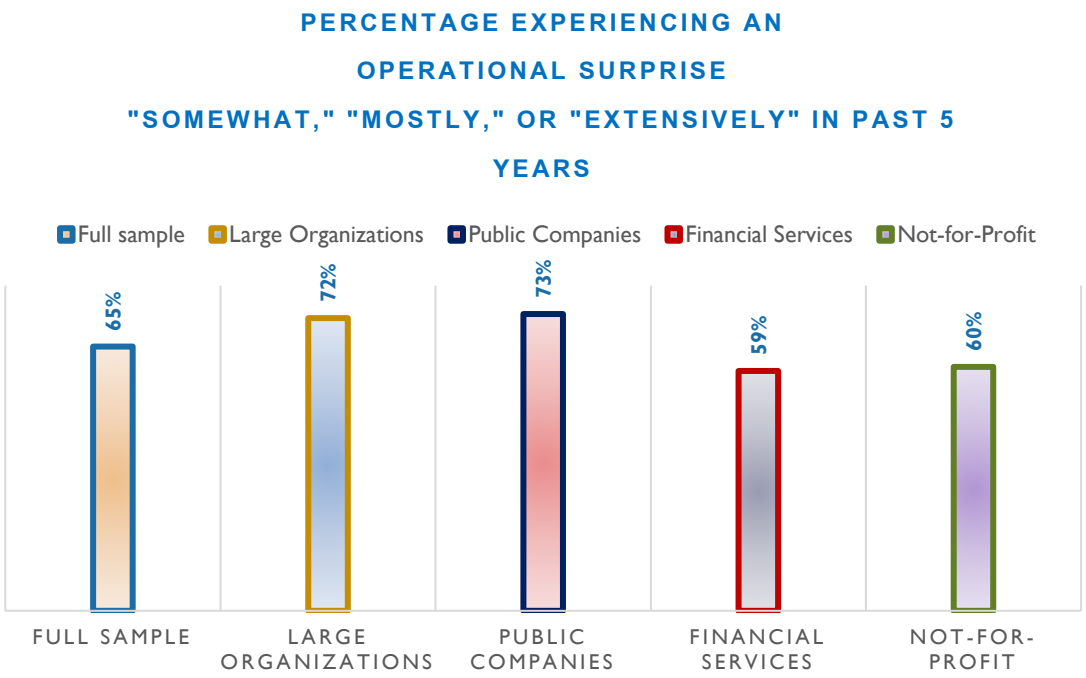


Some risks have actually translated into significant operational surprises for the organizations represented in our survey. About 8% noted that they have been affected by an operational surprise “extensively” within the last five years and an additional 26% of respondents noted that they have been affected “mostly” in that same time period. An additional 32% responded “somewhat” to this question. Collectively, this data indicates that the majority of organizations (66%) are being affected by real risk events (e.g., a competitor disruption, an IT systems breach, loss of key talent, among numerous others possible events) in their organizations that have affected how they do business, consistent with what we found in prior years.

	Percentage of Respondents				
Question	Not at All	Minimally	Somewhat	Mostly	Extensively
To what extent has your organization faced an operational surprise in the last five years?	5%	29%	32%	26%	8%

Back To Agenda

The rate of operational surprises is even higher for larger organizations and public companies where 72% and 73%, respectively, of respondents answered the question with “somewhat,” “mostly,” or “extensively.” The reality is that all organizations are dealing with unexpected risks. About 60% of the financial services entities and not-for-profit organizations in our sample responded with “somewhat” or higher to this question about the presence of operational surprises in the past five years.



While these percentages were closer to 80% in the prior year for large organizations and public companies and 70% for financial services, the percentages for the current year continue to reveal that an overwhelming majority of respondents across different types of organizations have experienced a significant operational surprise in the past five years. 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 these 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.

Back To Agenda

EXPECTATIONS GROWING FOR IMPROVED ENTERPRISE-WIDE RISK OVERSIGHT

- ***Boards of directors are placing significant expectations on management for increased senior executive involvement in risk oversight.***
- ***CEOs continue to seek more robust risk management practices.***
- ***Unfortunately for some organizations, it takes the occurrence of an unexpected risk event to prompt management to subsequently invest more in risk management.***

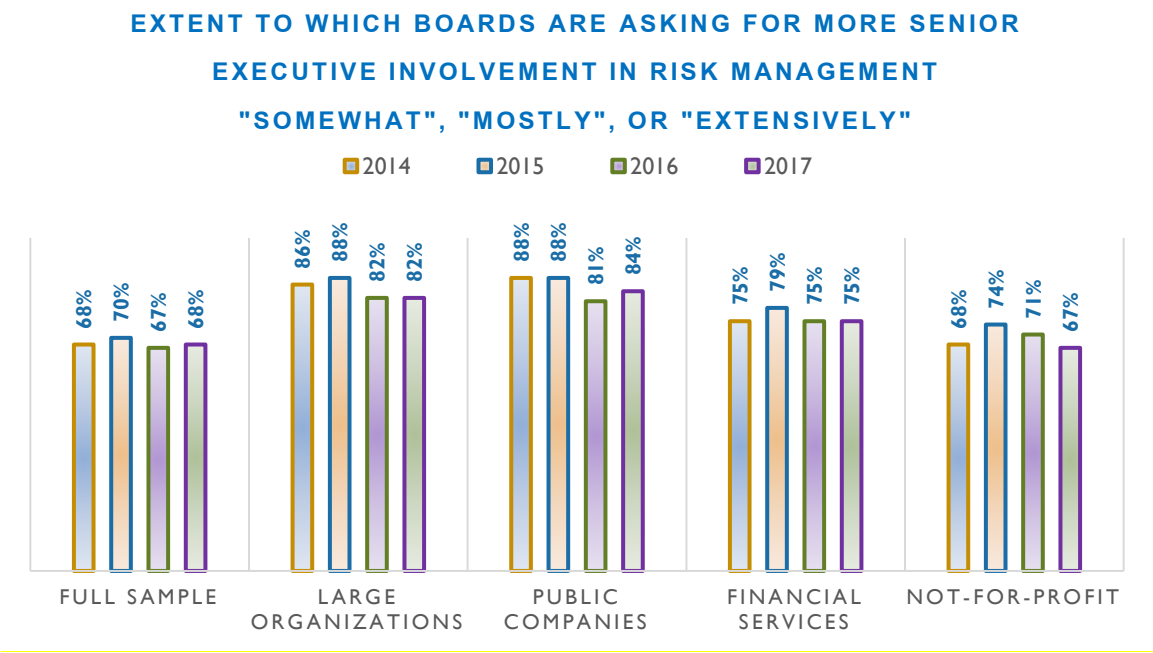
Our survey results indicate that board of director expectations for improving risk oversight in these organizations is strong, especially for the largest organizations, public companies, and financial services entities. Respondents noted that for 14% of the organizations surveyed, the board of directors 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."

	Percentage of Respondents				
Extent to which the board of directors is asking for increased senior executive involvement in risk oversight	Full Sample	Largest Organizations (Revenues >$1B)	Public Companies	Financial Services	Not-for-Profit Organizations
"Extensively"	14%	17%	22%	16%	9%
"Mostly"	27%	37%	33%	31%	31%
"Somewhat"	27%	28%	29%	28%	27%
Combined	68%	82%	84%	75%	67%

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 above. Interestingly, requests from the board of directors for increased risk oversight are high for not-for-profit organizations, too. And, as illustrated by the chart on the next page, the board's level of interest in more senior executive engagement in risk management has been holding strong for the past four years. This suggests that effective risk management is a priority among boards for management to consider.

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

Back To Agenda



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.

The board's interest in strengthened risk oversight may explain why the chief executive officer (CEO) is also calling for increased senior executive involvement in risk oversight. Almost half (46%) of the respondents indicated that the CEO has asked "mostly" or "extensively" for increased management involvement in risk oversight, which is an increase from the 43% we saw in 2016. An additional 26% 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 on the next page, while a small percentage (10%) 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 almost two-thirds (62%) of our respondents believe the external pressure to be more transparent about their risk exposures is "somewhat" to "extensive." That result is relatively consistent with the 62% reported last year.

