2023
THE STATE OF RISK OVERSIGHT
AN OVERVIEW OF ENTERPRISE RISK MANAGEMENT PRACTICES

14TH EDITION | JUNE 2023

MARK S. BEASLEY
ALAN T. DICKSON DISTINGUISHED PROFESSOR
DIRECTOR, ERM INITIATIVE

BRUCE C. BRANSON
ALUMNI DISTINGUISHED PROFESSOR OF ACCOUNTING
ASSOCIATE DIRECTOR, ERM INITIATIVE

AICPA®

NC STATE Poole College of Management
Enterprise Risk Management Initiative

ABOUT THIS STUDY

In light of evolving challenges linked to ongoing geopolitical turmoil, social change, economic volatility, disruptive technologies, environmental expectations, and a host of other uncertainties, innovative and forward-looking business leaders are strengthening how they proactively manage potentially emerging risks that can quickly derail their organization's strategic objectives and goals. Failure to anticipate changing uncertainties can quickly trigger a flow of risks that significantly impact business models and strategic plans.

Managing risks before they occur and in the context of what is strategically important can provide incredible competitive advantage, if done so more effectively than others in the marketplace. This occurs by strengthening their organizations' processes surrounding the identification, assessment, management, and monitoring of risks most likely to impact – both positively and negatively – the entity's strategic success.

Over the past two decades, governance and strategy best practice advocates have been encouraging boards and C-suite executives to embrace enterprise risk management (ERM) practices to provide an organization's leadership 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 strategic objectives.

We have partnered for more than a decade 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. Data was collected in winter/early spring 2023 through an online survey instrument sent to members of the AICPA's Management Accountants in Business and Industry group who serve in chief financial officer or equivalent senior executive positions.

This 14th Edition of our report reflects insights from **454** fully completed surveys from individuals representing different sizes and types of organizations (see Appendix A for details about respondents). This report provides a snapshot of the state of risk oversight maturity and includes a number of probing questions for executives and boards to use to assess the relative strength of their risk governance efforts.

Readers of this report can use the findings to benchmark their organization's approach to risk oversight against current practices. In addition to highlighting key findings for the full sample of 454 respondents, we also separately report many of the key findings for the following subgroups of respondents (Note: some organizations are included in more than one category, therefore the sum of these exceeds 454):

- 130 large organizations (those with revenues greater than $1 billion)
- 94 publicly traded companies
- 119 financial services entities
- 121 not-for-profit organizations

The following page provides an overview of the various aspects of an organization's risk management process that we examine, which is followed by a high-level summary of key take-aways from our research. The remainder of the report provides more detailed information about other key findings and related implications for risk oversight.

MARK S. BEASLEY
Alan T. Dickson Distinguished Professor
Director, ERM Initiative

BRUCE C. BRANSON
Alumni Distinguished Professor of Accounting
Associate Director, ERM Initiative

The ERM Initiative in the Poole College of Management at North Carolina State University provides thought leadership on enterprise risk management (ERM) and its integration with strategic planning and corporate governance, with a focus on helping boards of directors and senior executives gain strategic advantage by strengthening their oversight of all types of risks affecting the enterprise. Our website (https://www.erm.ncsu.edu) includes an ERM library that contains summaries of over 600 ERM resources. Additional ERM resources are also available at https://www.aicpa-cima.com.

OVERVIEW OF TOPICS ADDRESSED IN THIS STUDY

Our survey asked participants to respond to over 40 questions that address a number of aspects related to their organization's risk oversight processes. The data in this report summarizes key insights related to the following components of an organization's enterprise-wide risk management approach:

At the beginning of each of the sections, we present questions readers can consider as they review the findings summarized in that section. Those questions prompt readers to consider various aspects of their own organization's risk oversight processes as they review the benchmarking information. For each of the above topics, we subdivide the discussion into a number of subtopics. We provide "Key Insights" that highlight the primary take-aways we observe from the data.

The report concludes with a number of "Calls to Action" (see page 60) that include several questions that ERM leaders can use to identify opportunities for improvements in their organization's risk management processes. The Calls to Action encourage readers to consider questions related to these issues:

1. What are management's perceptions about the current approach to risk management?
2. Is there consensus about the most significant enterprise risks?
3. How is the output from risk management used in strategic planning?
4. Does management have access to robust key risk indicators?
5. Is our entity sufficiently prepared to manage a significant risk event?

EXECUTIVE SUMMARY OF KEY INSIGHTS

While this report provides detailed insights about specific dimensions of risk oversight practices, here are five overarching themes suggested by this year's aggregated findings:

5 Themes:

1. **Risk management processes may not be keeping pace with realities in the global business environment.** The broader business context is becoming increasingly complex and organizations are facing significant operational disruptions from risk events they have inadequately considered. While two-thirds of respondents describe the volume and complexity of risks as higher than prior levels, less than one-third describe their risk management processes as mature or robust. That suggests a disconnect between risk management capabilities and needs.

2. **Stakeholders are expecting business leaders to "up their game" in regards to how they anticipate and manage risks.** Boards of directors, regulators, and shareholders are pressuring management to strengthen their organization's resiliency and governance of organizational continuity. Unfortunately, the organization's leadership and culture may not see risk management as an important priority for their organization. Many leaders believe risk management is a distraction. The "tone at the top" may not be sufficiently embracing the value and relevance of risk management in the context of the organization's strategic success. Many tend to view risk management as bureaucratic and non-value adding.

3. **Entities struggle to integrate risk management and strategic oversight.** While executives appreciate the reality that risk and return are interconnected, most respondents do not view their organization's risk management efforts as providing strategic insight. A majority of respondents indicate their risk management processes are not focused on assessing emerging strategic, market, and industry risks. Instead, the focus is on more traditional internally focused risks related to IT, financial reporting, operations and compliance.

4. **Fundamental risk management elements are in place, but there is room for enhancing risk metrics to monitor emerging risks from both internal and external drivers.** There has been a surge in the creation of management level risk committees to help management monitor risks across the enterprise and many organizations have standardized templates to help them assess risk probabilities and impact of various risks. Despite that, only 28% describe their key risk indicators (KRIs) to monitor risks as robust and insightful for strategic decision making and most risk management processes are based on qualitative rather than quantitative approaches.

5. **Risk governance is an important responsibility for the full board of directors; however, most delegate that to a subcommittee.** Most organizations report risks to the board on an annual rather than a quarterly or more frequent basis, despite the ever-changing nature of the global risk environment. Only one-quarter of respondents believe risk information generated by the organization's ERM process is formally discussed by the full board of directors when it discusses the strategic plan. Rich insights about the interconnected nature of risks and their impact on the strategy of the organization should be a primary and regular input to overall board discussions and governance.

The following pages provide more specific highlights of a number of key findings from this year's survey results.

EXECUTIVE SUMMARY OF KEY INSIGHTS

DRIVERS FOR ENHANCED RISK MANAGEMENT	**Several factors are leading to calls for better risk management:** ▪ The volume and complexities of risks remain at high levels as organizations continue to deal with challenges related to the economy and inflation, geopolitical uncertainties affecting trade and supply chains, continual threats related to cyber security and privacy, and the conflict in Eastern Europe among a host of other risk triggers – no type of organization or industry is immune to risk. ▪ A large majority of organizations have experienced a significant operational surprise in the past five years, which may signal existing deficiencies in their enterprise-wide risk management processes. ▪ Strengthening organizational resiliency is a priority among many leaders, as risk events continue to unfold at record pace. There is need for real change in how organizations govern business continuity and crisis management. ▪ Shifting stakeholder expectations for organizations to improve their oversight of risks may be creating pressures for senior executives to be better prepared when unexpected risk events emerge to avoid being surprised. ▪ Individuals who serve on the board of directors are increasing their calls for effective risk management.
OVERALL STATE OF RISK MANAGEMENT MATURITY	**Existing enterprise-wide risk management processes may not be keeping pace with the realities of the fast-changing risk environment:** ▪ More than two-thirds of organizations surveyed still cannot claim they have "complete ERM in place." ▪ Fewer than half of respondents describe their organizations' approach to risk management as "mature" or "robust" here after despite the perception among over two-thirds of the respondents that the volume and complexity of risks has increased noticeably. ▪ Just over one-half of the public companies surveyed do not describe their risk management processes as robust or mature. Non-profit organizations are less likely to have structured risk management processes relative to other organizations.

EXECUTIVE SUMMARY OF KEY INSIGHTS

STRATEGIC VALUE OF RISK MANAGEMENT	**Organizations struggle to integrate risk management and strategy activities:** ▪ While risk insights should be an important input to strategic planning, most respondents do not believe their risk management processes provide strategic advantage. ▪ A large percentage of organizations' ERM process does not formally assess emerging strategic, market, or industry risks. ▪ Many organizations are not emphasizing the consideration of risk exposures when management evaluates different possible strategic initiatives or when making capital allocations. ▪ Most organizations do not formally articulate tolerances for risk taking as part of their strategic planning activities. ▪ There is noticeable room for improving ERM processes to help manage risks impacting reputation and brand. ▪ There are opportunities to reposition an entity's risk management process to ensure risk insights generated are focused on the most important strategic issues.
IMPACT OF CULTURE ON RISK MANAGEMENT	**Cultural factors, including the tone at the top set by the board and C-suite may explain the lack of ERM maturity across organizations:** ▪ A dominant belief exists in many organizations that "risks are managed in other ways besides ERM." Others believe there are other more important priorities that compete with the need to enhance risk management. ▪ Most organizations do not provide training and guidance on risk management, potentially creating a lack of understanding of how proactive versus reactive risk management might help. ▪ Few organizations embed risk management incentives in performance compensation arrangements. ▪ There may be a disconnect between desired versus actual risk management capabilities given the majority of organizations describe their risk culture as "strongly risk averse" to "risk averse" despite the finding that only a minority of respondents describe their risk management processes as "mature" or "robust."

EXECUTIVE SUMMARY OF KEY INSIGHTS

ASSIGNMENT OF RISK MANAGEMENT LEADERSHIP

Organizations are pinpointing leadership of ERM by assigning an individual to serve as chief risk officer and by creating management level risk committees:

- Identifying an executive to lead the risk management process is becoming more common relative to a decade ago; however, still less than one-half of our surveyed organizations are doing so.
- Individuals serving in the CRO or equivalent role most often report directly to either the CEO or CFO.
- A management level risk committee is quite common particularly for large organizations and public companies.
- Most risk committees meet quarterly, with an additional 33% meeting monthly.
- There is a nice mix of executives who serve on management level risk committees, with CFOs most often engaged.

RISK IDENTIFICATION AND ASSESSMENT PROCESSES

Structural components of an ERM process exist, but vary across organizations:

- There is substantial variation in the frequency of updating the identification of risks affecting the enterprise, with around half updating annually with an additional one-third updating semi-annually or quarterly.
- About half of organizations surveyed formally define the term “risk” and when they do, they tend to focus that definition on both the upside (opportunities) and downside (threats) dimensions of risks.
- Some form of standardization, such as a template, is commonly used to engage business leaders across an organization in risk identification activities.
- There is a heavy emphasis on risks related to technology, legal/compliance, and financial issues, with ERM processes less focused on emerging strategic/market/industry risks or risk related to reputation.
- There is a growing trend among organizations to maintain enterprise-level risk inventories compared to a decade earlier; however, the majority of organizations do not aggregate risk information to an enterprise-level inventory of top risks.
- Consistent with the recent past about two-thirds of the largest organizations, public companies, and financial services organizations provide explicit guidelines to business unit leaders for them to use when assessing risk probabilities and impact.
- While organizations on average use both a quantitative and qualitative approach to risk assessment, the process tends to be more qualitative than quantitative.

EXECUTIVE SUMMARY OF KEY INSIGHTS

RISK MONITORING PROCESSES	**Most management dashboards do not include key risk indicators for management to monitor risk trends:** ▪ Across the full sample, only 28% describe their key risk indicators as "mostly" to "extensively" robust, suggesting there is room for improvement in KRIs. ▪ Data analytic tools may provide opportunities for management to strengthen their management "dashboards" to include more information that helps track potential risks on the horizon. ▪ Risk communications to senior management are most likely to be *ad hoc* as part of other management meetings.
BOARD RISK OVERSIGHT STRUCTURE	**While risk oversight is a core board governance responsibility, most boards of directors delegate responsibility for risk oversight to a subcommittee:** ▪ Boards typically assign formal responsibility for overseeing management's risk assessment and risk management process to the audit committee, except for financial services organizations that have a risk committee at the board level. ▪ Delegated responsibility for risk oversight is usually specified in board committee charters. ▪ The presence of a formal risk management policy statement is mixed across organizations, with fewer than half of all organizations in our survey having a formal statem.
BOARD REPORTING AND MONITORING	**Most organizations prepare a formal report on top risks to the board at least annually:** ▪ Financial services organizations are more likely to report risks to the board on a quarterly versus annual basis whereas most other organizations are more likely to report annually rather than quarterly. ▪ The majority of boards set aside a specific meeting to discuss the aggregate report of top risk exposures facing the organization, particularly for public companies. ▪ There is noticeable variation in the number of top risk exposures reported to the board across different types of organizations, with most reporting between five and 19 risk exposures. ▪ The integration of risk information with discussion of the strategic plan is not occurring extensively across most organizations, suggesting there may be opportunities to enhance the integration of risk information with strategic planning efforts for most organizations. ▪ Organizations of all types are experiencing an increase in the public disclosure of risk information to external stakeholders.

A number of additional insights are contained in the pages that follow. It is our hope that this data provides important insights that business leaders can use to benchmark and improve their organization's strategic use of risk insights for competitive advantage.

DRIVERS FOR ENHANCED RISK MANAGEMENT

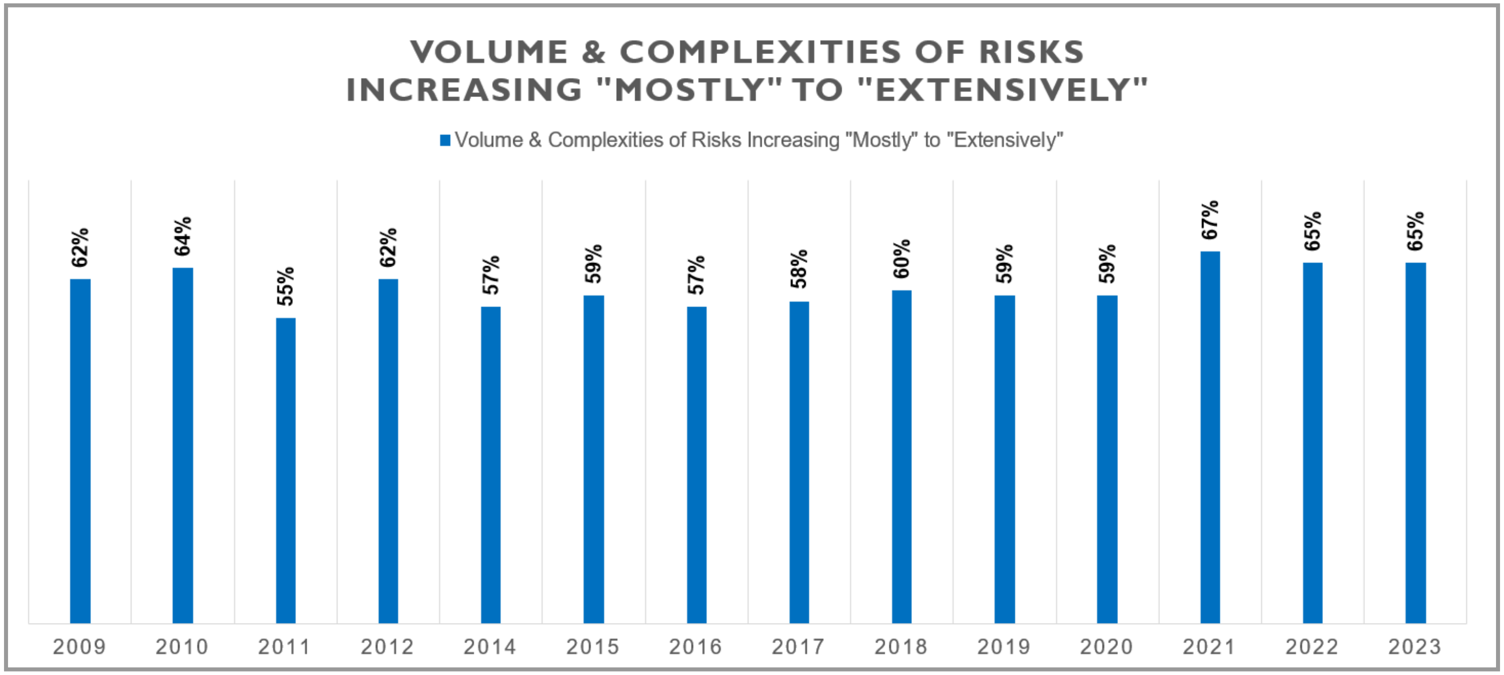
This section highlights a number of factors that are motivating leadership teams of all types of organizations to enhance their risk management efforts.

We Suggest These Questions to Assess Your Organization's Risk Readiness:

1. How is the overall business environment changing risks affecting your organization?
2. How might recent significant operational surprises be hinting that the organization's risk management processes are insufficiently robust?
3. How are external stakeholder expectations driving improvements in how your organization's leaders identify and manage ongoing risks?
4. Who within your organization's leadership team is calling for more management involvement in risk management activities?

PERCEPTIONS OF CURRENT RISK ENVIRONMENT

To get a sense for the extent of risks faced by organizations represented by our respondents, we asked respondents to describe how the volume and complexity of risks have increased in the last five years. We have asked this question in all 14 years that we have conducted this study. The chart below shows the percentages responding "mostly" or "extensively" to this question for each of those 14 years.[1]



Note: We did not issue a report in 2013.

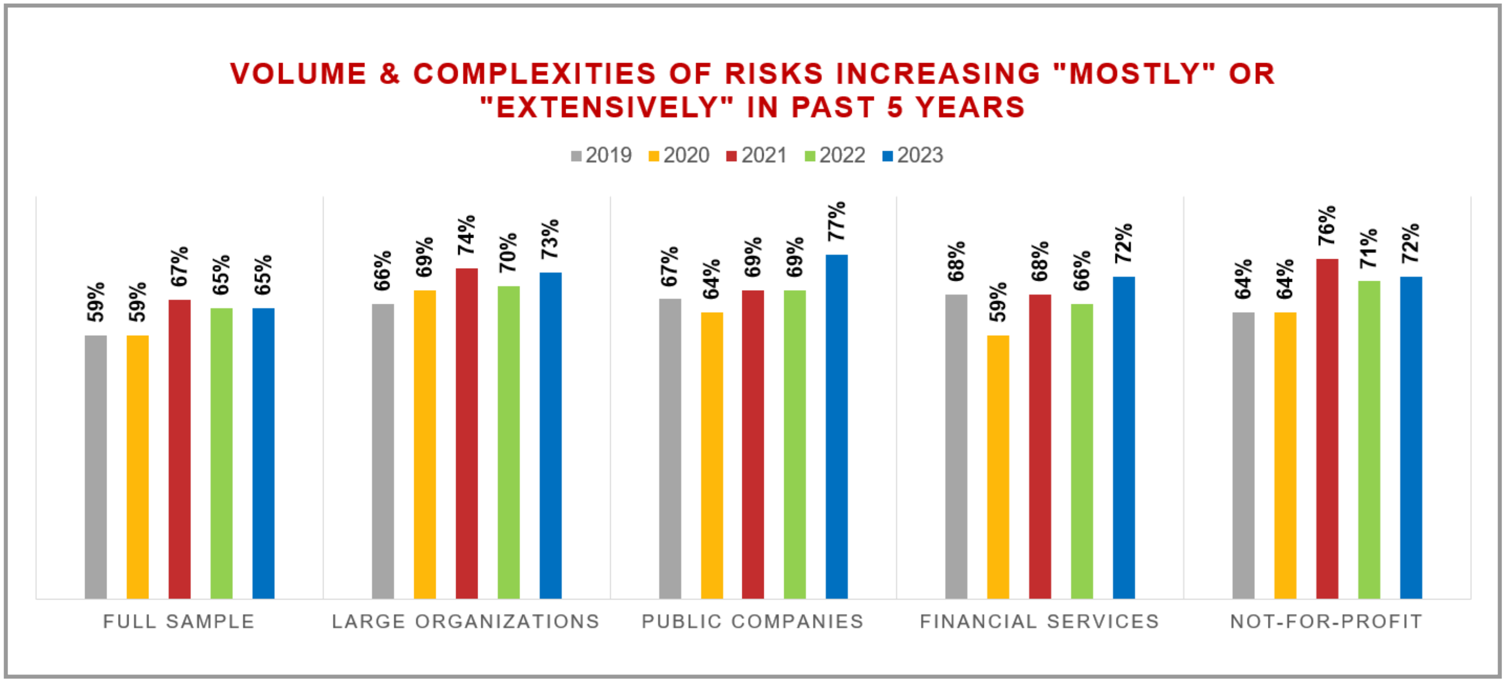
KEY INSIGHT

- Continued uncertainties linked to the economy and inflation, geopolitical challenges, emerging AI innovations, ever-present cyber threats are triggering perceptions of risks that are close to their highest levels in the 14 years, including during the 2008- 2010 financial crisis.

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

DRIVERS FOR ENHANCED RISK MANAGEMENT

PERCEPTIONS OF CURRENT RISK ENVIRONMENT



KEY INSIGHT

- No one is immune to the current risk environment. Different types of organizations experienced a perceived high level in the volume and complexity of risks, with public companies reporting the highest level of increase in the volume and complexity of risks.

KEY INSIGHTS

- The speed of change in the global business environment creates a wide range of uncertainties that can trigger unexpected risks at any point in time. Business leaders who ignore that reality put themselves in a reactive posture as risks emerge.
- The need for effective risk management is unlikely to decline over time, given new risks will continue to emerge with increasingly complex dimensions. Evaluating an organization's approach to enterprise-wide risk management just makes good business sense.

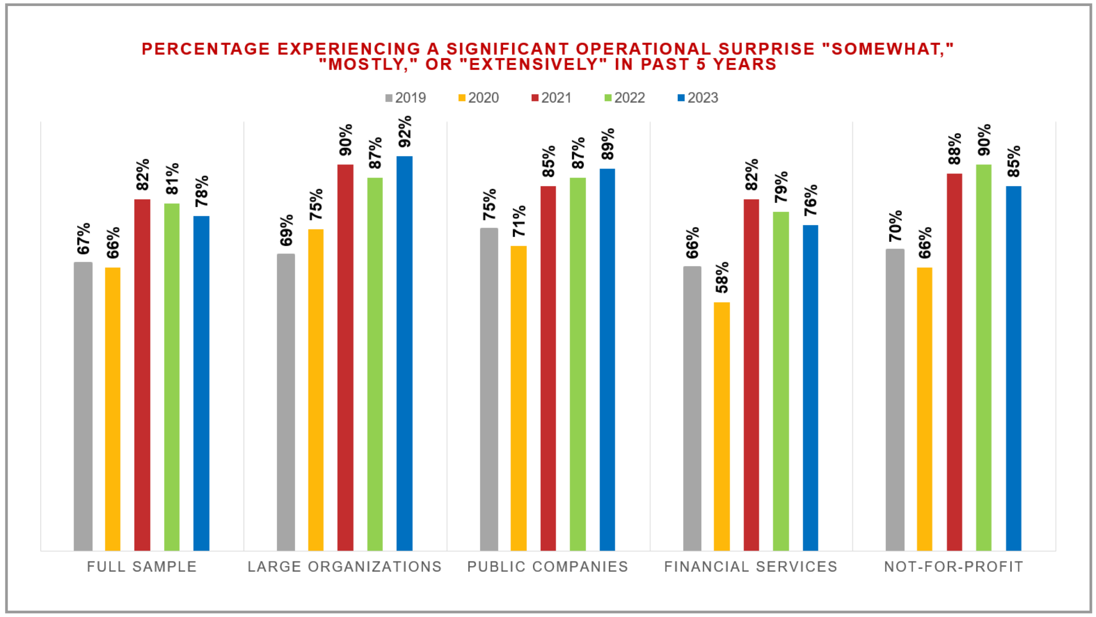
DRIVERS FOR ENHANCED RISK MANAGEMENT

RISKS IMPACT CONTINUITY OF OPERATIONS

Most executives do not want to be blindsided by unexpected events. Unfortunately, a number of uncertainties tied to talent, inflation, supply chain disruptions, ransomware threats, the crisis in Eastern Europe, among many others, continue to introduce a large volume of operational surprises impacting almost all entities. To get a sense for the impact risk events are having on existing operations, we asked respondents about the extent to which their organization has faced a significant operational surprise in the last five years, with the results shown below.

KEY INSIGHTS

- Core operations were significantly impacted by real risk events (e.g., a competitor disruption, an IT systems breach, loss of key talent, among numerous others possible events) in 78% of organizations in our sample, with large organizations and public companies impacted the most.
- The increase in 2021 over the prior years that has continued into early 2023 is significant for all types of organizations, but the largest organizations and public companies reveal continued increases in the extent of unexpected operational surprises.
- Unexpected surprises may be revealing deficiencies in the organization's risk management process.



We also asked specifically whether recent experiences might change how their organizations think about their business continuity planning and crisis management efforts.

Percentage of respondents who are "Somewhat," "Mostly," to "Extensively" concerned about...	Full Sample	Largest Organizations (Revenues >$1B)	Public Companies	Financial Services	Not-for-Profit Organizations
To what extent do you believe there will be significant changes in your organization's approach to business continuity planning and crisis management?	72%	76%	76%	73%	75%

KEY INSIGHT

- Many organizations are concluding that their approaches to business continuity planning and crisis management are not at the level of preparedness desired, with almost three-fourths indicating significant changes in those processes will occur.

TABLE OF CONTENTS

EXTERNAL PARTIES DEMAND RISK INFORMATION

We 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.

PERCENTAGE OF RESPONDENTS SELECTING "MOSTLY" OR "EXTENSIVELY"

Percentage of respondents who are "Mostly" to "Extensively" concerned about...	Full Sample	Largest Organizations (Revenues >$1B)	Public Companies	Financial Services	Not-for-Profit Organizations
External parties applying pressure on senior executives to provide more information about risks affecting the organization	29%	38%	41%	39%	26%

KEY INSIGHTS

- External expectations for large organizations, public companies and financial services organizations to provide more information about risks are noticeable.

The call for more senior executive involvement in risk management is coming from many external parties, particularly boards of directors.

PERCENTAGE OF RESPONDENTS SELECTING "MOSTLY" OR "EXTENSIVELY"

Which external parties are asking "Mostly" or "Extensively" for increased senior executive involvement in risk oversight?	Full Sample	Largest Organizations (Revenues >$1B)	Public Companies	Financial Services	Not-for-Profit Organizations
Board of Directors	34%	35%	37%	32%	41%
Key Stakeholders	21%	20%	21%	21%	23%
Regulators	23%	22%	27%	34%	21%

KEY INSIGHTS

- The board of directors' request for more engagement of senior executives in risk management is strong for all organizations, especially for not-for-profit organizations.
- Regulator expectations are highest for financial services organizations, even higher than board requests.

TABLE OF CONTENTS

EXTERNAL PARTIES DEMAND RISK INFORMATION

The sense that management does not really like surprises is apparent. When asked about factors encouraging management to increase senior executive focus on risk management related activities, the factor creating the most pressure is "unanticipated risk events affecting the organization" for most types of organizations. However, public companies and financial services organizations indicate that emerging best practice expectations and emerging corporate governance requirements are also having a noticeable impact for them.

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
Unanticipated risk events affecting organization	35%	47%	38%	33%	45%
Unanticipated risk events affecting competitors	15%	19%	17%	14%	15%
Emerging best practice expectations	29%	30%	38%	32%	28%
Emerging corporate governance requirements	24%	28%	43%	30%	20%

KEY INSIGHTS

- Over one-third of the full sample (almost one-half of large organizations) indicated that unanticipated risk events affecting the organization were putting pressure on management to do more related to risk management.
- There is a general sense that both emerging best practices and corporate governance requirements are collectively pressuring management to increase their focus on risk management activities in most organizations.

TABLE OF CONTENTS

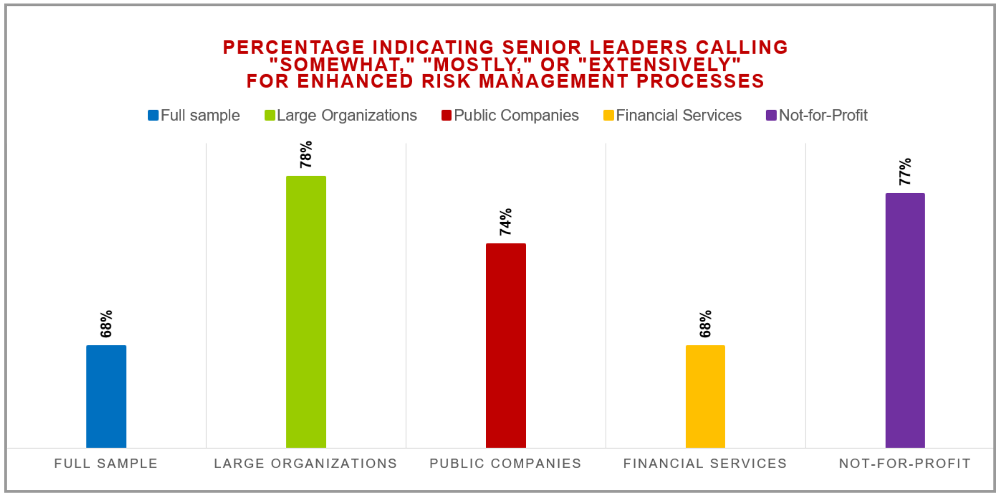
DRIVERS FOR ENHANCED RISK MANAGEMENT

SENIOR LEADERS CALL FOR RISK MANAGEMENT

While there are growing external expectations for organizations to increase senior leadership involvement in risk management, there are also requests by the management team for enhanced risk management. We specifically asked "In light of the ongoing uncertainties in the global marketplace, *to what extent will your organization's senior leadership team be calling for more enhanced risk management processes?"*

KEY INSIGHT

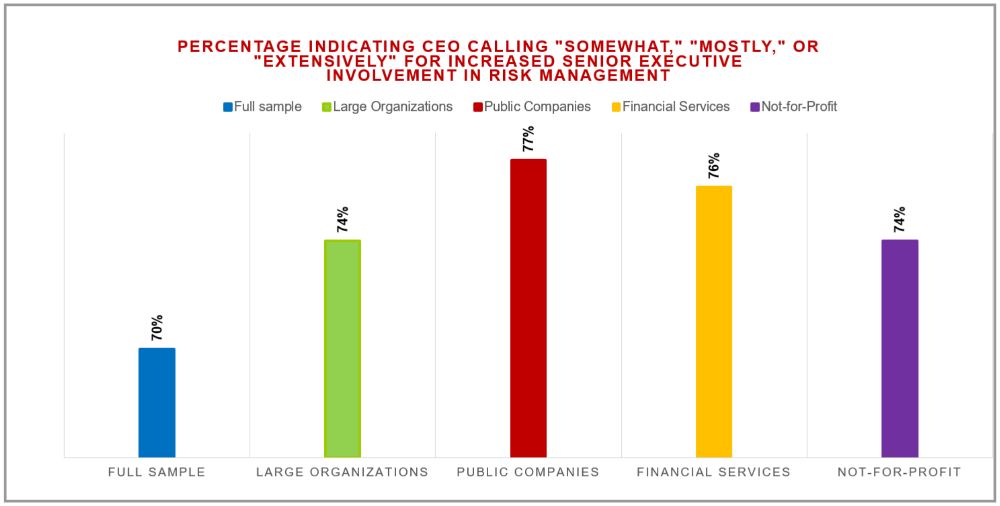
- Overwhelmingly, there is a strong indication that senior management will be looking for ways to enhance the organization's approaches to risk management going forward.



Interestingly, CEOs are also asking for increased senior executive involvement in risk oversight.