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

External pressures are notably stronger for financial services entities, likely from regulators who are becoming more vocal proponents of ERM in financial services. Respondents in 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. However, we did observe some reduction from the 83% reported last year for financial services (with similar levels

Back To Agenda

of reductions for large organizations and public companies). Interestingly, the 55% reported for not-for-profit organizations is up from the 48% reported last year, suggesting that not-for-profit organizations are under greater pressure to strengthen senior management's engagement in risk management.

	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"	10%	11%	11%	17%	4%
"Mostly"	22%	22%	22%	25%	19%
"Somewhat"	30%	34%	36%	29%	32%
Combined	62%	67%	69%	71%	55%

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 unanticipated risk events, emerging best practice expectations, and regulator demands are the three most frequently cited factors for increasing senior executive involvement. However, as illustrated by the table below, regulator demands seem to be putting even greater pressure on senior executives in financial services organizations along with emerging best practices. Board of director requests for enhanced risk oversight are particular strong for the largest organizations and public companies. The view that effective risk management practices are an emerging best practice seems to be the primary motivator for not-for-profit organizations to increase senior executive focus on risk management activities.

	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	31%	36%	37%	50%	24%
Unanticipated risk events affecting organization	35%	39%	40%	34%	37%
Emerging best practice expectations	39%	38%	38%	44%	53%
Emerging corporate governance requirements	28%	28%	34%	39%	24%
Board of Director requests	31%	43%	49%	36%	25%

The above table highlights that there are a number of drivers for enhanced risk management activities. We did note, however, reduction in some of these percentages for the current year. For example, regulatory demands for financial services of 50% in the current year is noticeably lower than the 66% reported last year (not shown in the above table). This may be a reflection of the emphasis being placed by the current U.S. presidential administration on reducing some of the perceived regulatory burden affecting organizations.

Back To Agenda

NATURE OF RISK MANAGEMENT PROCESSES IN PLACE TODAY

- ***Risk management practices in most organizations remain relatively immature.***
- ***Larger organizations, public companies, and financial services entities have more advanced risk management practices relative to other organizations.***
- ***The percentage of organizations implementing enterprise risk management (ERM) practices is increasing, although fewer than half of the organizations surveyed have complete ERM practices in place.***

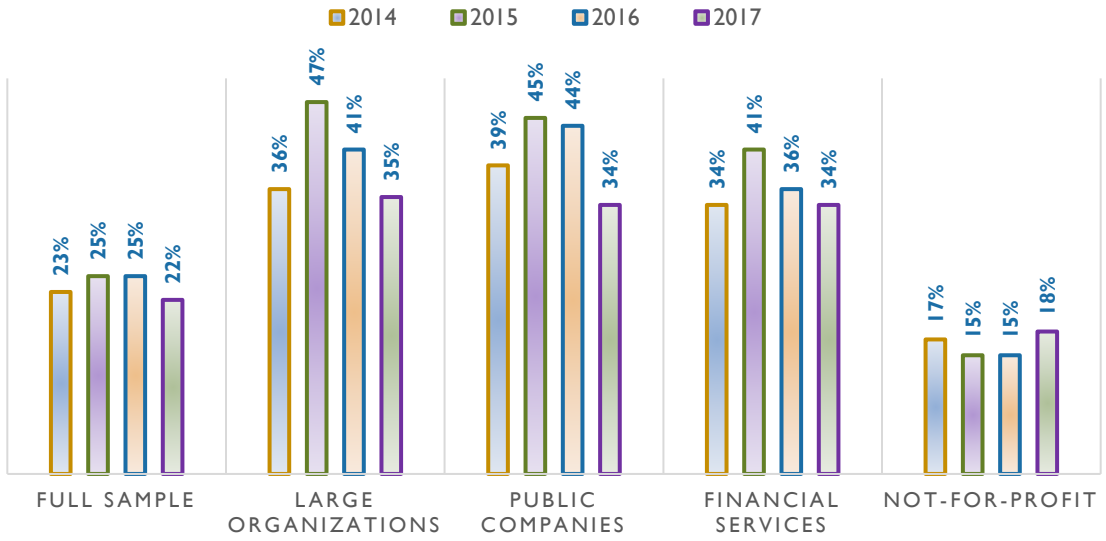
To get a sense for the overall sophistication of risk management practices, we asked a series of questions to tease out the state of risk management practices in organizations today. In particular, we asked respondents to provide their assessment of the overall level of their organization's risk management 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 about one-third of those responding to our survey. When asked to describe the level of maturity of their organization's approach to risk oversight, we found that 16% 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 39% self-describe the sophistication of their risk oversight as immature to developing (this is mostly unchanged from the 38% reported in our prior year study). Only 5% responded that their organization's risk oversight was "robust," consistent with responses noted in prior reports.

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

	Percentage of Respondents				
What is the level of maturity of your organization's risk management oversight?	Very Immature	Developing	Evolving	Mature	Robust
Full Sample	16%	23%	39%	17%	5%
Largest Organizations	6%	17%	42%	27%	8%
Public Companies	7%	19%	40%	25%	9%
Financial Services	8%	15%	43%	27%	7%
Not-for-Profit Organizations	11%	24%	47%	13%	5%

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 and the bar graph on the next page, respondents in larger organizations, public companies, and financial services organizations are more likely to describe their organization's approach to ERM as either "mature" or "robust" relative to the full sample and to not-for-profit organizations. That has been the case for the past few years.

Back To Agenda



While the level of risk oversight maturity is higher for these subsets of organizations than the full sample, 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.

This is especially intriguing given a majority of the respondents in the full sample indicated that their organization's risk culture is one that is either "strongly risk averse" (8%) or "risk averse" (45%). Similarly, just over one-half of the largest organizations, public companies, and financial services companies indicated their risk culture is "strongly risk averse" or "risk averse." The overall lack of ERM maturity for the full sample is somewhat surprising, when the majority of organizations are in organizations with notable aversion to significant risk-taking. The level of risk management maturity may not clearly reconcile to the organization's risk-averse culture.

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.

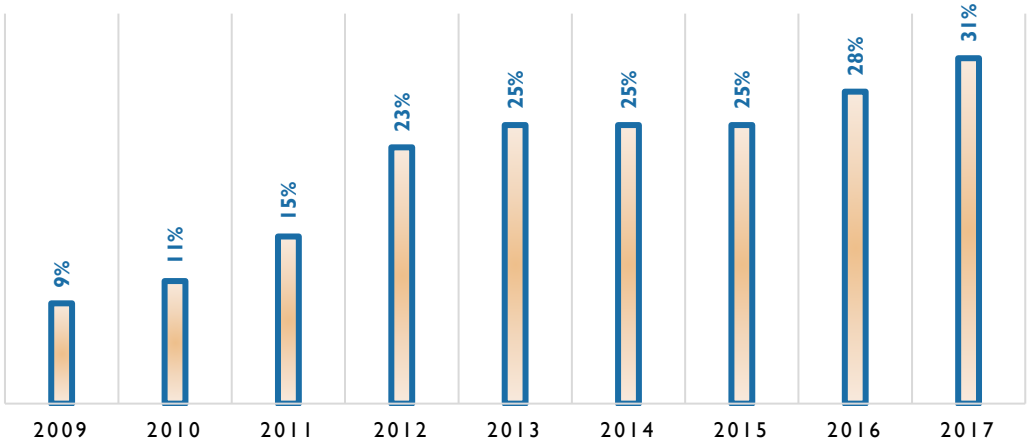
To obtain a sense for the current state of ERM maturity, we asked survey participants to respond to a number of questions to help us get a sense for the current level of risk oversight in organizations surveyed. One of the questions asked them to select from the following the best description of the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

Back To Agenda

- No enterprise-wide process in place
- Currently investigating 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

Over the past two years, there has been a slight uptick in 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, we did see a small increase in the number of organizations at that level of maturity for 2017 relative to 2016.