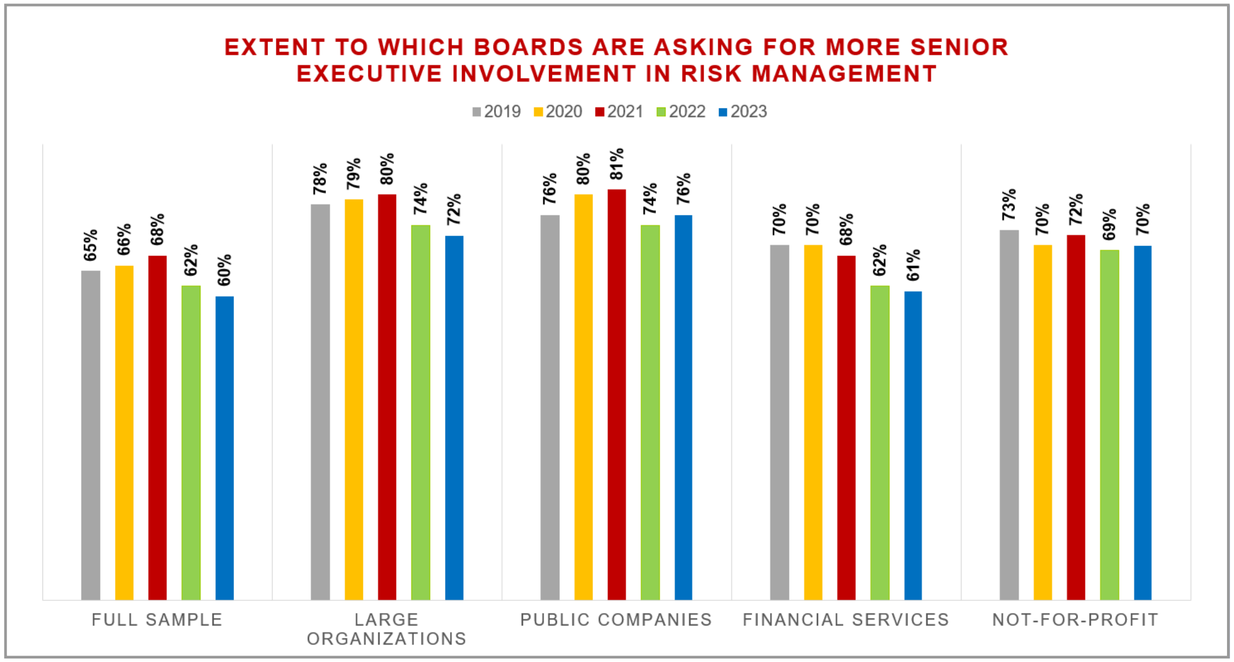
KEY INSIGHT

- CEOs are calling on other senior executives to increase their level of engagement in risk management, especially those in large organizations or public companies.



BOARDS SEEK MORE EXECUTIVE ENGAGEMENT IN RISK MANAGEMENT

In light of the board's overall responsibility for overseeing management's risk-taking actions, boards are naturally interested in the risk management processes and infrastructure designed and implemented by senior executives to manage risks affecting the organization. Our survey finds that boards of directors continue to ask "somewhat," "mostly," or "extensively" for increased senior executive involvement in risk oversight, although at slightly decreased levels compared to prior years, as shown by the chart below.



KEY INSIGHTS

- While board expectations for increased senior executive involvement in risk oversight is strong across all types of organizations, it is interesting to observe a slight decline in that over the past two years for the full sample, large organizations, and financial services entities.
- Effective risk management is clearly a priority among boards and merits increased management attention.

OVERALL STATE OF RISK MANAGEMENT MATURITY

This section highlights the overall state of risk management maturity across organizations.

We Suggest These Questions to Assess Your Organization's Risk Readiness:

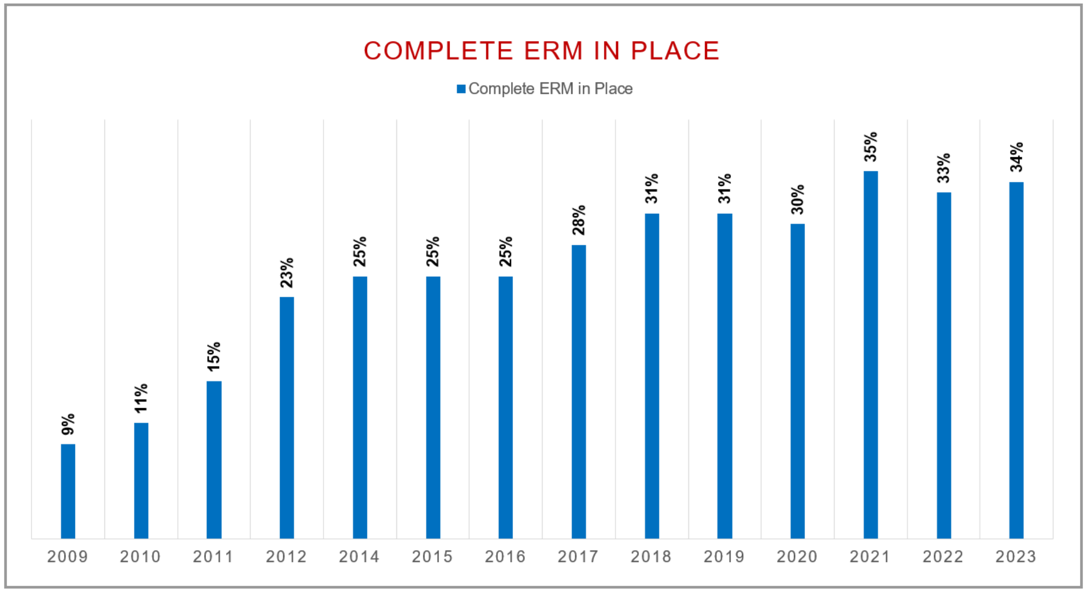
1. How would your organization's senior leadership team describe the overall maturity of the organization's risk management processes? Might that view differ from the view of the board of directors?
2. What has your organization done to invest more time, attention, and resources to explicitly identify, assess, and manage risks across the enterprise?
3. Would you describe your organization's approach to risk management as explicit, structured, coordinated, or would you describe it as more implicit, *ad hoc*, informal?
4. To what extent is risk management a siloed activity that exists within different business functions with little coordination and aggregation of risk insights at an enterprise level?

EMBRACE OF ENTERPRISE-WIDE RISK MANAGEMENT (ERM)

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

- 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

We observe a small increase in the percentage of organizations that believe they have a "*complete formal enterprise-wide risk management process in place*" relative to the plateau we observed in 2018-2020.



Note: We did not issue a report in 2013.

KEY INSIGHTS

- While progress has been made in implementing complete ERM over the fourteen years we have conducted this survey, there is still relatively slow progress in continuing to move towards a more robust, complete enterprise-wide approach to risk management.
- In 2009, only 9% of organizations claimed to have complete ERM processes in place; however, in early 2023 the percentage has increased to 34% for the full sample. So, greater adoption of ERM has occurred, although not at a level many might expect in light of the risk environment we now face.
- There continues to be significant opportunity for improvement in most organizations, given that more than two-thirds of organizations surveyed in early 2023 still cannot yet claim they have "complete ERM in place."

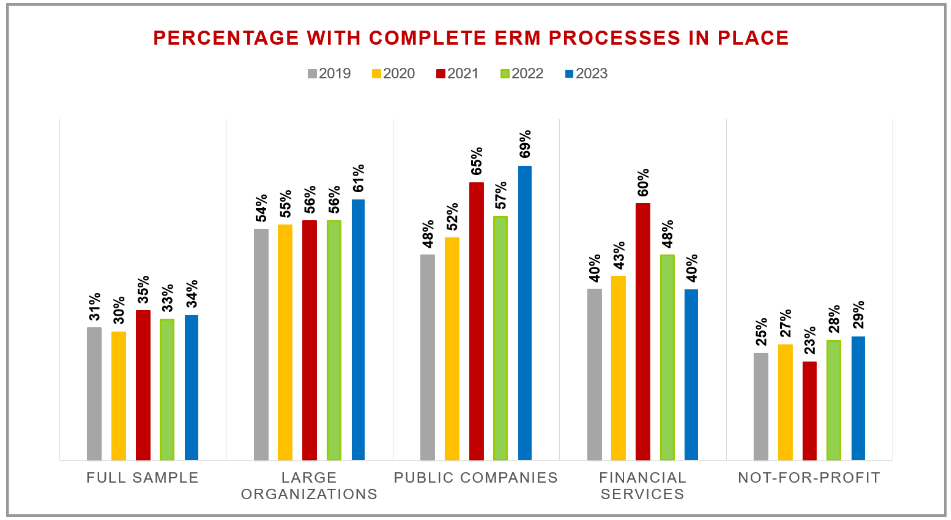
OVERALL STATE OF RISK MANAGEMENT MATURITY

EMBRACE OF ENTERPRISE-WIDE RISK MANAGEMENT (ERM)

There is noticeable variation across different types of organizations in the development of complete ERM processes.

KEY INSIGHTS

- Public companies and large organizations are the most likely to have "complete ERM processes" in place relative to other types of organizations. Interestingly, there was an increase in the percentages for those types of organizations in the current year.
- Non-profit organizations significantly lag other types of organizations in implementing complete ERM processes.



For the full sample, we found that 18% of the respondents have no enterprise-wide risk management process in place. An additional 8% 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.

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	**18%**	**1%**	**3%**	**14%**	**7%**
Currently investigating concept of enterprise-wide risk management, but have made no decisions yet	**8%**	**2%**	**2%**	**6%**	**5%**
No formal enterprise-wide risk management process in place, but have plans to implement one	**8%**	**7%**	**3%**	**9%**	**10%**
Partial enterprise-wide risk management process in place (i.e., some, but not all, risk areas addressed)	**32%**	**29%**	**23%**	**31%**	**49%**
Complete formal enterprise-wide risk management process in place	**34%**	**61%**	**69%**	**40%**	**29%**

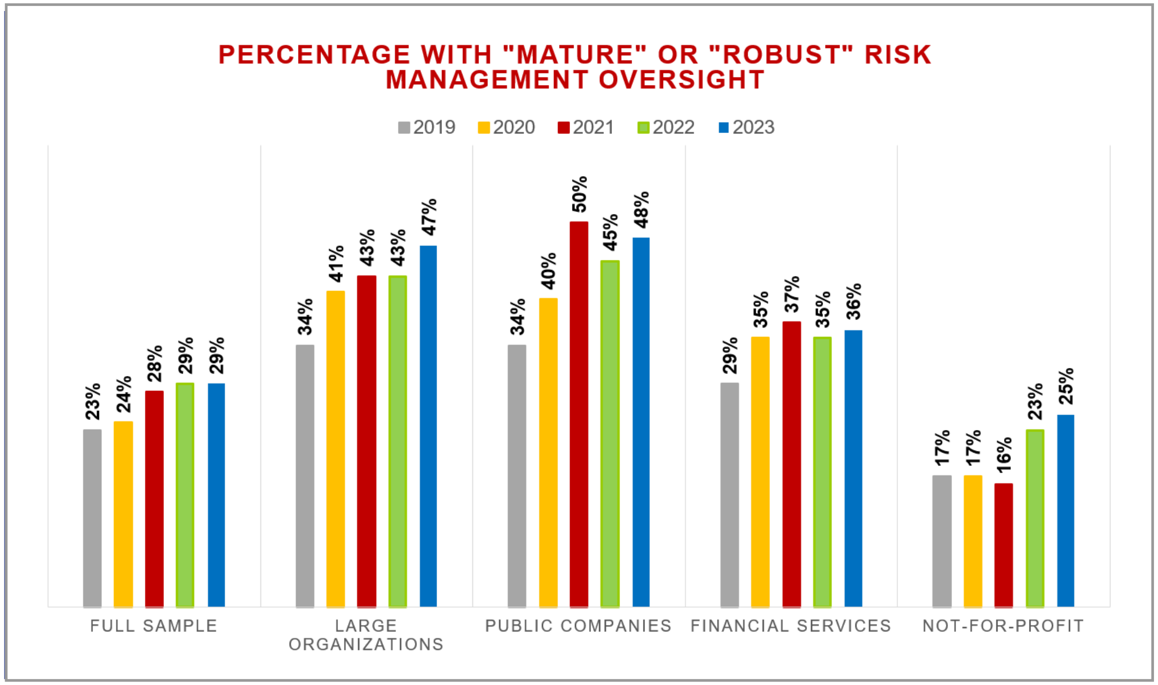
KEY INSIGHT

- In light of the current environment, it is puzzling that, on a combined basis, just over one-fourth of respondents (26%) have no formal enterprise-wide approach to risk oversight and are currently making no plans to consider this form of risk oversight.

LEVEL OF RISK MANAGEMENT MATURITY

While we observe a relatively steady percentage of entities that describe their risk oversight processes as "complete ERM processes," that does not mean those ERM processes are mature. To obtain a sense for the current state of ERM maturity, we asked survey participants to respond to several questions to help us get a sense for the current level of risk oversight in organizations surveyed.

For example, 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."



KEY INSIGHTS

- Most types of organizations believe their risk management oversight remains at relatively similar levels of robustness or maturity as in the prior years, with the exception of large organizations and public companies that report small increases in maturity levels.
- Interestingly, only 29% of full sample respondents describe their organizations' approach to risk management as "mature" or "robust" and less than half of large organizations and public companies rate their risk management oversight as "mature" or "robust."
- In light of the current business environment, it is interesting to observe such low levels of risk management maturity.

LEVEL OF RISK MANAGEMENT MATURITY

When we break down the descriptions of their organization's risk oversight processes, we find room for improvement continues to exist.

PERCENTAGE OF RESPONDENTS					
What is the level of maturity of your organization's risk management oversight?	**Very Immature**	**Developing**	**Evolving**	**Mature**	**Robust**
Full Sample	**15%**	**21%**	**35%**	**24%**	**5%**
Largest Organizations	**5%**	**16%**	**32%**	**37%**	**10%**
Public Companies	**3%**	**11%**	**38%**	**38%**	**10%**
Financial Services	**16%**	**17%**	**31%**	**29%**	**7%**
Not-for-Profit Organizations	**10%**	**25%**	**40%**	**21%**	**4%**

KEY INSIGHTS

- The level of sophistication of underlying risk management processes still remains fairly immature (e.g., "very immature" or "developing") for just over one-third of the full sample of those responding to our survey.
- The lack of overall maturity for financial services organizations is surprising, especially that 33% describe their processes as "very immature" or "developing."

In light of the possibility that the questions we used do not reflect how respondents think about their risk management maturity, we provided four possible descriptions of risk management processes and asked respondents to select the statement that best reflects their risk management process.

PERCENTAGE OF RESPONDENTS					
Description of the Current Stage of ERM Implementation	**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.	**40%**	**68%**	**69%**	**46%**	**43%**
Our process is mostly informal and unstructured, with *ad hoc* reporting of aggregate risk exposures to the board.	**25%**	**15%**	**19%**	**24%**	**27%**
We mostly track risks by individual silos of risks, with minimal reporting of top risk exposures to the board.	**18%**	**14%**	**9%**	**14%**	**17%**
There is no structured process for identifying and reporting top risk exposures to the board.	**17%**	**3%**	**3%**	**16%**	**13%**

KEY INSIGHTS

- Over two-thirds of large organizations and public company respondents describe the current state of their ERM process as systematic, robust and repeatable.
- Non-profit organizations are less likely to have structured risk management processes relative to other organizations.

STRATEGIC VALUE OF RISK MANAGEMENT

This section highlights how risk management practices are providing strategic insights for decision making.

We Suggest These Questions to Assess the Strategic Value of Your Organization's Risk Management Processes:

1. To what extent are risk insights generated by your organization's risk management processes an important input for strategic decision making?
2. Is the emphasis on measuring and monitoring "return" greater than the emphasis on measuring and monitoring "risks" despite the fact we know risk and return are related?
3. Does your organization's risk management process explicitly prompt management to identify strategic risks?
4. Would you describe the current focus of your organization's ERM process as heavily weighted towards internally focused operational and compliance risks with less focus on strategic risks that may be triggered by events external to the organization?

TABLE OF CONTENTS

STRATEGIC VALUE OF RISK MANAGEMENT

COMPETITIVE ADVANTAGE PROVIDED BY RISK MANAGEMENT

Most business leaders understand the reality that to generate returns the organization must take risks. Thus, they recognize the direct connection of risk with return. Despite that understanding, a number of business leaders fail to appreciate how investing in risk management processes should provide important insights to strategic planning. Many organizations fail to integrate their risk management and strategic decision-making efforts.