COMPLETE ERM IN PLACE: FULL SAMPLE



In 2009, only 9% of organizations claimed to have complete ERM processes in place; however, in 2017 the percentage increased to 31% for the full sample. So, greater adoption of ERM has occurred. However, there continues to be significant opportunity for improvement in most organizations, given that more than two-thirds of organizations surveyed in 2017 still cannot yet claim they have "complete ERM in place."

For the full sample, we found that 16% of the respondents have no enterprise-wide risk management process in place. An additional 9% 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, a quarter of respondents have no formal enterprise-wide approach to risk oversight and are currently making no plans to consider this form of risk oversight. That is a bit surprising as you consider the growing level of uncertainty in today's marketplace.

Back To Agenda

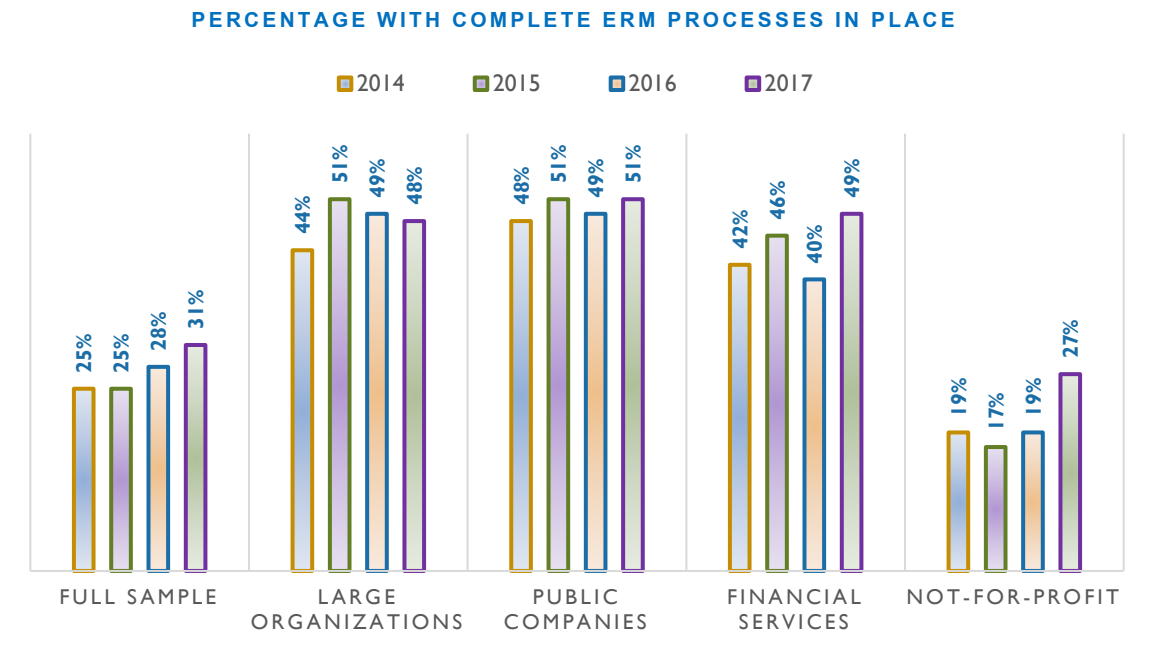
The adoption of ERM is greatest for larger companies, public companies, and financial services as summarized in the table below.

	Percentage of Respondents				
Description of the State of ERM Currently in Place	Full Sample	Largest Organizations (Revenues >$1B)	Public Companies	Financial Services	Not-For-Profit Organizations
No enterprise-wide management process in place	16%	4%	2%	7%	9%
Currently investigating concept of enterprise-wide risk management, but have made no decisions yet	9%	3%	4%	2%	13%
No formal enterprise-wide risk management process in place, but have plans to implement one	7%	5%	4%	4%	11%
Partial enterprise-wide risk management process in place (i.e., some, but not all, risk areas addressed)	37%	40%	39%	38%	40%
Complete formal enterprise-wide risk management process in place	31%	48%	51%	49%	27%

The chart on the next page shows that larger organizations, public companies, and financial services organizations are more likely to have complete ERM processes in place and that has been the case for the past few years. 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.

The adoption of ERM is much further along for large organizations, public companies, and financial institutions.

Back To Agenda



Back To Agenda

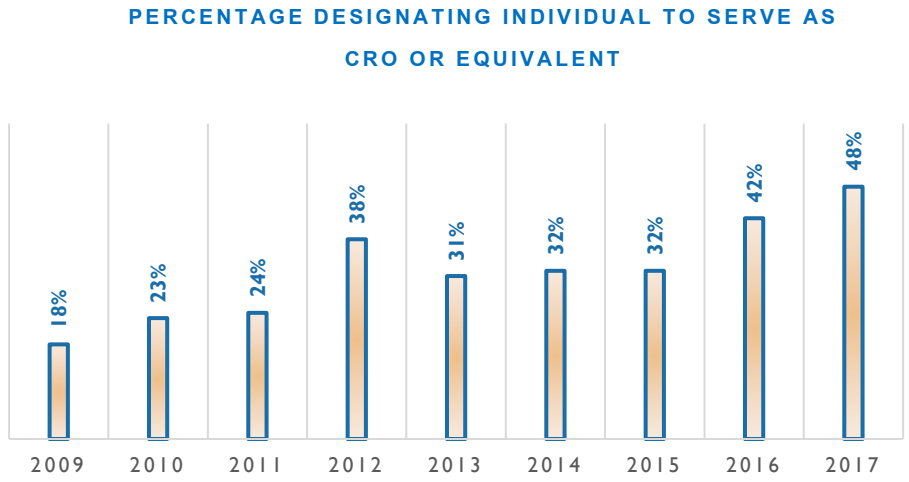
STRENGTHENING RISK MANAGEMENT INFRASTRUCTURE

- ***Higher percentages of organizations are appointing individuals to lead the organization's risk management process.***
- ***Even higher percentages of organizations are creating management-level risk committees.***
- ***Board of directors continue to delegate risk oversight to a board committee, which is most often the audit committee.***

Part of the challenge of ensuring that the risk management process is effectively integrated with strategy may be linked to the extent of executive leadership of the risk function. If risk management leaders are not at a level that is engaged in strategic planning, there may be a strategy and risk disconnect.

Large organizations, public companies, and financial services entities are similarly likely to appoint individuals to serve as Chief Risk Officer (CRO) or equivalent than other organizations.

The percentage of organizations formally designating an individual to serve as the Chief Risk Officer (CRO) or equivalent senior risk executive continues to increase, with almost half of the organizations surveyed now appointing individuals to lead the risk management role. Even over the past two years, the percentage of organizations with CROs or equivalent has grown from 32% to 48%, as illustrated by the bar chart below.