We asked several questions to obtain information about the intersection of risk management and strategy in the organizations we surveyed. Responses to the question about the extent to which respondents believe the organization's risk management process is a proprietary strategic tool reveal how risk management is viewed in those organizations.

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?	38%	26%	25%	9%	2%

KEY INSIGHT

- Organizations continue to struggle to integrate their risk management and strategic planning efforts. Just under two-thirds (64%) responded to this question by indicating "not at all" or "minimally," consistent with what we have observed in prior years.

Furthermore, as shown by the bar graph below, the assessment of the strategic value of the organization's risk management process is noticeably low for all organizations.

KEY INSIGHTS

- Overwhelmingly, most organizations do not perceive their risk management processes as providing important risk insights that management can use to create or enhance strategic value.
- There appear to be opportunities to reposition an entity's risk management process to ensure risk insights generated are focused on the most important strategic issues.

FOCUS ON EMERGING STRATEGIC RISKS

To delve deeper into the strategic value of risk management practices, we asked about the extent to which the ERM process formally identifies, assesses, and responds to emerging risk issues. We are particularly interested in the extent to which the entity's risk management processes explicitly encourage management to think about emerging strategic, market, or industry risks.

PERCENTAGE OF RESPONDENTS					
Extent to which the organization's ERM process formally identifies, assesses and responds to emerging strategic, market, or industry risks:	**Full Sample**	**Largest Organizations (Revenues >$1B)**	**Public Companies**	**Financial Services**	**Not-for-Profit Organizations**
Extensively	**14%**	**22%**	**28%**	**21%**	**15%**
Mostly	**26%**	**32%**	**31%**	**22%**	**31%**
Somewhat	**32%**	**35%**	**36%**	**33%**	**31%**
Minimally	**13%**	**8%**	**3%**	**12%**	**14%**
Not at All	**15%**	**3%**	**2%**	**12%**	**9%**

KEY INSIGHTS

- Interestingly, the majority of large organizations and public companies indicate that their organization's ERM process formally focuses "mostly" to "extensively" on emerging strategic, market, and industry risks. Ideally, that percentage would be much higher for all organizations (ideally it should be at 100%).
- When pairing these results with those on the prior page, organizations appear to be struggling to integrate information about emerging strategic, market, and industry risks into their strategic decision-making processes.

INTEGRATION OF RISKS WITH STRATEGIC PLANNING

To better understand factors that might impact the strategic value of risk management processes, we asked three questions to delve more deeply into potential opportunities for risk management considerations to be explicitly embedded in strategic planning decisions.

PERCENTAGE OF RESPONDENTS SAYING "MOSTLY" OR "EXTENSIVELY"

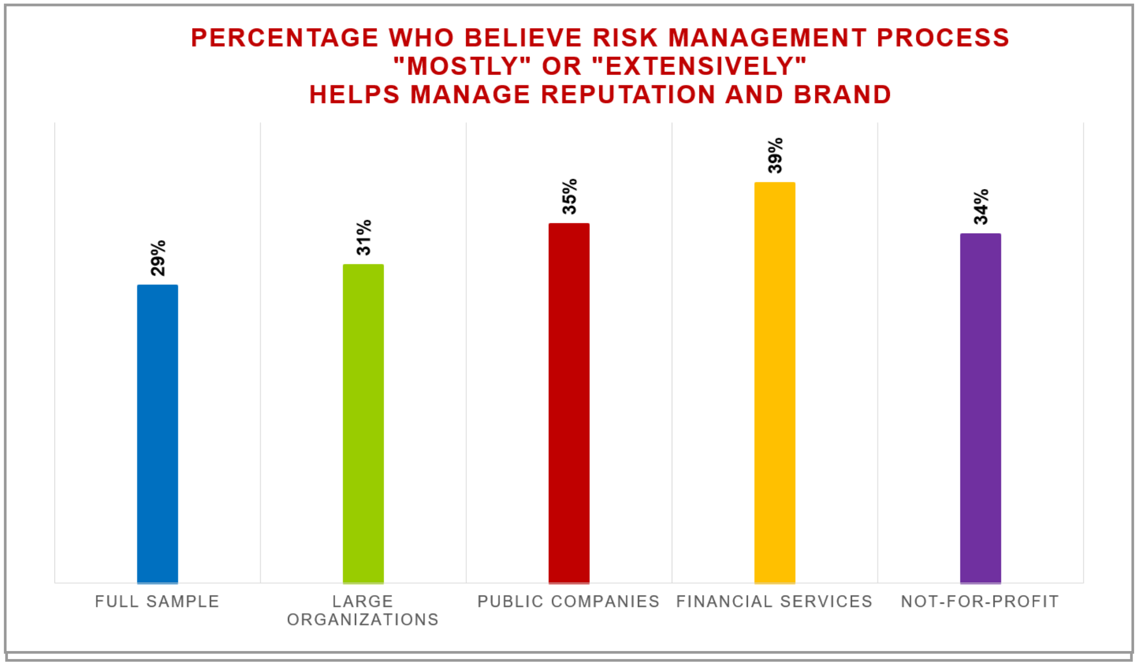
Percentage of respondents who selected "Mostly" to "Extensively" to the following statements	Full Sample	Largest Organizations (Revenues >$1B)	Public Companies	Financial Services	Not-for-Profit Organizations
Existing risk exposures are considered when evaluating possible new strategic initiatives	45%	45%	51%	55%	45%
Organization has articulated its appetite for or tolerance of risks in the context of strategic planning	32%	31%	37%	51%	26%
Risk exposures are considered when making capital allocations to functional units	36%	38%	38%	38%	38%

KEY INSIGHTS

- About one-half of most organizations are significantly emphasizing the consideration of risk exposures when management evaluates different possible strategic initiatives.
- A majority of organizations outside of financial services do not formally articulate tolerances for risk taking as part of their strategic planning activities.
- Risk dimensions do not appear to be a significant explicit consideration when making capital allocation or budgeting decisions. That is, capital allocations are often made without considering differences in risk exposures.

MONITORING RISKS TO REPUTATION AND BRAND

When risk events occur, they can often significantly damage an entity's reputation and brand. More robust risk management processes should aid management and the board in monitoring and responding to risk more proactively rather than reactively, and an effective ERM process should help inform management and the board on a timely basis about events that may be emerging that may impact reputation and brand. We asked respondents about the extent to which organizations are using their ERM processes to identify and manage significant risk events capable of harming the organization's reputation and brand.



KEY INSIGHTS

- While some organizations find value from their ERM process in helping navigate risks to reputation and brand, there is noticeable room for improvement.
- There may be opportunities for management to identify the primary factors that affect reputation and brand for important stakeholders to then ensure the risk identification processes are focused on identifying and assessing risks to those drivers of reputation and brand.

IMPACT OF CULTURE ON RISK MANAGEMENT

This section highlights how an organization's culture and "tone at the top" may impact the level of engagement in risk management for strategic decision making.

We Suggest These Questions to Assess Your Organization's Risk Culture:

1. How is your organization's overall culture affecting the risk management process?
2. How would you describe the organization's "tone at the top" regarding the importance of engaging in more robust risk management activities?
3. What are the common points of resistance that you experience as you try to engage different business function leaders in risk management discussions?
4. To what extent has your organization's leaders had opportunities to learn about what ERM is and how it could be better integrated with strategic decision making?
5. Could executive reluctance to engage in ERM be due to a lack of understanding and training instead of the strategic value of more proactive versus reactive risk management?

IMPEDIMENTS TO EMBRACING ERM

While organizations have engaged in risk management activities for centuries, the concept of ERM has only fully emerged over the past two decades. So, relative to traditional risk management activities, the concept of ERM is still fairly new. There often is confusion about what ERM represents and there is a lack of understanding as to how ERM might be beneficial to senior leadership and the board.

To get a sense of impediments to the embrace of ERM, we asked respondents whose organizations have not yet implemented an enterprise-wide risk management process to provide some perspective on that decision. Respondents could indicate more than one hurdle or obstacle to ERM progress as shown in the table below.

PERCENTAGE OF RESPONDENTS SAYING "MOSTLY" OR "EXTENSIVELY"					
Percentage of respondents indicating that each of the following "Mostly" to "Extensively" is impeding risk management progress	**Full Sample**	**Largest Organizations (Revenues >$1B)**	**Public Companies**	**Financial Services**	**Not-for-Profit Organizations**
Risks are monitored in other ways besides ERM	**26%**	**22%**	**28%**	**24%**	**26%**
Too many other pressing needs	**19%**	**22%**	**17%**	**24%**	**24%**
No requests to change our risk management approach	**20%**	**18%**	**14%**	**22%**	**21%**
Do not see benefits exceeding costs	**13%**	**18%**	**24%**	**12%**	**5%**
No one to lead effort	**13%**	**16%**	**10%**	**13%**	**17%**
Would overcomplicate what can be best done *ad hoc*	**9%**	**4%**	**7%**	**5%**	**7%**

KEY INSIGHTS

- There are a number of impediments to the embrace of ERM, with the most frequently cited obstacle reflecting a sentiment that organizations manage risks in other ways besides ERM. That is important to consider in addition to the 13% who indicate that leaders "do not see the benefits exceeding the costs."
- A lack of clear direction and leadership of an ERM implementation is also a factor that restricts ERM progress as indicated by the percentages of respondents selecting "No requests to change our risk management approach (20%)" and "No one to lead effort (13%)."
- Earlier we reported that 65% of our respondents noted that the volume and complexity of risks have drastically increased over the past five years and 36% of the full sample indicated that their organization's risk oversight processes are "very immature" or "developing." However, as noted above 26% believe risks are monitored in other ways besides ERM and 19% indicate "there are too many other pressing needs" to spend time on implementing more robust risk management processes. This may represent an important disconnect that business leaders should consider as they evaluate their risk management processes.

CULTURAL BARRIERS THAT LIMIT PROGRESS

An organization's overall culture and the "tone at the top" can have a direct impact on attitudes and perceptions about the need for and benefits of a more robust risk management process. Cultural barriers often exist that lead to resistance to investing time and energy in risk management processes, despite the reality that risks continue to grow in volume and complexity for most organizations. Several perceived barriers appear to limit management from taking the necessary actions to strengthen their approach to risk oversight.

We asked respondents to identify the impact of several cultural barriers that restrain progress in advancing an organization's ERM processes. Respondents could indicate more than one barrier as shown in the table below.

PERCENTAGE IDENTIFYING EACH AS A BARRIER TO ERM IMPLEMENTATION

Percentage of respondents who describe each of the following as being a "barrier" or "significant barrier" to effective ERM	Full Sample	Largest Organizations (Revenues >$1B)	Public Companies	Financial Services	Not-for-Profit Organizations
Competing priorities	46%	48%	40%	49%	55%
Insufficient resources	46%	47%	45%	50%	52%
Lack of perceived value	31%	32%	35%	31%	32%
Perception ERM adds bureaucracy	27%	28%	29%	25%	26%
Lack of board or senior executive ERM leadership	21%	15%	15%	20%	25%
Legal or regulatory barriers	7%	5%	6%	7%	7%

KEY INSIGHTS

- The two most common barriers in the full sample to advancing an organization's risk management processes are a perception that there are other more important priorities for the organization or there are insufficient resources to invest in ERM, with 46% identifying these as "barriers" or "significant barriers" to the organization's implementation of ERM processes.
- It is likely a combination of barriers that need to be considered based on the data shown above which indicates that several cultural factors may need to be addressed if the organization desires to advance its risk management processes.

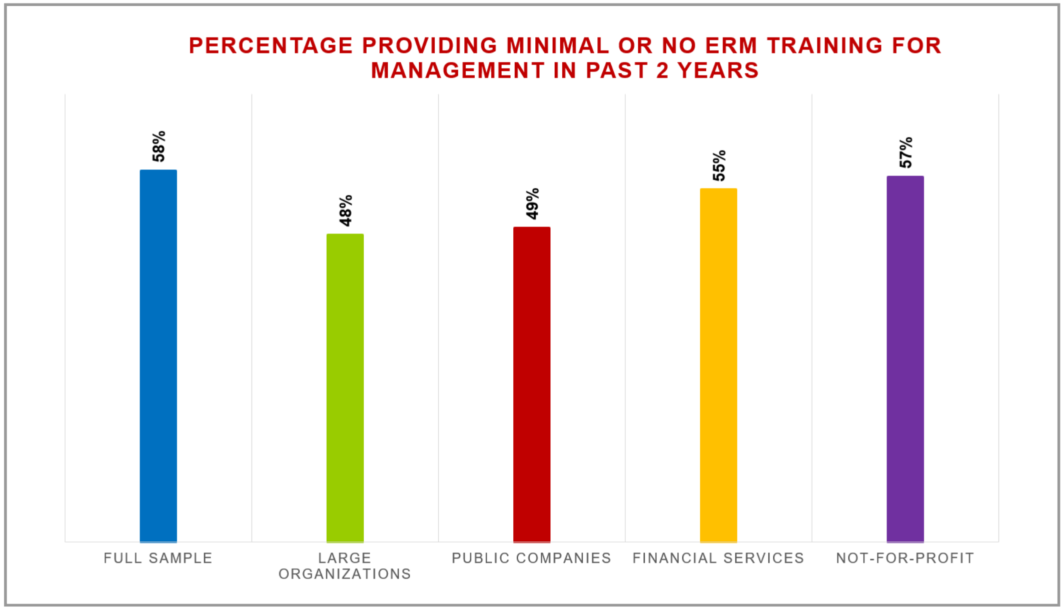
TABLE OF CONTENTS

IMPACT OF CULTURE ON RISK MANAGEMENT

EDUCATION AND AWARENESS OF ERM

Some of the overall reluctance to embrace ERM across an organization may be due to a lack of understanding and knowledge of what an enterprise-wide risk management process actually entails relative to traditional approaches organizations use to manage risks. ERM is a relatively new business paradigm that business leaders are hearing about but may lack an understanding of how it might help them achieve their strategic objectives.

To get a sense for the extent that organizations are providing training about ERM processes we asked respondents to describe the extent of risk management training provided to the management team.



KEY INSIGHTS

- Most organizations (58%) have not provided or only minimally provided training on risk management in the past two years for senior executives or key business unit leaders. Other organizations are slightly more likely to have provided ERM training, although the percentages that have not done so is close to the full sample. Not-for-profit entities are least likely to have provided any ERM training.
- The lack of robustness in ERM maturity we discuss earlier in this report 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.

IMPACT OF CULTURE ON RISK MANAGEMENT

INCENTIVES TO ENGAGE IN RISK MANAGEMENT

Some of the overall reluctance to embrace ERM across an organization may be due to a lack of incentives and accountabilities for individual business leaders to assume ownership of risk management responsibilities. We asked respondents about the extent to which risk management activities are an explicit component of determining management performance compensation.

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	34%	34%	26%	25%	43%
Minimally	29%	32%	30%	29%	26%
Combined	**63%**	**66%**	**56%**	**54%**	**69%**

KEY INSIGHTS

- Most organizations have not incorporated risk management incentives and accountabilities into management's performance compensation plans.
- Even large organizations, public companies, and financial services organizations are unlikely to factor risk management activities into performance compensation.
- The increasing focus on compensation and risk-taking should lead more organizations over time to consider modifications to their compensation policies and procedures.

TABLE OF CONTENTS

IMPACT OF CULTURE ON RISK MANAGEMENT

OVERALL RISK MANAGEMENT CULTURE

The level of engagement in designing and implementing enterprise-wide risk management processes may be influenced by the overall willingness for the organization to take risks. Organizations that are more averse to risk-taking may have a greater interest in having robust ERM processes, whereas other organizations with a much higher willingness to take risks may perceive less need in investing in risk management processes and infrastructures.

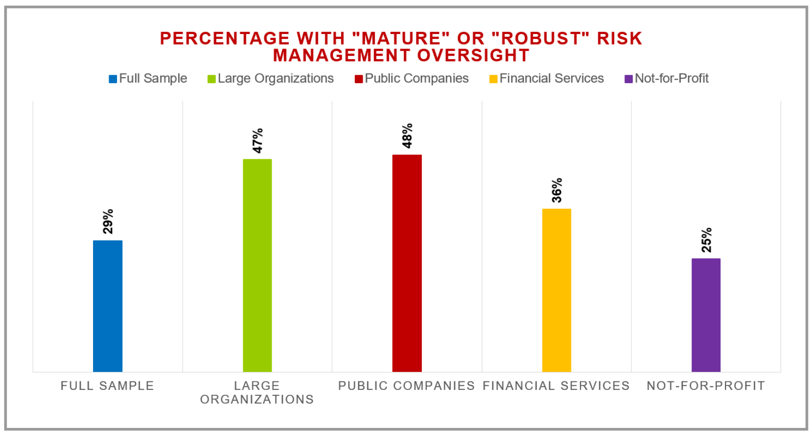
To obtain a sense of the overall risk management culture, we asked respondents to select what best describes their organization's current attitude towards risk taking.