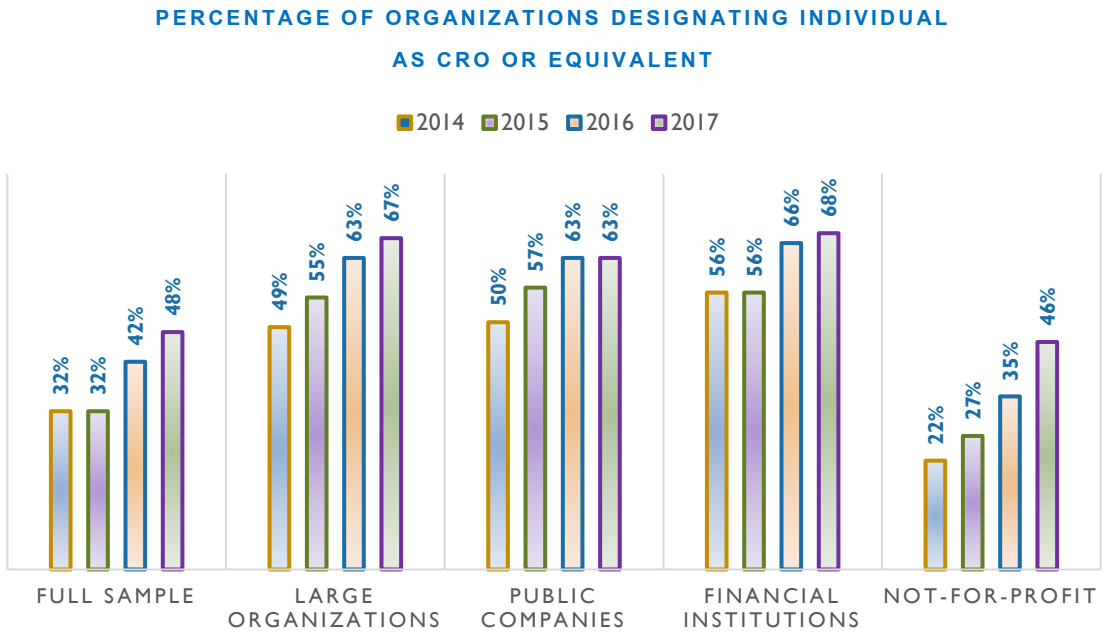


Large organizations, public companies, and financial services organizations are even more likely to have designated an individual to serve as CRO or equivalent, with more than two-thirds of those organizations doing so, as shown in the table on the next page.

Back To Agenda

	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	48%	67%	63%	68%	46%

The increase in the percentage of organizations designating an individual to serve as CRO or equivalent occurred across all types of organizations as shown in the bar graph below. Perhaps this is in response to the growing reality that the volume and complexities of risks are not getting easier to manage and require more focused risk management efforts. More organizations are concluding that leadership is needed to help management design and implement more robust risk management processes.



For firms with a chief risk officer position, the individual to whom the CRO most often reports is the CEO or President (42% of the instances for the full sample) followed by 20% that directly report to the CFO. Interestingly, in the prior year, 51% reported to the CEO or President while 15% reported to the CFO. Thus, there appears to be some realignment in reporting structures with more CROs reporting to the CFO in the current year than in prior years. For 23% of the organizations with a CRO position, the individual reports formally to the board of directors or its audit committee. Last year 21% reported to the board or one of its committees.

Back To Agenda

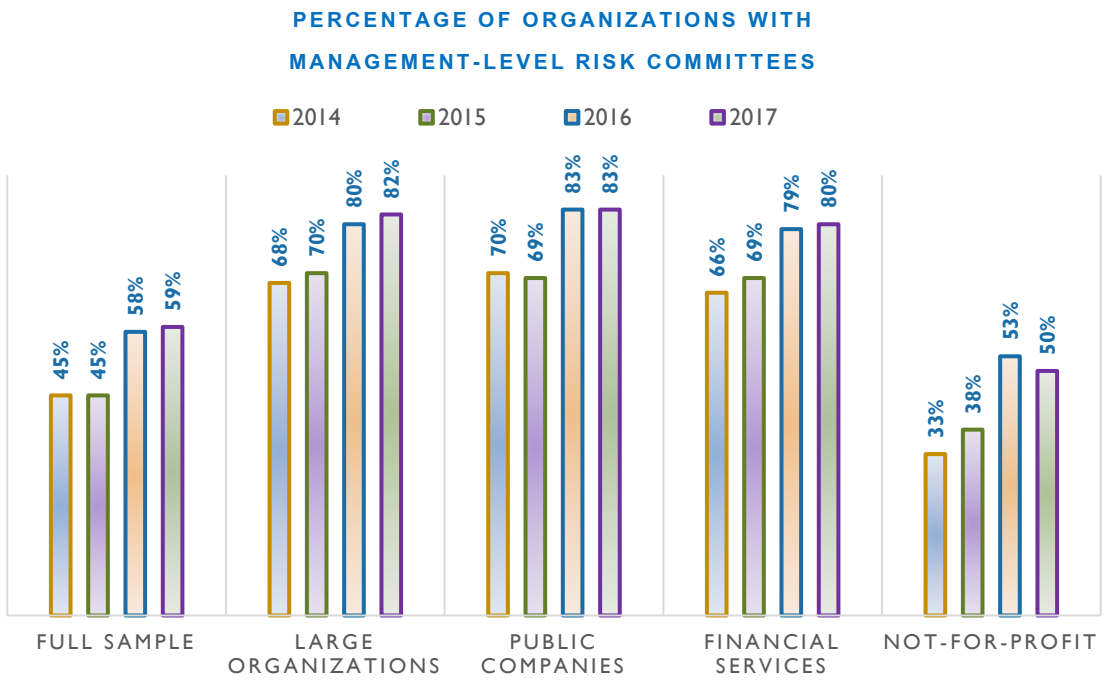
When you examine the largest organizations, public companies, and financial services entities separately, there are some notable differences as shown in the table below. Direct reporting to the CEO or President is most common; however, similar to the overall sample, we noticed a reduction from the prior year in percentages reporting to the CEO or President with more reporting to the CFO for large organizations, public companies, and not-for-profit organizations.

	Percentage of Respondents				
To Whom Does the CRO Formally Report?	Full Sample	Largest Organizations (Revenues >$1B)	Public Companies	Financial Services	Not-for-Profit Organizations
Board of Directors or Committee of the Board	23%	11%	24%	25%	19%
Chief Executive Officer or President	42%	40%	39%	59%	32%
Chief Financial Officer	20%	29%	22%	12%	23%

Similar to our observation that almost half (48%) of organizations are designating an executive to lead the risk oversight function (either as CRO or equivalent) in 2017, we also observed that a number of organizations have a management-level risk committee or equivalent. For 2017, 59% of the full sample has a risk committee as compared to 45% two years ago.

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 82%, 83%, and 80%, respectively, of those organizations had an internal risk committee. And, the increased use of a management-level risk committee was observed across all types of organizations as illustrated by the chart on the next page.

Back To Agenda



For the organizations with a formal executive risk oversight committee, those committees met most often (49% of the time) on a quarterly basis, with an additional 30% 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 77% of the risk committees that exist among organizations represented in our survey. The CEO/President serves on 56% of the risk committees while the chief operating officer serves on 52% of the risk committees. In around half 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.

It will be interesting to monitor whether overall ERM maturity advances in the next few years, given the increase in the percentage of entities creating a risk committee or designating someone to serve in a CRO role.

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.

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

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 57% of the

Back To Agenda

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 78%, 81%, and 74% 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, just under half (46%) are assigning that task to the audit committee. Almost one third of firms assign oversight to a risk committee. The largest organizations and not-for-profit organizations are most likely to assign formal risk oversight to the audit committee.

	Percentage of Respondents				
If board delegates formal responsibility of risk oversight to a subcommittee, which committee is responsible?	Full Sample	Largest Organizations (Revenues >$1B)	Public Companies	Financial Services	Not-for-Profit Organizations
Audit committee	46%	56%	48%	31%	54%
Risk committee	31%	24%	34%	51%	15%
Executive committee	8%	4%	2%	6%	8%

Back To Agenda

LINKING RISK OVERSIGHT AND STRATEGIC PLANNING

- ***The majority of organizations struggle to effectively integrate risk management with strategic planning efforts.***
- ***Only a small percentage of organizations view their risk management process as an important strategic tool.***
- ***Most organizations do not engage their board of directors in explicit discussions about top risk exposures as they discuss their strategic plans.***

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.