PERCENTAGE OF RESPONDENTS					
How would you describe the risk management culture at your organization?	**Full Sample**	**Largest Organizations (Revenues >$1B)**	**Public Companies**	**Financial Services**	**Not-for-Profit Organizations**
Strongly Risk Averse	**10%**	**10%**	**6%**	**11%**	**9%**
Risk Averse	**45%**	**45%**	**43%**	**40%**	**52%**
Risk Neutral	**33%**	**29%**	**33%**	**34%**	**27%**
Risk Seeking	**12%**	**15%**	**17%**	**14%**	**12%**
Strongly Risk Seeking	**0%**	**1%**	**1%**	**1%**	**0%**

KEY INSIGHTS

- The majority of organizations (55%) in our full sample describe their risk culture as "strongly risk averse" or "risk averse" with an additional 33% selecting "risk neutral," and this is in line with large organizations (55%) and public companies (49%) that describe their risk management culture as "strongly risk averse" to "risk averse." That suggests that in general the overarching "culture" for risk taking is neutral to averse.
- A slightly higher percentage of public companies view their organization as "risk seeking" relative to other types of organizations. Not-for-profit organizations are noticeably more likely to have a risk culture that is "strongly risk averse" or "risk averse."

To put the above in perspective, we show (again) how these organizations describe the overall maturity of their risk management processes.



KEY INSIGHTS

- While the majority of organizations describe their risk management culture as "strongly risk averse" or "risk averse," much smaller percentages of organizations describe their risk management processes as "mature" or "robust."
- There may be a disconnect between desired versus actual risk management capabilities. If organizations are more averse to risk taking, one might expect greater investment in risk management infrastructure and processes to meet that expectation.

ASSIGNMENT OF RISK MANAGEMENT LEADERSHIP

This section highlights benchmarking information related to how leadership of the risk management process is assigned and structured.

We Suggest These Questions to Assess How Your Organization Approaches Risk Management Leadership:

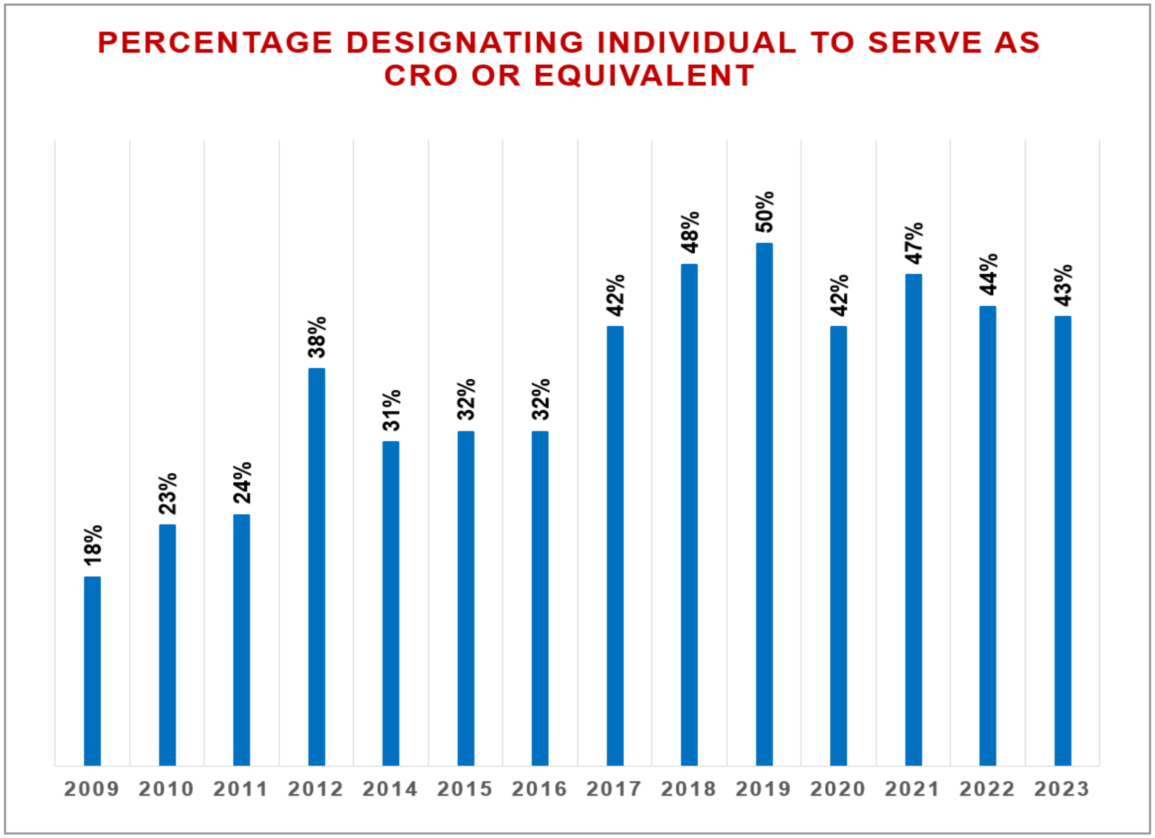
1. Who is leading the enterprise risk management process? Is that responsibility formally assigned?
2. What are the lines of reporting within the organizational chart for the leader of the ERM process? Is the position at the appropriate level of the leadership structure?
3. What committee(s) oversee the risks identified to assess the appropriateness of how the entity is managing enterprise level risks?
4. If the organization has a management level risk committee, what functions are represented and is the committee composed of individuals who can provide a multi-functional lens on risks?
5. How frequently is the risk committee meeting and are the agendas of those meetings leading to ongoing, robust risk conversations?

ASSIGNMENT OF RISK MANAGEMENT LEADERSHIP

DESIGNATION OF A CHIEF RISK OFFICER

Designing and implementing a robust risk management process does not happen without dedicated leadership of that process. Assigning responsibilities for leading an ERM effort is critical for an organization to make progress in risk management. Given all the demands on business leaders' time, individual leaders are less likely to carve out time to explicitly design effective risk management techniques. Rather, they need someone with the responsibility to be the organization's risk management champion to organize and coordinate the organization's risk management efforts.

To get a sense for whether organizations are explicitly naming an individual to serve as risk champion, we asked respondents to indicate whether their organization has formally designated an individual to serve as the Chief Risk Officer (CRO) or senior executive equivalent.



Note: We did not issue a report in 2013.

KEY INSIGHT

- Pinpointing an executive to lead the risk management process is becoming more common relative to a decade ago; however, still less than one-half of our surveyed organizations are doing so.

ASSIGNMENT OF RISK MANAGEMENT LEADERSHIP

DESIGNATION OF A CHIEF RISK OFFICER

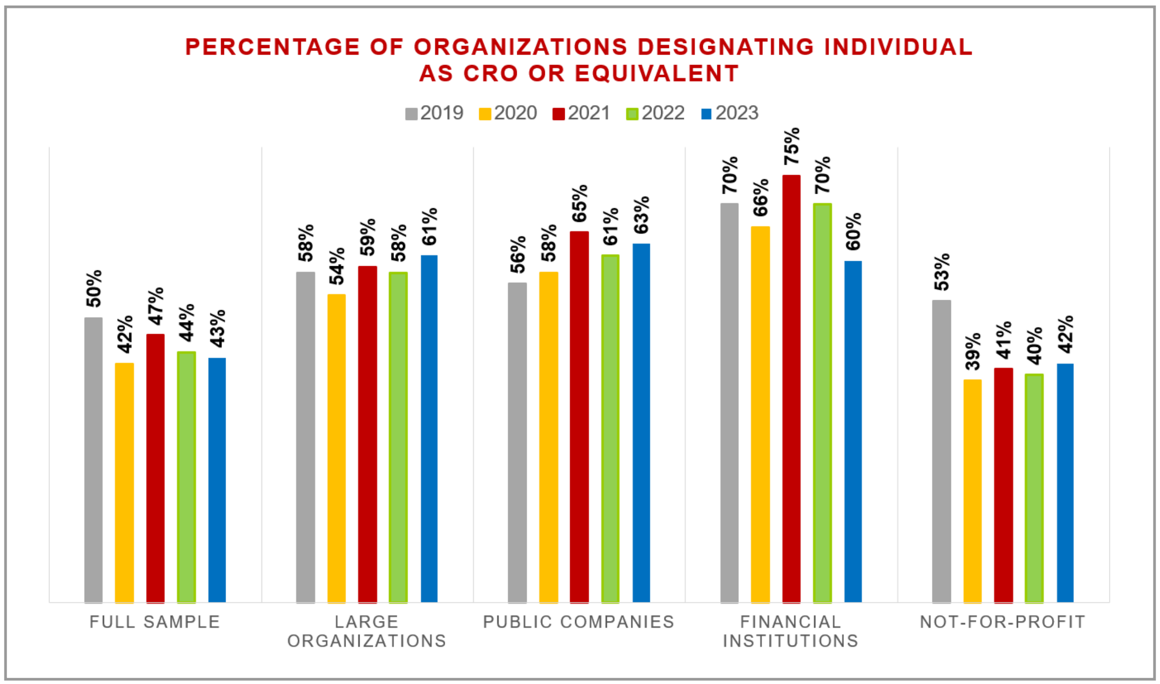
When comparing the percentages of organizations formally designating an individual to serve as CRO or equivalent, there are noticeable differences across different organization types.

PERCENTAGE OF RESPONDENTS					
	Full Sample	**Largest Organizations (Revenues >$1B)**	**Public Companies**	**Financial Services**	**Not-for-Profit Organizations**
Percentage of organizations dedicating a CRO or equivalent	**43%**	**61%**	**63%**	**60%**	**42%**

KEY INSIGHTS

- Just under two-thirds of the largest organizations, public companies, and financial services organizations have an appointed CRO or equivalent position.
- It is especially interesting is to see that even many not-for-profit organizations are appointing someone to serve as CRO.

The trend in recent years in the percentage of organizations designating an individual to serve as CRO or equivalent seems to be relatively stable, although it is interesting to observe the downward trend for financial services organizations.



KEY INSIGHT

- Larger entities, public companies, and financial services organizations are more likely to have a dedicated risk leader.

ASSIGNMENT OF RISK MANAGEMENT LEADERSHIP

LINES OF REPORTING FOR RISK LEADERS

The overall positioning of the risk champion role within an organization's leadership can directly affect the overall impact that individual can have on the risk management process. While an organization might designate an individual to be the risk leader for the organization, if that individual is too far removed from the senior leadership of the organization, the ERM process is less likely to get visibility and focus from those at the enterprise level.

To get a sense for where the risk champion resides in the leadership structure, we asked respondents from organizations that appointed an individual to serve as CRO or equivalent to whom that individually formally reports.

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	**20%**	**15%**	**5%**	**14%**	**21%**
Chief Executive Officer or President	**47%**	**44%**	**53%**	**63%**	**31%**
Chief Financial Officer	**18%**	**23%**	**30%**	**13%**	**22%**
General Counsel	**8%**	**10%**	**7%**	**4%**	**14%**
Chief Operating Officer	**3%**	**3%**	**2%**	**3%**	**8%**
Other "C-Level" Officer	**3%**	**3%**	**0%**	**3%**	**2%**
Other – Below "C-Level"	**1%**	**2%**	**3%**	**0%**	**2%**

KEY INSIGHTS

- There is a mixture of lines of reporting across different risk champions. Financial services organizations and public companies are more likely to have the risk champion reporting formally to the chief executive officer or president.
- The chief financial officer (CFO) is also often the position overseeing the risk champion's work.

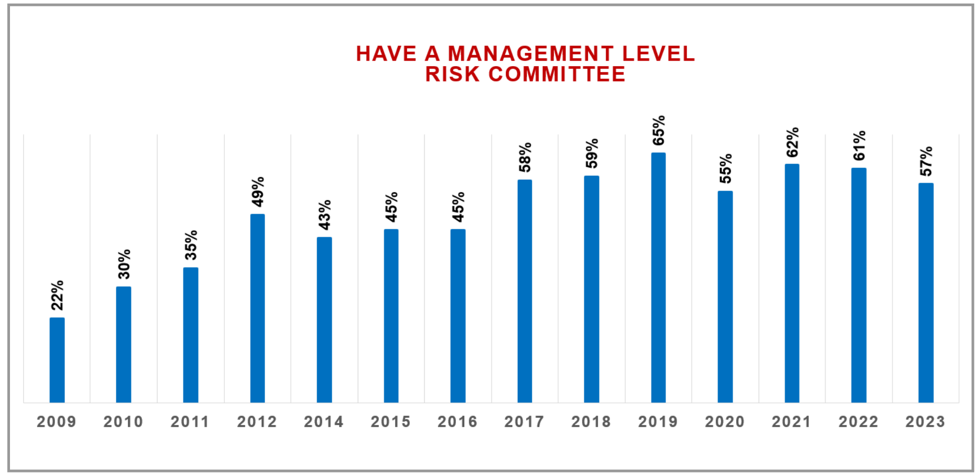
MANAGEMENT LEVEL RISK COMMITTEES

To help organizations develop a more enterprise-wide view of risks, a number of organizations are creating management level risk committees that are comprised of individuals across multiple functions of the organization. Bringing individuals from different functions together to discuss risk issues helps the leadership team develop a more robust, enterprise-wide perspective of how risks might impact the organization as a whole.

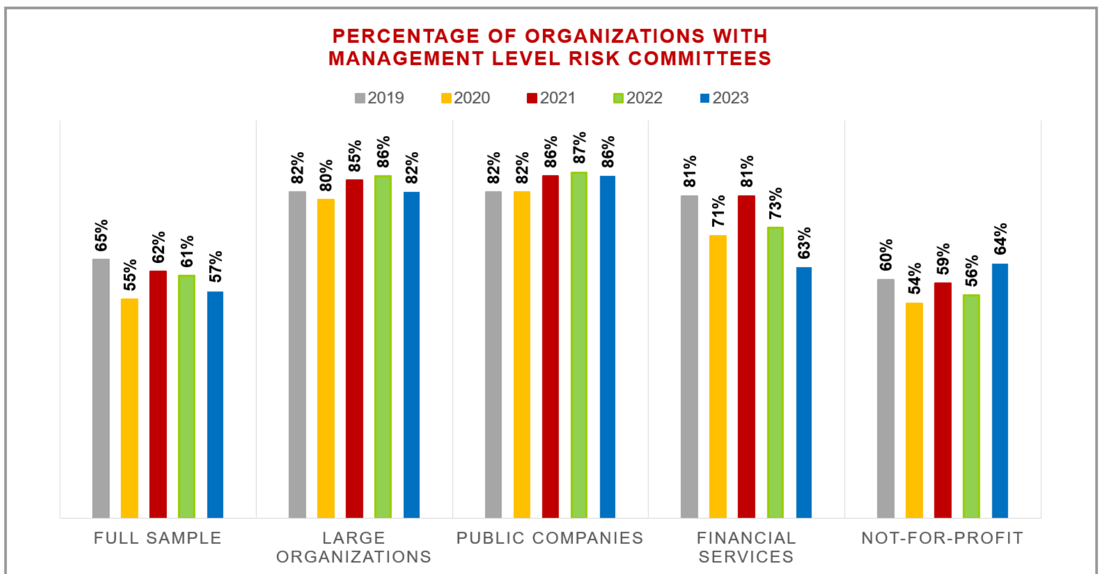
We asked respondents to indicate whether their organization has a management level risk committee.

KEY INSIGHTS

- We observe that a majority of organizations have a management level risk committee or equivalent and that has been the case beginning in 2017.
- While there was a slight drop in that percentage for the current year, events surrounding the economy, talent, supply chains, social unrest, and the war in Ukraine, among other matters, appear to be encouraging organizations to think again about the benefits of an internal management level risk committee.
- Interestingly, the likelihood that an organization has a management level risk committee is higher (at 57%) than the likelihood they have appointed a CRO or equivalent (43%).



Note: We did not issue a report in 2013.



KEY INSIGHT

- The presence of an internal management level risk committee is noticeably more likely to be present in the largest organizations and public companies where 82% and 86% respectively, of those organizations have such a committee. It is important to highlight that risk committees are also common for not-for-profit organizations.

MANAGEMENT LEVEL RISK COMMITTEES

To get a sense for the frequency of meetings for the risk management committee, we asked respondents to indicate the cadence of their meeting schedule.

PERCENTAGE OF RESPONDENTS					
How Frequently Does the Management Level Risk Committee Meet?	**Full Sample**	**Largest Organizations (Revenues >$1B)**	**Public Companies**	**Financial Services**	**Not-for-Profit Organizations**
Semi-Annually	**6%**	**6%**	**4%**	**3%**	**8%**
Quarterly	**49%**	**56%**	**59%**	**47%**	**43%**
Monthly	**33%**	**30%**	**31%**	**41%**	**34%**

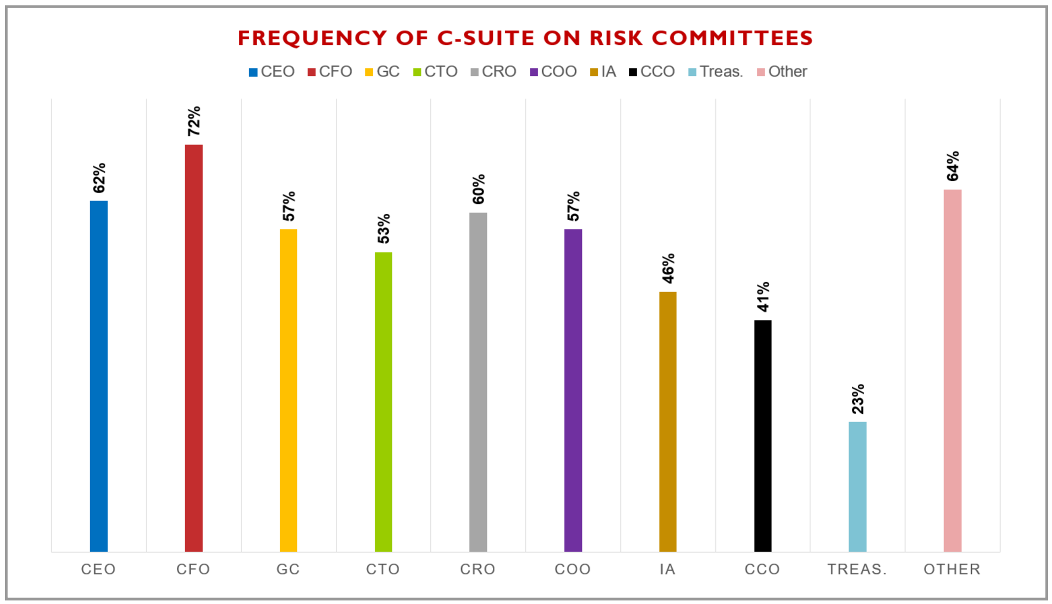
KEY INSIGHT

- For organizations with a formal management level risk committee, those committees most commonly meet on a quarterly basis, although about one-third of them meet on a monthly basis.

For those respondents that indicated their organizations have a risk management committee, we asked them to identify the titles of positions of individuals who serve on the committee to obtain a sense of the overall composition of the committee.

KEY INSIGHTS

- The officer most likely to serve on the executive risk committee is the chief financial officer (CFO), who serves on 72% of the risk committees that exist among organizations represented in our survey.
- The CEO/President serves on 62% of the risk committees.
- Other positions typically represented on the risk management committee include the general counsel (57%), chief technology officer (53%), chief risk officer (60%), and chief operating officer (57%).
- The reason why some positions are not as frequent may be due to the fact the organization does not have an individual with that position title. For example, as noted earlier, not all entities have a chief risk officer position.



RISK IDENTIFICATION AND RISK ASSESSMENT PROCESSES

This section highlights benchmarking information related to techniques entities use to engage management in the identification and prioritization of risks affecting the enterprise.

We Suggest These Questions to Assess Your Organization's Risk Identification and Assessment Processes:

1. What techniques are used to prompt management to identify top risks on the horizon?
2. What types or categories of risks seem to be the primary focus of the entity's risk identification process and what new and emerging categories should be added?
3. To what extent is your organization's ERM process fostering not only consideration of near-term risks but also long-term risks (e.g., 5 to 10 years out)?
4. What processes does your organization use to rank-order the most important risks?
5. Would you describe your risk management process as mostly quantitative or qualitative in nature? What should change to enhance the value of that process for strategic decision-making?

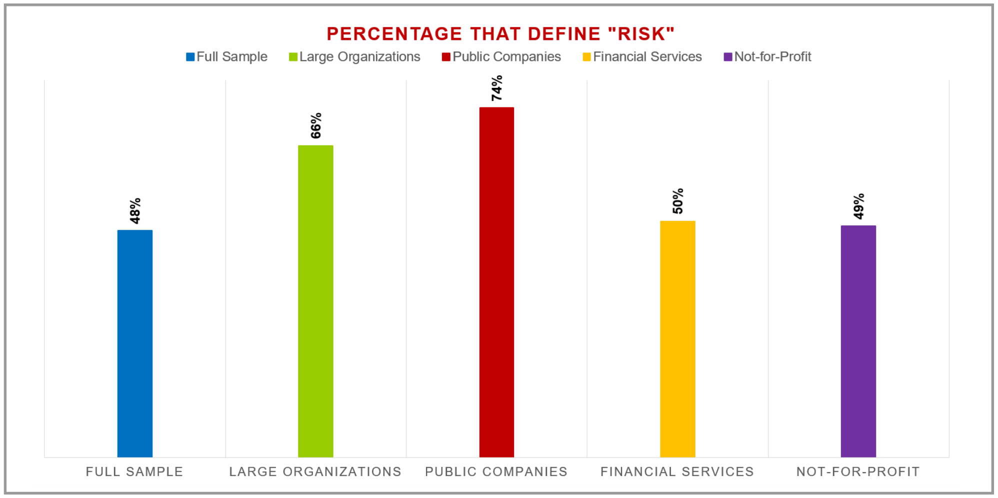
TABLE OF CONTENTS

RISK IDENTIFICATION AND RISK ASSESSMENT PROCESSES

DEFINING MEANING OF "RISK"

As organizations engage business leaders in risk identification tasks, sometimes they face confusion among leaders about what is meant by the term "risk." That can occasionally lead to a lack of clarity as to what leaders should be thinking about as they assess the potential for emerging issues that might trigger risk events for the organization. That may lead to frustration among leaders about the ERM process in general.

To get a sense for whether organizations provide guidance about the kinds of issues management should consider as it thinks about risks, we asked respondents whether or not the organization has formally defined the meaning of the term, "risk."



KEY INSIGHTS

- Just under one-half (48%) of the full sample has formally defined the meaning of the term "risk" for employees to use as they identify and assess key risks.
- Defining "risk" occurs more often for large organizations and public companies.

For those organizations that define the term "risk," we asked them to describe whether that definition focuses mostly on the "downside" of risk (e.g., risks as a threat) or whether it also focuses on the "upside" potential for risks (e.g., risks as an opportunity).

PERCENTAGE OF RESPONDENTS					
The definition of "risk" focuses	**Full Sample**	**Largest Organizations (Revenues >$1B)**	**Public Companies**	**Financial Services**	**Not-for-Profit Organizations**
Both on "upside" risks (risk opportunities) and "downside" risks (threats to the organization)	**66%**	**71%**	**69%**	**62%**	**71%**
Only on "downside" of risks (threats to the organization)	**33%**	**29%**	**29%**	**37%**	**29%**
Neither	**1%**	**0%**	**2%**	**1%**	**0%**

KEY INSIGHT

- If an organization defines the term "risk," the majority focus the definition to emphasize both the "upside" (opportunities for the organization) and "downside" (threats to the organization) of risk.

TABLE OF CONTENTS

FREQUENCY OF RISK IDENTIFICATION UPDATES

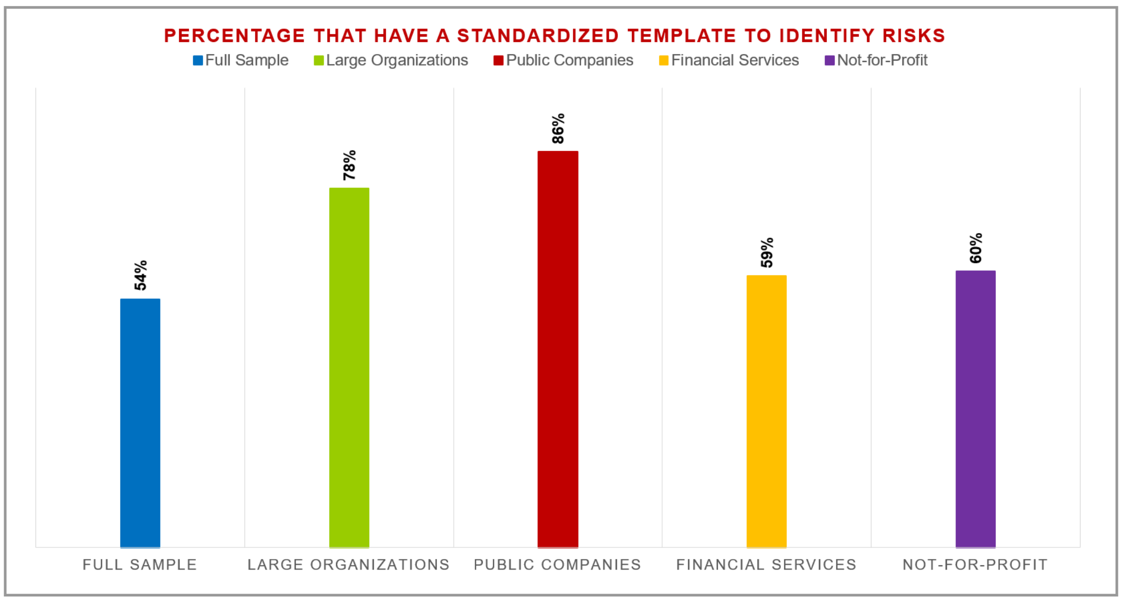
Risks emerge constantly and thus it is important for management to stay abreast of top risks on the horizon for the organization. To get a sense for the frequency of activities organizations engage in to identify risks, we asked respondents to describe how often they go through a dedicated process to update their key risk inventories.

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**
Annually	**39%**	**48%**	**45%**	**40%**	**47%**
Semi-Annually	**11%**	**12%**	**13%**	**10%**	**13%**
Quarterly	**17%**	**22%**	**25%**	**20%**	**18%**
Monthly, Weekly, or Daily	**6%**	**4%**	**7%**	**6%**	**3%**
Not At All	**27%**	**14%**	**10%**	**24%**	**19%**

KEY INSIGHT

- While there is substantial variation as to whether they go through an update process, when organizations do update their risk inventories, it is generally done annually, although a noticeable percentage of organizations update their risk inventories quarterly.

We also asked respondents to indicate whether their organizations use any kind of standardized process or template for identifying and assessing risks.



KEY INSIGHT

- Some form of standardization, such as a template, is commonly used to engage business leaders across an organization in risk identification activities.

RISK IDENTIFICATION AND RISK ASSESSMENT PROCESSES

CATEGORIES OF RISKS

The goal of enterprise risk management is to identify, assess, manage, and monitor any type of risk that might affect the entity's strategic success. All kinds of risks, such as those that are operational, compliance, financial, reputational, or strategic in nature, for example, can be triggered by internal or external issues and events. Unfortunately for some organizations, they limit their focus of risk management to more traditional areas of risks that primarily identify internal operational or compliance issues, with minimal explicit focus on strategic and external areas of emerging risk issues.

We asked respondents to indicate the extent to which their organization's ERM process formally identifies, assesses, and responds to several risk categories. The table below summarizes the percentage that describe their organization's focus as "mostly" to "extensively."

PERCENTAGE OF RESPONDENTS INDICATING EXTENT AS "MOSTLY" TO "EXTENSIVELY"					
To what extent does your organization's ERM process "Mostly" to "Extensively" formally consider these risk categories?	**Full Sample**	**Largest Organizations (Revenues >$1B)**	**Public Companies**	**Financial Services**	**Not-for-Profit Organizations**
Emerging Strategic/Market/Industry Risks	**40%**	**54%**	**59%**	**44%**	**46%**
Operational/Supply Chain/Process Risks	**49%**	**73%**	**78%**	**49%**	**55%**
Financing/Investing/Financial Reporting Risks	**53%**	**71%**	**78%**	**63%**	**56%**
Information Technology System Risks	**62%**	**78%**	**81%**	**71%**	**66%**
Legal Regulatory/Compliance Risks	**60%**	**78%**	**82%**	**71%**	**64%**
Reputational/Political Risk	**45%**	**60%**	**57%**	**53%**	**56%**

KEY INSIGHTS

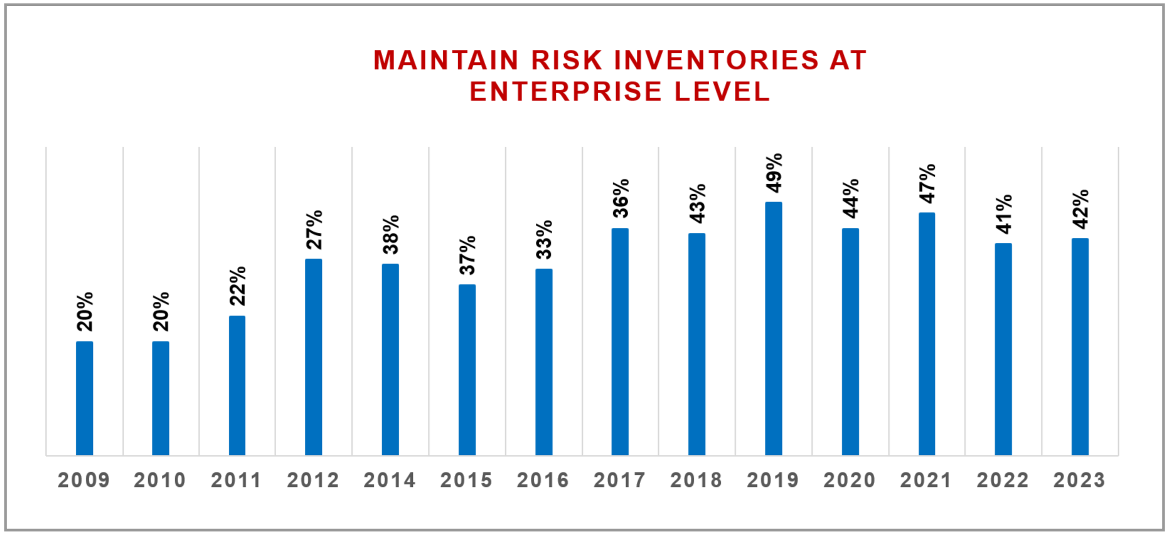
- While most ERM processes focus on a number of different categories of risks, the dominant focus is on risks related to information technology systems, legal regulatory/compliance, and financial related risks.
- ERM processes tend to focus less on emerging strategic/market/industry risks and risks related to reputation/political issues.
- For most types of organizations, their ERM processes are least likely to focus on strategic/market/industry risks relative to other risk areas.

RISK IDENTIFICATION AND RISK ASSESSMENT PROCESSES

USE OF RISK INVENTORIES

As organizations go through the process of identifying risks, they compile that information at an enterprise level to stay abreast of the universe of risks that might impact the organization. Over time, they use risk inventories as a repository of potential risk concerns that they can monitor and track over time. We asked participants to indicate whether they have some process or system to formally maintain an enterprise-level inventory of potential risks to have an aggregate view of the population of risks issues affecting the enterprise.

Less than one-half (42%) of the organizations maintain enterprise-level risk inventories compared to 41% in the prior year. When compared to 2010, we definitely see more awareness of the importance of maintaining an understanding of the universe of risk facing the organization.



Note: We did not issue a report in 2013.

KEY INSIGHTS

- The percentages of organizations that maintain enterprise-level risk inventories is relatively unchanged in the past few years.
- However, the majority of organizations (58%) do not aggregate risk information to have an enterprise-level inventory of top risks. For those organizations, they only track risks within specific business functions, if at all.