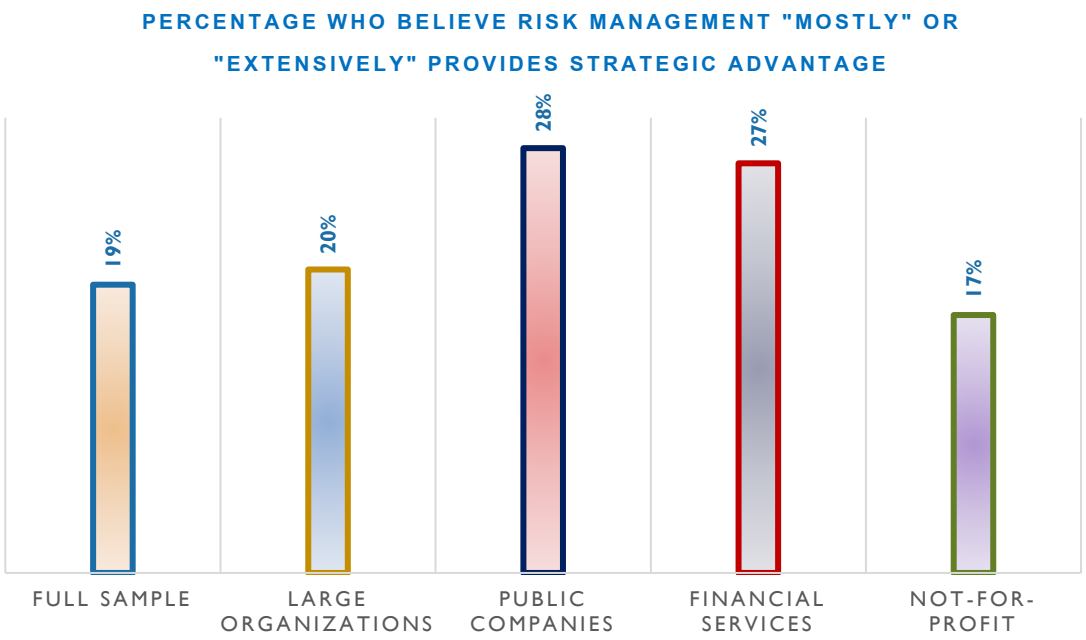
Better understanding of risks facing the organization should provide rich input to the strategic planning process so that management and the board can design strategic goals and initiatives with the risks in mind. If functioning effectively, a robust ERM process should be an important strategic tool for management.

Responses to the question about the extent to which respondents believe the organization's risk management process is a proprietary strategic tool that provides unique competitive advantage shed 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," consistent with what we observed in prior years. Organizations continue to struggle to integrate their risk management and strategic planning efforts.

	Percentage of Respondents				
	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?	28%	24%	29%	14%	5%

Furthermore, as shown by the bar graph on the next page, the assessment of the strategic value of the organization's risk management process was somewhat higher for public companies and financial services organizations; however, the percentage indicating that their risk management had "mostly" or "extensive" strategic value is still around one-third for public companies and financial services organizations. Thus, there may still 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.

Back To Agenda



We found that 32% of organizations in our full sample currently do only minimal or 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 39% 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 18%, 15%, and 17% of those organizations, respectively, signaled that they have no or only minimal formal assessments of these kinds of emerging risks.

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

When organizations formally assess risks, most do so in a predominantly qualitative (17%) manner or by using a blend of qualitative and quantitative assessment tools (54%). 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 (41%) of our respondents believe that existing risk exposures are considered "mostly" or "extensively" when evaluating possible new strategic initiatives and about 30% 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, 31% of the respondents indicate that risk exposures are considered "mostly" or "extensively" when making capital allocations to functional units.

Back To Agenda

	Percentage of Respondents Saying "Mostly" or "Extensively"				
Extent that	Full Sample	Largest Organizations (Revenues >$1B)	Public Companies	Financial Services	Not-for-Profit Organizations
Existing risk exposures are considered when evaluating possible new strategic initiatives	41%	38%	47%	51%	44%
Organization has articulated its appetite for or tolerance of risks in the context of strategic planning	29%	32%	38%	47%	21%
Risk exposures are considered when making capital allocations to functional units	31%	32%	40%	37%	31%

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, just under 30% 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 just under 30% 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.

	Percentage of Respondents				
Extent to which top risk exposures are formally discussed by the Board of Directors when they discuss the organization's strategic plan	Full Sample	Largest Organizations (Revenues >$1B)	Public Companies	Financial Services	Not-for-Profit Organizations
"Extensively"	8%	12%	30%	26%	21%
"Mostly"	21%	24%	15%	13%	5%
Combined	29%	36%	45%	39%	26%

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.

Back To Agenda

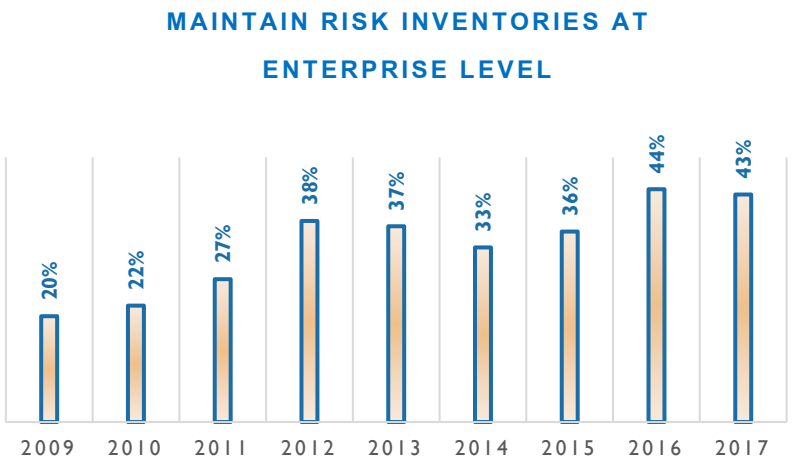
STATUS OF KEY ELEMENTS OF A RISK MANAGEMENT PROCESS

- ***More organizations are maintaining inventories of risks at the enterprise level and most organizations are attempting to update their understanding of key risks at least annually.***
- ***Larger companies, public companies, and financial services organizations have more formalized risk management processes, although there are signs this is increasing for other types of organizations as well.***

Just under half of the organizations in the full sample (45%) 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 (61%), public companies (68%), and financial services entities (69%), where regulatory and best practice expectations have a greater influence. Not-for-profit organizations are least likely to have a formal policy in place (only 37% do), which may be partially attributable to the lack of external influences related to risk management.

Percentage of Respondents					
	Full Sample	Largest Organizations (Revenues >$1B)	Public Companies	Financial Services	Not-For-Profit Organizations
Organization has a formal policy statement regarding enterprise-wide approach to risk management	45%	61%	68%	69%	37%

A higher percentage of organizations now maintain inventories of risks at the enterprise level than in prior years, as illustrated by the bar graph below. In 2017, 43% of the organizations now maintain enterprise-level risk inventories compared to 36% two years ago. When compared to 2009, we definitely see more awareness of the importance of maintaining an understanding of the universe of risks facing the organization.



The majority of the large organizations (79%) and public companies (80%) have a standardized process or template for identifying and assessing risks, while 66% of the financial services organizations have those kinds of procedures in place. In contrast, only 54% of not-for-profit organizations structure their risk identification and assessment processes in that manner.

Back To Agenda

A greater percentage of large organizations, public companies, and financial services firms maintain risk inventories at the enterprise level as shown in the table 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	43%	58%	62%	58%	48%

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 or semi-annually.

Percentage of Respondents					
Frequency of Going Through Process to Update Key Risk Inventories	Full Sample	Largest Organizations (Revenues >$1B)	Public Companies	Financial Services	Not-for-Profit Organizations
Not at all	25%	11%	7%	10%	29%
Annually	36%	51%	41%	39%	45%
Semi-Annually	12%	12%	13%	14%	11%
Quarterly	19%	19%	30%	27%	11%
Monthly, Weekly, or Daily	8%	7%	9%	10%	4%

Half (50%) 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, 28% focus their definition on “downside” risks (threats to the organization) and just over one-third (37%) focus on both the “upside” (opportunities for the organization) and “downside” of risk.

About 40% of the full sample provides explicit guidelines or measures to business unit leaders on how to assess the probability and impact of a risk event (43% and 40%, respectively). We found similar results for not-for-profit organizations. However, consistent with 2016 almost two-thirds 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 public companies are the most likely to provide this guidance. In 2017, 68% and 62% of public companies provide guidelines for assessing risk probabilities and impact, respectively.

Percentage of Respondents					
Percentage that provide guidelines to assess risk	Full Sample	Largest Organizations (Revenues >$1B)	Public Companies	Financial Services	Not-For-Profit Organizations
- Probability	43%	62%	68%	56%	39%
- Impact	40%	58%	62%	55%	35%

Back To Agenda

AGGREGATING RISK INFORMATION FOR ENTERPRISE VIEW

- ***Most organizations provide a formal report of top risk exposures to the board of directors at least annually.***
- ***Nearly three-fourths of respondents indicate that their board of directors discusses at a specific meeting the top risk exposures facing the organization.***
- ***Between one-half and two-thirds of large organizations, public companies, and financial services organizations describe their processes to report top risks to the board as systematic, robust, and repeatable. That drops to one-third for not-for-profit organizations.***

We asked respondents about their current stage of risk management processes and reporting procedures. More than one-third (36%) 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 26% describe their risk management processes as informal and unstructured with *ad hoc* reporting of aggregate risk exposures to the board.

Interestingly, however, just over one-third (38%) 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 2016 report (35%) and our 2015 report (33%).

Percentage of Respondents					
Percentage who describe their ERM implementation as	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.	38%	55%	62%	57%	33%

Thus, while a majority of organizations in our full sample 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.

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

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, about half (53%) of organizations communicate key risks merely on an *ad hoc* basis at management meetings. Only 30% 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 nine years we have tracked this data point (30% in 2016, 27% in 2015, 27% in 2014, 34% in 2013, 33% in 2012, 33% in 2011, 29% in 2010 and 2009).

Back To Agenda

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
Ad hoc discussions at management meetings	53%	37%	33%	39%	52%
Scheduled agenda discussion at management meetings	30%	41%	39%	37%	33%
Written reports prepared either monthly, quarterly, or annually	49%	76%	82%	74%	37%

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

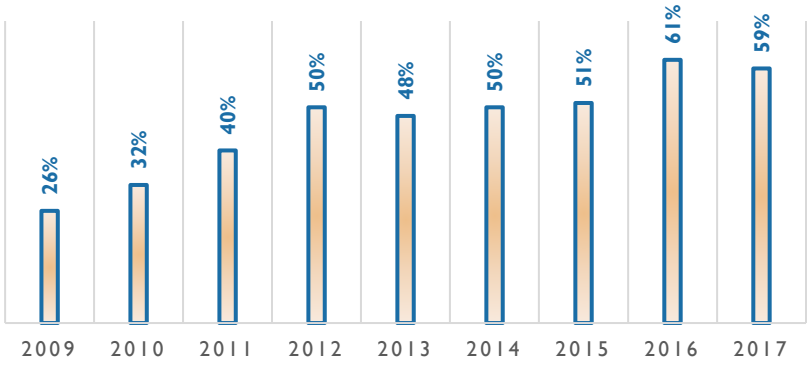
Surprisingly, just over half (55%) of those in the full sample indicate that the full board formally reviews and discusses the top risk exposures in a specific meeting of the board. This is much more likely for boards of the largest organizations, public companies and financial services organizations.

Percentage of Respondents					
Percentage of organizations where the	Full Sample	Largest Organizations (Revenues >$1B)	Public Companies	Financial Services	Not-for-Profit Organizations
Board of Directors reviews and discusses in a specific meeting the top risk exposures facing the organization	55%	72%	75%	72%	43%

As illustrated by the graph below, 59% 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. This is noticeably higher than the percentages doing so in 2009 when we found that only 26% of organizations provided that kind of information to the board at least annually. Two years ago, that percentage was 51% but a higher percentage of management teams are doing so in the most recent two years.

Back To Agenda

PROVIDE FORMAL REPORT TO BOARD DESCRIBING TOP RISK EXPOSURES AT LEAST ANNUALLY

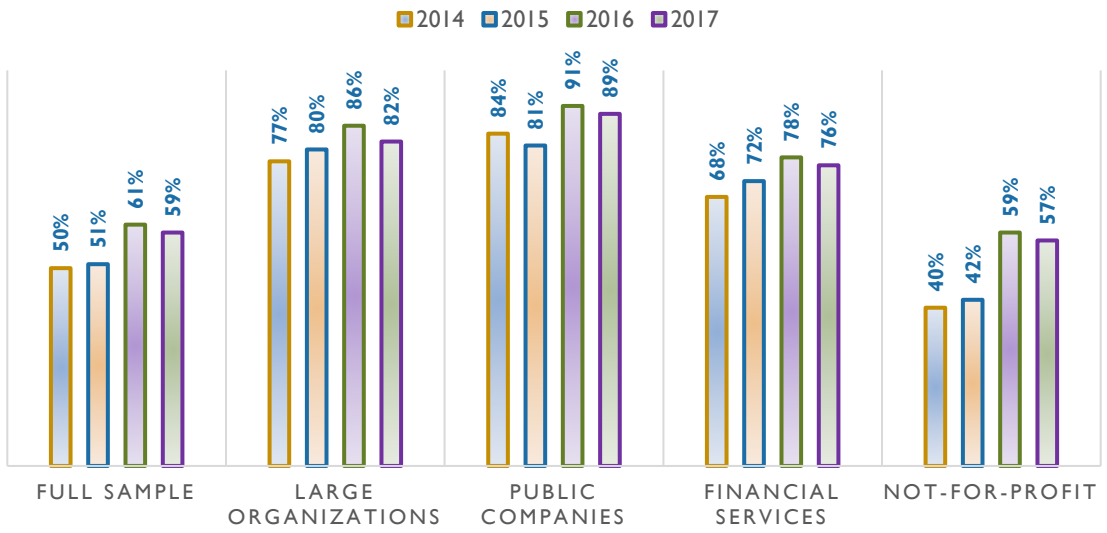


As illustrated by the table below, an overwhelming percentage (82%) of large organizations and public companies (89%) formally report top risk exposures to the board of directors or one of its committees at least annually. In 2017, over three-fourths (76%) of financial services organizations also formally report top risk exposures to the board; also 57% of 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 formally report top risk exposures to the board at least annually	59%	82%	89%	76%	57%

Formal reporting of top risks to the board at least annually has been gradually increasing across all organizations over the past three years. In light of this, boards and management teams may benefit from evaluating the robustness of the underlying risk management processes that management is using to identify and assess risks for reporting to the board.