The following table shows the breakdown by type of organization.

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	**42%**	**60%**	**61%**	**50%**	**45%**

KEY INSIGHT

- Large organizations and public companies are most likely to maintain an enterprise-level inventory of risks.

EXPLICIT GUIDELINES FOR ASSESSING RISKS

Once risks are identified, management needs to assess the importance of each risk to determine which risks deserve management's attention first. Typically, the assessment of a risk is based on considerations of the probability/likelihood that a risk event might occur and the impact/consequence to the organization should the risk occur. Other dimensions that may be considered include the speed/velocity of a risk and the organization's level of preparedness for managing the risk.

Some organizations provide guidelines to assist management in assessing the likelihood and impact of a risk. We asked respondents to indicate whether their organization provides explicit guidelines or measures to business unit leaders on how to assess the probability or frequency of a risk event and how to assess the impact of a risk event.

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	**41%**	**70%**	**76%**	**47%**	**37%**
Impact	**41%**	**67%**	**79%**	**49%**	**36%**

KEY INSIGHTS

- Less than half 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 (41% for both probability and impact). We found slightly lower results for not-for-profit organizations.
- Consistent with recent years, about two-thirds of the largest organizations and three-fourths of public companies provide explicit guidelines or measures to business unit leaders for them to use when assessing risk probabilities and impact.
- If guidelines are provided, they usually are provided for assessing both likelihood and impact of the risk.

QUALITATIVE VERSUS QUANTITATIVE APPROACHES

Most business leaders prefer to make decisions using quantified data and that desire holds true for decisions related to risk management. That works well when there are structured databases available with data that shed insights about emerging risks that can be analyzed. However, for a number of risks on the horizon, there is a lack of available structured data that might help inform decision making. As a result, management must rely on qualitative versus quantitative data to make a number of strategic decisions.

We asked respondents to provide an overview of whether their organization's risk assessment process is perceived as taking a mostly quantitative approach to risk assessment or whether that process is more qualitative in nature.

PERCENTAGE OF RESPONDENTS					
Quantitative Versus Qualitative Approach to Risk Assessment	**Full Sample**	**Largest Organizations (Revenues >$1B)**	**Public Companies**	**Financial Services**	**Not-for-Profit Organizations**
Mostly Quantitative Assessment (Models)	**1%**	**2%**	**1%**	**2%**	**1%**
A Blend, But More Quantitative	**18%**	**22%**	**25%**	**26%**	**16%**
A Blend, But More Qualitative	**37%**	**48%**	**54%**	**35%**	**44%**
Mostly Qualitative Assessments	**19%**	**23%**	**15%**	**16%**	**23%**
N/A – No Formal Assessment Done	**25%**	**5%**	**5%**	**21%**	**16%**

KEY INSIGHTS

- While organizations, on average, use both a quantitative and qualitative approach to risk assessment, the process tends to be more qualitative than quantitative.
- Even large organizations, public companies, and financial services organizations have a predominantly qualitative approach to risk assessment.

A LONGER-TERM FOCUS ON RISK IDENTIFICATION AND ASSESSMENT

While many ERM programs focus on risks that might emerge within the time horizon of the strategic plan, many are realizing the importance of complimenting a near term risk focus with a long-term risk focus. We wanted to obtain a sense for the extent that organizations are also identifying longer-term risk issues and the extent to which they are using scenario planning techniques to pinpoint potential risk exposures.

We asked two questions specific to this issue.

PERCENTAGE OF RESPONDENTS RESPONDING "MOSTLY" OR "EXTENSIVELY"					
Is there a longer-term focus on risk identification and assessment?	**Full Sample**	**Largest Organizations (Revenues >$1B)**	**Public Companies**	**Financial Services**	**Not-for-Profit Organizations**
To what extent is the organization's risk management process explicitly engaging management in thinking about long-term risks (e.g., risks at least 5-10 years out)?	**18%**	**22%**	**19%**	**22%**	**22%**
To what extent will your organization increase its use of formalized scenario planning activities to anticipate future risks?	**18%**	**25%**	**23%**	**19%**	**21%**

KEY INSIGHTS

- About one-fifth of the respondents indicate that their organization's risk management process is thinking about long-term risks.
- The use of scenario planning is not that common for most organizations.

RISK MONITORING PROCESSES

This section highlights benchmarking information related to techniques entities use to monitor risks over time.

We Suggest These Questions to Assess Your Organization’s Risk Monitoring Process:

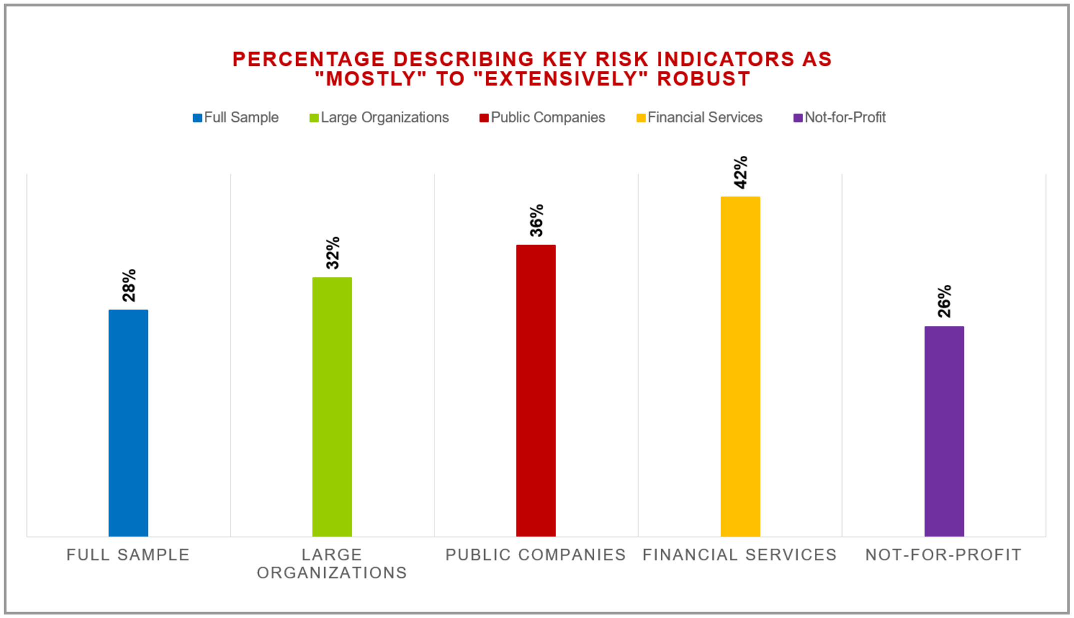
1. What kinds of metrics does your organization use to keep an eye on emerging risk trends?
2. How frequently does the CRO (or other executives) communicate risk information to senior management?
3. How satisfied is senior management with the nature and frequency of risk reports received from the ERM function?

RISK MONITORING PROCESSES

USE OF KEY RISK INDICATORS

Most organizations track a number of key performance indicators (KPIs) that provide an historical lens on how the organization is performing. Management dashboards provide trend information about how KPIs are changing over time. In addition to KPIs, a number of organizations are also including additional metrics that provide a forward-looking, and often external, view of risks that may be emerging on the horizon. These are known as key risk indicators (KRIs), which are metrics that help management begin to identify trends that suggests risks may be emerging.

We asked respondents to describe the overall robustness of their organization's suite of key risk indicators.



KEY INSIGHTS

- There appears to be an opportunity for most organizations to improve the nature and type of key risk indicators included in their management dashboard systems. Across the full sample, only 28% report that their KRIs are "mostly" to "extensively" robust.
- Surprisingly, fewer than one-half of the financial services organizations have KRIs that are "mostly" to "extensively" robust.
- The growing use of data analytics may provide opportunities for management to strengthen their management "dashboards" to include more information that helps track potential risks on the horizon.

RISK MONITORING PROCESSES

FREQUENCY OF RISK COMMUNICATIONS TO SENIOR EXECUTIVES

As chief risk officers and risk committees aggregate and discuss risk information generated by the entity's ERM process, they periodically elevate risk information to the senior executive team, particularly when risks are escalating at a rapid pace. To get a sense about the frequency of communications to senior executives, we asked respondents to indicate how often they communicate key risks to senior executives. Respondents could indicate more than one type of communication frequency.

PERCENTAGE OF RESPONDENTS					
How are key risks communicated to senior executives?	**Full Sample**	**Largest Organizations (Revenues >$1B)**	**Public Companies**	**Financial Services**	**Not-for-Profit Organizations**
Ad hoc discussions at management meetings	**40%**	**28%**	**25%**	**35%**	**35%**
Scheduled agenda discussion at management meetings	**24%**	**27%**	**25%**	**26%**	**27%**
Monthly written risk report submitted by management	**4%**	**5%**	**7%**	**4%**	**3%**
Quarterly written risk report submitted by management	**18%**	**25%**	**28%**	**25%**	**16%**
Annual written risk report submitted by management	**14%**	**15%**	**15%**	**10%**	**19%**

KEY INSIGHTS

- Across the full sample, risk communications to senior management are most likely to be *ad hoc* and reported as part of other management meetings.
- About one-quarter of organizations communicate risk information to senior executives as part of a scheduled agenda discussion at management meetings, while many provide a written report submitted to management usually on a quarterly basis.

BOARD RISK OVERSIGHT STRUCTURE

This section highlights benchmarking information related to how the board of directors organizes its risk oversight processes.

We Suggest These Questions to Assess Your Board's Risk Oversight Structure:

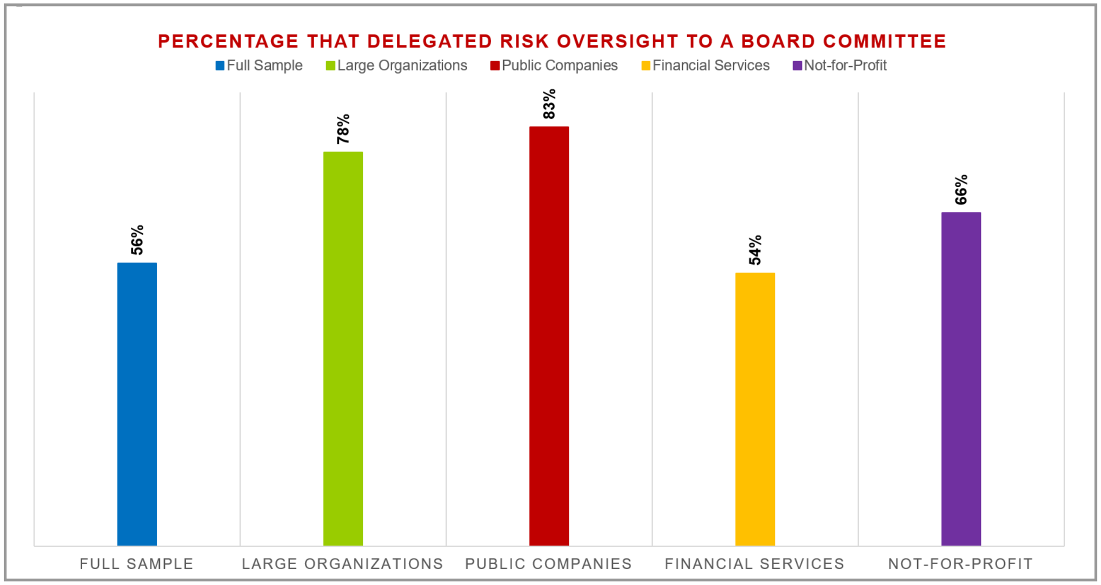
1. How does your board of directors manage its responsibility for risk oversight?
2. To what extent does your board of directors delegate risk oversight to a subcommittee? If they do, which committee is most likely to be responsible for risk oversight?
3. Do board committee charters formally describe responsibilities for risk oversight?
4. Has your organization established a formal policy on enterprise risk management?

BOARD RISK OVERSIGHT STRUCTURE

DELEGATION OF RISK OVERSIGHT

An entity's board of directors has primary responsibility for overseeing management's risk-taking actions on behalf of shareholders. Ultimately, it is the board's responsibility to ensure that management is not taking risks beyond the appetite of the entity's key stakeholders. Board risk oversight is an important aspect of board governance.

A number of boards delegate their risk oversight responsibilities to others. We asked respondents to indicate whether their organization's board of directors has delegated risk oversight to a board-level subcommittee.



KEY INSIGHTS

- More often than not, boards of directors assign formal responsibility for overseeing management's risk assessment and risk management process to a board committee.
- Delegation of risk oversight to a board subcommittee is most common among large organizations and public companies.

BOARD RISK OVERSIGHT STRUCTURE

BOARD SUBCOMMITTEE WITH PRIMARY OVERSIGHT RESPONSIBILITY

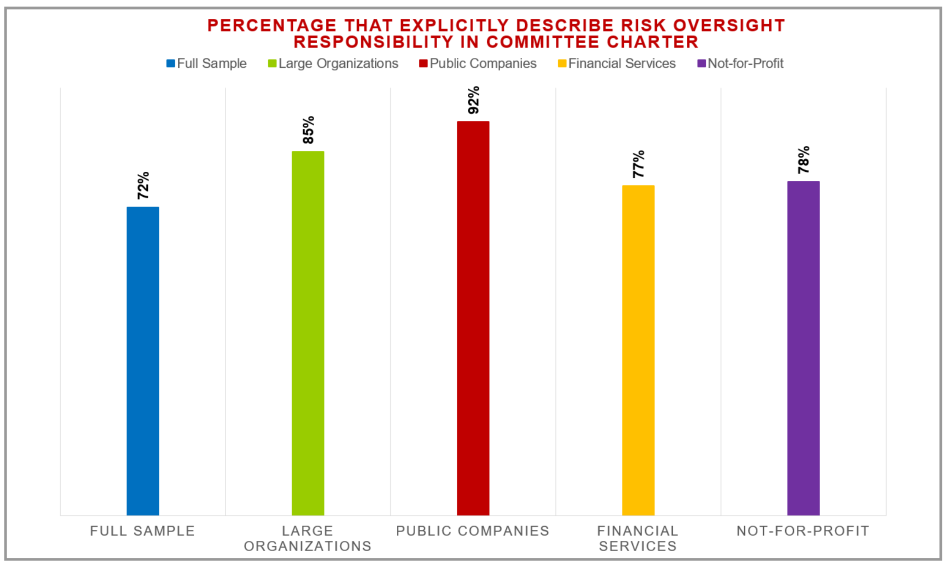
We asked respondents of those organizations whose board of directors delegates responsibility to a subcommittee to indicate which committee is the recipient of that delegation. The table below summarizes the key findings.

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	**49%**	**65%**	**66%**	**27%**	**59%**
Risk committee	**27%**	**25%**	**32%**	**60%**	**15%**
Executive committee	**12%**	**4%**	**1%**	**8%**	**9%**
Corporate governance committee	**4%**	**2%**	**1%**	**2%**	**2%**
Other	**8%**	**4%**	**0%**	**3%**	**15%**

KEY INSIGHTS

- If the board delegates risk oversight responsibility to a board subcommittee, the audit committee most often is the recipient of that designation, except for financial services organizations.
- Financial services organizations are most likely to have a board level risk committee that is responsible for the board's risk oversight, although an increasing number of public companies have risk committees.

We also asked whether the subcommittee with delegated risk oversight responsibility has explicitly noted that responsibility in the committee's charter.