Back To Agenda



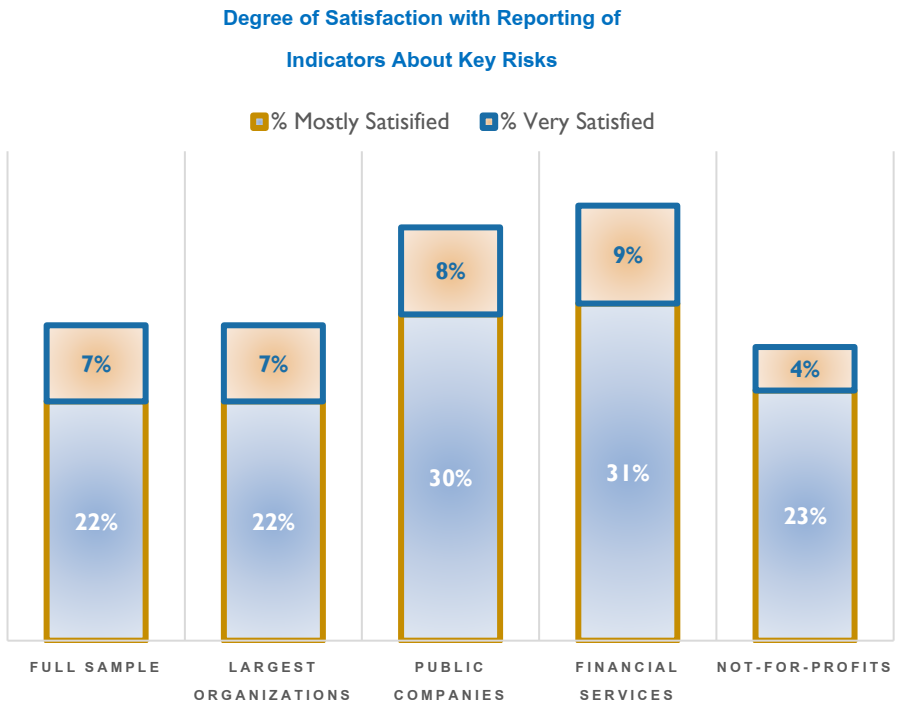
We also asked about the number of risk exposures that are typically presented to the board or one of its committees. As illustrated in the table below, just over one third of the full sample and not-for-profit organizations report less than five risk exposures to the board. However, about 70% of the large organizations, public companies, and financial services organizations formally report between 5 and 19 risks to the board.

	Percentage of Respondents				
Percentage of organizations reporting the following number of risk exposures to the board of directors or one of its committees:	Full Sample	Largest Organizations (Revenues >$1B)	Public Companies	Financial Services	Not-for-Profit Organizations
Less than 5 risks	37%	15%	12%	20%	38%
Between 5 and 9 risks	25%	26%	22%	37%	19%
Between 10 and 19 risks	31%	45%	54%	33%	38%
More than 20 risks	7%	14%	12%	10%	5%

Overall, there seems to be room for improvement in the nature of risk information being reported to senior executives. Given the lack of available data, finding good metrics to monitor emerging risks can be challenging, and entities appear to be struggling to find effective measures that they can use to help them monitor top risk exposures. 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 internal reporting of key risk indicators (known as KRIs) to senior executives. Similar levels of dissatisfaction, 41% and 41%, were observed in our 2016 and 2015 reports, respectively. In contrast, only 29% are “mostly satisfied” or “very satisfied” with the nature and extent of internal reporting of key risk indicators to senior executives. The growing use of data analytics may provide opportunities

Back To Agenda

for management to strengthen their management "dashboards" to include more information that helps track potential risks on the horizon.



While respondents for public companies and financial services organizations signal a greater level of satisfaction about the nature and extent of reporting of key risk indicators, that level of satisfaction is still not greater than 40%, which suggests that majority of all types of organizations see room for improvement in their 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 just 20% believed their disclosures had changed "mostly" while an additional 11% 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 37% and "extensively" for 28%. When taken together, these findings are interesting in that 65% of respondents perceive that the volume and complexity of risks has changed mostly or extensively in the past five years, but only 31% have seen changes in the nature of their risk disclosures to investors. That may cause some to wonder whether the required Form 10-K Item 1.A risk factor disclosures that describe key risks affecting the company provide a realistic view of the risk profiles of the organizations.

Back To Agenda

PROVIDING INCENTIVES FOR RISK OWNERSHIP

- ***Few organizations are explicitly incorporating risk management activities into compensation plans.***

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, 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 incentivized 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.

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

We asked respondents about the extent to which risk management activities are an explicit component of determining management performance compensation. We found that in 36% of the organizations surveyed, risk management is "not at all" a component of the performance compensation and for another 30% the component is only "minimally" considered. Thus, in two-thirds of the organizations surveyed (66%), the extent that risk management activities are an explicit component in determining management compensation is non-existent or minimal. These findings are similar to what we observed last year.

Percentage of Respondents					
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	36%	32%	25%	20%	48%
Minimally	30%	30%	27%	36%	27%
Combined	66%	62%	52%	56%	75%

Even public companies and financial services are unlikely to factor risk management activities into performance compensation, generally around one-half of 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.

Back To Agenda

PINPOINTING CHALLENGES TO ENHANCED RISK OVERSIGHT

- ***A number of barriers to strengthening ERM processes exist that may need to be addressed before real advancement in risk oversight is realized.***

While our analysis suggests that organizations have made significant progress 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 more rapid advances 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 48% 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?"*

Other responses were "no requests to change our risk management approach" and "do not see benefits exceeding costs," noted by 36% and 23%, respectively, of respondents in the full sample. Twenty-nine percent of those same respondents also noted that there are "too many pressing needs" while 26% 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. This is somewhat surprising given 38% of the full sample describe their risk oversight processes as very immature or just developing, 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 (57%) relative to the full sample noted that competing priorities are the primary barrier to their embrace of ERM.

Back To Agenda

	Percentage Believing Barrier is		
Description of Barrier	"Barrier"	"Significant Barrier"	Combined Percentage
Competing priorities	29%	18%	47%
Insufficient resources	27%	17%	44%
Lack of perceived value	24%	15%	39%
Perception ERM adds bureaucracy	19%	11%	30%
Lack of board or senior executive ERM leadership	18%	11%	29%
Legal or regulatory barriers	4%	2%	6%

Most organizations (57%) 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 slightly lower for the largest organizations (53%), public companies (44%), and financial services (41%). 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.

Back To Agenda

CALLS TO ACTION

The environment in which organizations operate contains a number of complex issues that boards of directors and management must navigate. Geopolitical events, innovation, technological advancements, immigration policy issues, tax law changes, shifts in social demographics and consumer tastes, cyber threats, low interest rates and unemployment, are just a few of the complex issues that may trigger opportunities or risks for an enterprise. Most believe the pace of change in these drivers will only increase. If organizations are not prepared to navigate this rapidly escalating volume and complexity of risks, they may lack the resiliency and agility needed to successfully survive in the highly competitive global business environment.

While the findings in this study indicate some slowly progressing improvements in how organizations are proactively managing risks on the horizon, many of the findings suggest boards of directors and management should consider more aggressive action to ramp up their organization's infrastructure surrounding risk oversight:

- **Be honest about the organization's risk management capabilities.** Given most respondents indicate that the risk landscape is increasing significantly in volume and complexity, why are only one-quarter of them describing their risk management as "mature" or "robust"? An organization's leaders may want to evaluate whether the current level of their organization's risk management maturity is capable of keeping pace with emerging risks.
- **Find ways to connect risk management and strategic planning.** Business leaders understand that as they seek to generate a higher return, they must be willing to take more risks. However, a small percentage of respondents believe their organizations' risk management process is providing strategic value. This may be due to the finding that less than half of the organizations formally consider existing risk exposures when evaluating new possible strategic opportunities and less than one-third of the organizations have their boards of directors formally discuss risk exposures when they discuss the strategic plan. Boards and management may want to consider how they can more explicitly integrate their risk management efforts with their strategic planning efforts. Doing so may help leaders see the strategic value and power of having better intelligence about risks on the horizon.
- **Challenge the basis for identifying risk information reported to boards and others.** While almost 60% of organizations provide a formal report to the board describing top risk exposures at least annually, only 43% of those organizations maintain risk inventories at the enterprise level. If management is not maintaining an inventory of its top enterprise-level risks, what is the basis for their formal report about risks provided to the board? Boards of directors may want to inquire of management about the processes that management has in place to prepare the top risk report for the board. Is there sufficient basis for the information provided?
- **Expand management dashboards to include risk indicators.** Sixty percent of organizations surveyed believe the volume and complexity of risks has increased "mostly" or "extensively" in the past five years. Unfortunately, less than 30% of respondents in those organizations are "mostly satisfied" or "very satisfied" with the reporting of indicators about key risks. Boards and management teams may want to consider how they can strengthen their performance dashboards to include more indicators that are focused on emerging risks.
- **Find ways to incentivize management to invest in risk management.** Almost two-thirds of respondents in organizations surveyed indicate that a number of external parties are applying pressure on senior executives to provide more information about risks affecting the organization. Typically, the board of directors is one group

Back To Agenda

that is asking for more senior management involvement in risk oversight. However, the level of risk management maturity seems to be only slowly improving. Perhaps that is due to the fact that almost two-thirds of those organizations do not include risk management activities as a component for determining management's performance compensation. Boards of directors may want to focus more attention on how they can place more accountabilities on executives for risk management responsibilities.

- **Provide training and education on the value of robust, proactive risk management.** There are a number of barriers that inhibit progress in risk management improvements in organizations. Perceptions that investing in risk management is a competing priority relative to other organizational initiatives or perceptions that managing risks lacks value may signal a lack of understanding about how effective risk oversight may actually improve the organization's ability to proactively and resiliently navigate emerging risks. This lack of understanding may be due to the finding that almost 60% of the organizations surveyed provide no training and guidance on risk management. Business leaders may want to invest in fundamental training on the role risk management can play in helping them achieve their strategic objectives.

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 and the AICPA's ERM Web site). 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.

Back To Agenda

APPENDIX A: OVERVIEW OF RESPONDENT DEMOGRAPHICS

This is the ninth 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) Management Accounting - Business, Industry, and Government Team. Data was collected during the fall of 2017 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 474 fully completed surveys. This report summarizes our findings.

Results are based on responses from 474 executives, mostly serving in financial leadership roles, representing a variety of industries and firm sizes.

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 are the same across all nine of our editions of the surveys that we have conducted each year from 2009 - 2017. 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.

A variety of executives participated in our survey, with 22%[1] of respondents having the title of chief financial officer (CFO), 14% serving as chief risk officer (CRO), 12% as controller, and 8% leading internal audit, with the remainder representing numerous other executive positions.

Nature of Organizations Represented

The respondents represent a broad range of industries. Consistent with our prior year survey, the four most common industries responding to this year's survey were finance, insurance, and real estate (29%), followed by not-for-profit (23%), manufacturing (15%), and services (15%).The mix of industries is generally consistent with the mix in our previous reports.

[1] Throughout this report we have rounded the reported percentages to the nearest full percent for ease of discussion.

Back To Agenda

Industry (SIC Codes)	Percentage of Respondents
For-Profit Entities:	
Finance, Insurance, Real Estate (SIC 60-67)	29%
Manufacturing (SIC 20-39)	15%
Services (SIC 70-89)	15%
Wholesale/Distribution (SIC 50-51)	5%
Construction (SIC 15-17)	5%
Retail (SIC 52-59)	4%
Mining (SIC 10-14)	2%
Transportation (SIC 40-49)	2%
Not-for-Profit (SIC N/A)	
Government Agencies, Universities, Non-Profits	23%

The respondents represent a variety of sizes of organizations. As shown in the table below, about two-thirds (62%) of organizations that provided data about their financial performance generated revenues up to $500 million in their most recent fiscal year.[2] An additional 9% generated revenues between $500 million and $1 billion while 29% of organizations providing revenue data earned revenues in excess of $1 billion. Almost all (80%) of the organizations are based in the United States.

Range of Revenues in Most Recent Fiscal Year	Percentage of Respondents
$0 <x ≤ $10 million	12%
$10 million < x ≤ $100 million	31%
$100 million < x ≤ $500 million	19%
$500 million < x ≤ $1 billion	9%
$1 billion < x ≤ $2 billion	7%
$2 billion < x ≤ $10 billion	12%
x > $10 billion	10%

Throughout this report, we highlight selected findings that are notably different for the 130 largest organizations in our sample, which represent those with revenues greater than $1 billion. Additionally, we also provide selected findings for the 138 publicly-traded companies, 137 financial services entities, and 103 not-for-profit organizations included in our sample.

[2] Thirty-one of the 474 respondents did not provide information about revenues.

Back To Agenda

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. Currently, he is a member of the United Nation's Internal Control Advisory Group. He consults with 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 an Alumni Distinguished 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 has chaired the risk policy and credit committees and currently serves on the governance 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 the compensation committee.

Contact us at: erm_initiative@ncsu.edu or 919.513.0901.

NC STATE Poole College of Management
Enterprise Risk Management Initiative

Back To Agenda

Board of Trustees

Audit, ERM, Compliance, and Ethics Committee Meeting

April 19, 2018

Agenda Item:	V.A. Information Security
Responsible Person:	Don Sweet
Action Requested:	None - Information
Notes:	N/A

Back To Agenda

ECU Board of Trustees
Audit, ERM, Compliance, & Ethics Committee

April 19, 2018

Information Security

-Don Sweet, CIO

New UNC Information Security Policy

- Adopted January 26, 2018
- To establish an Information Security Program AND
- Designate a senior officer accountable to the Chancellor, Board of Governors, and Board of Trustees to oversee Information Security (Don Sweet, CIO)
- Present to the Board of Trustees at least annually on information security matters

Back To Agenda

General Data Protection Regulation
(GDPR)
Effective May 25, 2018

- New data protection law for processing the personal data of individuals located within the 28 countries comprising the European Union.
- Must be compliant by May 25, 2018.
- Has specific rules that we must adhere to that are different than U.S. data privacy laws:
  - Must acquire & track formal consent from individuals
  - Right to be forgotten
  - Right of access to the data by the individuals

ECU

General Data Protection Regulation
(GDPR)

Who is affected:

- ECU students in study abroad programs
- ECU Faculty and those hired w/in the EU
- Third-parties: contractors, donors w/in the EU
- EU students taking online ECU courses from w/in EU
- EU students playing sports for ECU
- ECU researchers sharing personal data with the EU

ECU

Back To Agenda

General Data Protection Regulation (GDPR)

Failure to comply with the GDPR:

- Financial penalties up to $24M or 4% annual revenue *(whichever is greater)*
- Penalties imposed by National Data Protection Agency
- Reputational damage to ECU
- **Note:** *The National Data Protection Agency can request a compliance audit at any time. However, it appears that U.S. institutions **may** not be audited for a couple of years as they will concentrate on those entities within the EU itself first.*

ECU

ECU Security Improvements

Multi-Factor Authentication

- Requires more than 1 method of identification to verify a user's identity during login
- Purpose is to further protect ECU's assets
- Summer 2017: 1,000+ users fall victim to phishing schemes causing accounts to get disabled

ECU

Back To Agenda

ECU Security Improvements

Implementing 2-Factor Email Authentication
(ONLY required when off campus)

- Phase 1: Students by mid-April 2018
- Phase 2: Faculty & Staff Fall 2018

ECU

ECU Security Improvements

Mandatory Employee Training

- Security training required for all employees within first 30 days, refresher training every 2 years
- Online Cornerstone course, completions recorded in the official employee training transcript
- Supervisors monitor employee participation via Cornerstone
- 94.2% of employees have completed the course

ECU

Back To Agenda

Fun ECU Email Tidbits

During the month of February 2018:

- **15,374,351**: Emails stopped from entering our front door *(spam, virus, malware, malicious URLs, etc.)*
- **1,953,244**: Emails sent to ECU employees marked as marketing, social networking and bulk messages
- **2,694,417**: Emails considered to be "clean" *(in addition to the previous bullet)*
- **1,914,840**: Total number of emails sent out by ECU employees

ECU

End of Presentation

ECU

Back To Agenda

Board of Trustees

Audit, ERM, Compliance, and Ethics Committee Meeting

April 19, 2018

Agenda Item:	VI. Closed Session
Responsible Person:	Kel Normann, Chair
Action Requested:	
Notes:	N/A

Back To Agenda

Board of Trustees

Audit, ERM, Compliance, and Ethics Committee Meeting

April 19, 2018

Agenda Item:	VII. Other Business
Responsible Person:	Kel Normann, Chair
Action Requested:	
Notes:	N/A

Back To Agenda