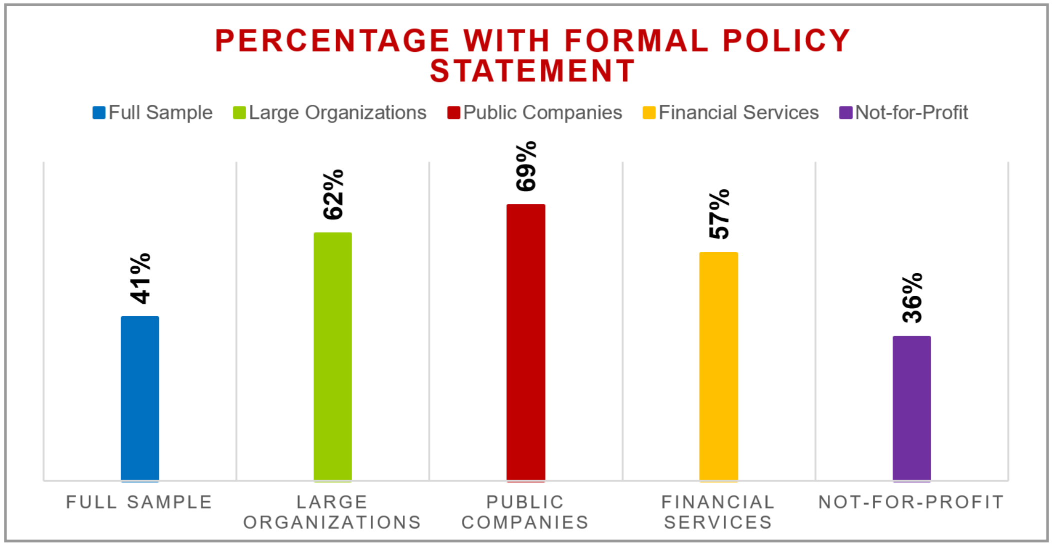


KEY INSIGHT

- Most board committees responsible for risk oversight explicitly describe that responsibility in the committee's charter.

FORMAL POLICY ON RISK MANAGEMENT

Some organizations have prepared formal policy statements articulating the organization's approach to risk management. We asked respondents to indicate whether their organization has issued a formal policy regarding its enterprise-wide approach to risk management.



KEY INSIGHTS

- The presence of a formal risk management policy statement is mixed across organizations, with fewer than half of all organizations in our survey having such a statement.
- The largest organizations and public companies, however, are noticeably more likely to have a formal risk management policy statement relative to other types of organizations.
- Not-for-profit entities are least likely to have a formal risk management policy statement.

BOARD REPORTING AND MONITORING

This section highlights benchmarking information related to the nature and frequency of risk reporting to the board of directors and how the board uses risk information provided to it by management.

We Suggest These Questions to Assess Board Reporting and Monitoring Activities:

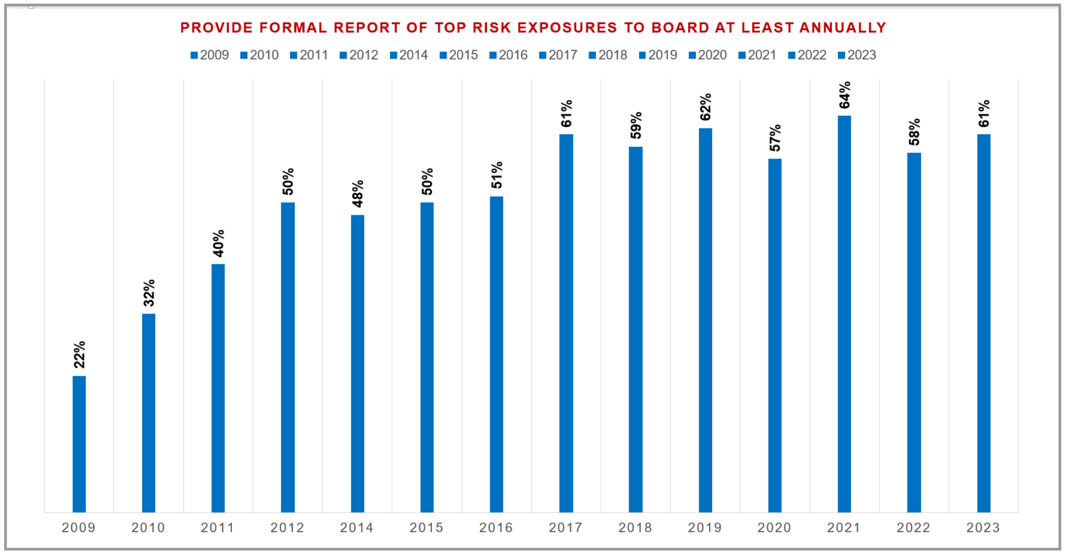
1. How frequently does management prepare formal risk reports for the board?
2. How many top risk exposures does management generally share with the board?
3. To what extent does the board consider risk information as part of the board's engagement in strategic planning and oversight?
4. How are public disclosures of risks to external stakeholders changing over time?

BOARD REPORTING AND MONITORING

FORMAL REPORT ON TOP RISKS TO BOARD

A major responsibility of the board of directors is to oversee the nature of risk-taking on the part of management. As part of their governance responsibilities, boards engage in discussions with management about risks on the horizon. While those discussions are ongoing with boards, we are especially interested in the nature and types of risk reporting by management to the board. We asked a series of questions to better understand the nature of risk reporting.

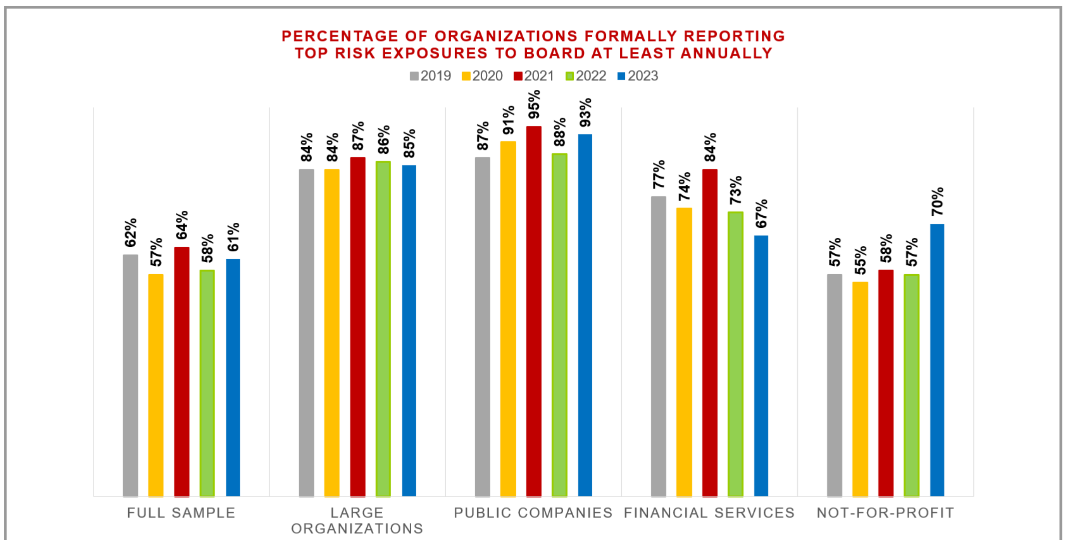
We asked respondents whether management provides a formal report describing the entity's top risk exposures to a committee of the board of directors or the full board at least annually.



Note: We did not issue a report in 2013.

KEY INSIGHTS

- Management reporting to the board about top risks has increased slightly over the past decade.
- Almost two-thirds of the full sample prepares a formal report on top risks to the board at least annually, although that is a smaller percentage than those doing so in 2021.



KEY INSIGHTS

- The percentages of organizations providing a formal report of top risks to the board has remained fairly steady for the largest organizations and public companies, but declined for financial services organizations.
- Formal risk reporting to the board increased noticeably for not-for-profit organizations.

FORMAL REPORT ON TOP RISKS TO BOARD

For those that report top risks to the board at least annually, we also asked respondents to indicate the frequency of that reporting.

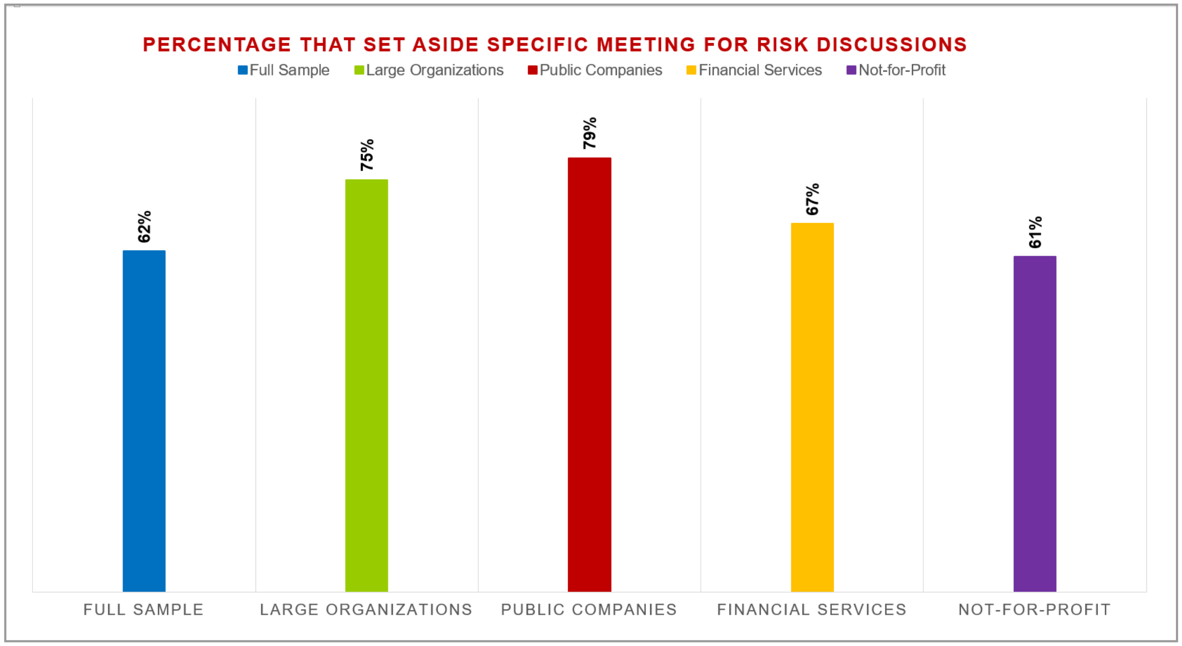
PERCENTAGE OF RESPONDENTS					
How often is the report of top risks reported to the board?	**Full Sample**	**Largest Organizations (Revenues >$1B)**	**Public Companies**	**Financial Services**	**Not-for-Profit Organizations**
Annually	**43%**	**50%**	**48%**	**27%**	**53%**
Quarterly	**41%**	**38%**	**42%**	**55%**	**36%**
At every meeting	**16%**	**12%**	**10%**	**18%**	**11%**

KEY INSIGHTS

- More organizations report top risks to the board on an annual basis, followed by reporting on a quarterly basis. The exception is financial services organizations that are more likely to report quarterly than annually.
- 16% of organizations report top risk exposures to the board at every board meeting.

DEDICATED MEETING TO DISCUSS AGGREGATE REPORT OF TOP RISKS

While management teams generally formally present a report of top risks to the board at least annually, we also wanted to get a sense for how often the board sets aside agenda time at a specific meeting of the board to talk about the top risk exposures. Most ERM processes engage management in an annual process to identify and prioritize the top risks. We are interested in understanding if the board explicitly focuses a meeting of the board on these top risks.



KEY INSIGHT

- The majority of boards set aside a specific meeting to discuss the aggregate report of top risk exposures facing the organization, particularly for large organizations and public companies.

NUMBER OF TOP RISKS REPORTED TO BOARD

It is management's responsibility to manage risks impacting an organization's achievement of objectives. While the board does not need to be apprised of all the risks being tracked by management, generally boards prioritize their efforts on the most important risks. We asked respondents to indicate the number of risk exposures formally presented 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	**42%**	**13%**	**11%**	**37%**	**32%**
Between 5 and 9 risks	**26%**	**26%**	**27%**	**32%**	**31%**
Between 10 and 19 risks	**24%**	**49%**	**51%**	**20%**	**26%**
20 or more risks	**8%**	**12%**	**11%**	**11%**	**11%**

KEY INSIGHTS

- There is noticeable variation in the number of top risk exposures reported to the board across different types of organizations.
- For the full sample, 68% of organizations report nine or fewer risks to the board; however 78% of public companies report between five and 19 risk exposures to the board.
- Reporting 20 or more risks to the board is least common.

BOARD REPORTING AND MONITORING

RISK DISCUSSIONS AS PART OF BOARD'S STRATEGY DISCUSSIONS

A primary objective of an ERM process is to help management and the board identify, assess, manage, and monitor risks that might impact the organization's strategic success. Risk information should inform both management and the board on issues that might affect the success of that plan and it should also help them identify opportunities for increased risk taking.

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.

PERCENTAGE OF RESPONDENTS					
Extent that 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**
Not at All	18%	8%	6%	13%	14%
Minimally	21%	24%	24%	20%	22%
Combined	**39%**	**32%**	**30%**	**33%**	**36%**

KEY INSIGHTS

- The integration of risk information with discussion of the strategic plan is not occurring in about one-third of most organizations.
- There may be opportunities to enhance the integration of risk information with strategic planning information for most organizations.

TABLE OF CONTENTS

BOARD REPORTING AND MONITORING

IMPACT ON RISK FACTOR DISCLOSURES

Public companies are required by the United States Securities and Exchange Commission (SEC) to discuss the top risks facing the entity in its Item 1.A. of the Form 10-K filed with the SEC annually. An ERM process should inform management of the risks that should be included in the Form 10-K disclosure. While other non-public organizations are not subject to similar requirements, there may be other pressures for more public disclosure about top risks to external stakeholders. We asked respondents to indicate the extent their organization's public risk disclosures have increased in the past five years.

PERCENTAGE OF RESPONDENTS RESPONDING "MOSTLY" TO "EXTENSIVELY"					
	Full Sample	**Largest Organizations (Revenues >$1B)**	**Public Companies**	**Financial Services**	**Not-for-Profit Organizations**
To what extent has your organization's public disclosures of risk to external stakeholders increased in the past five years?	**15%**	**23%**	**36%**	**24%**	**10%**

KEY INSIGHTS

- Organizations of all types are perceiving an increase in the public disclosure of risk information to external stakeholders.
- Public companies are especially increasing the extent of public disclosures of risk information to external parties.

CALLS TO ACTION

This report provides extensive benchmarking information that executives can use to assess the overall state of their organization's approach to risk oversight. While the findings in this study indicate some progress in how organizations are proactively managing risks on the horizon, many of the findings suggest boards of directors and senior executives may still need to engage in robust and honest assessments regarding their organization's current capabilities for managing the ever-changing landscape of risks on the horizon.

This final section highlights a number of calls to action executives can consider to strengthen their organization's approach to enterprise-wide risk management.

We Suggest These Questions to Assess Your Organization's Overall Approach to Risk Management:

1. What about our organization's approach to risk management is working well?
2. What aspects of our organization's approach need to be enhanced?
3. What are the top action-items for strengthening the integration of risk information into strategic decision making for our enterprise?
4. What should be tackled first?

TABLE OF CONTENTS

WHAT ARE MANAGEMENT'S PERCEPTIONS ABOUT THE CURRENT APPROACH TO RISK MANAGEMENT

If an organization opens its doors to do business today, then realistically the organization is managing risks. So many business leaders quickly conclude that they are effectively engaged in risk management. However, it is important for ERM leaders to obtain feedback from senior executives about their perspectives regarding the organization's current approach to risk management.

QUESTIONS TO CONSIDER

- Does the organization's risk management process mostly focus on pockets or silos of risks impacting particular business functions and operations, and is that process leading to a top-down, holistic view of the entity's most critical risks impacting its strategic objectives?
- Is the coordination and implementation of risk management activities across the organization mostly *ad hoc* or informal?
- To what extent does that process help executives and boards see related risks emerging across different silos of the business that might snowball into bigger, enterprise-wide issues?
- Does the existing risk management process tend to focus on already known risks mostly linked to internal operations and compliance issues?
- Would most employees describe the organization's risk management process as bureaucratic and non-value adding?
- How effective is that process in prompting management to think outside the status quo to pinpoint unknown, but knowable risks?
- Is management's focus on risk including both short-term (e.g., next 2-3 years) and long-term risks (e.g., a decade from now)?

IS THERE CONSENSUS ABOUT THE MOST SIGNIFICANT ENTERPRISE RISKS?

Many executives believe the uncertainties associated with the rapid pace of change in the global business environment is triggering an ever-evolving and expanding portfolio of risks on the horizon for most organizations. If executives fail to stay in constant dialogue about emerging risk issues, they may find themselves chasing after the wrong risks or they may actually be creating risks for other parts of the organization as they manage risks within their area of responsibility.

QUESTIONS TO CONSIDER

- To what extent is the senior executive team engaging in dialogue about the top enterprise-level risks and reaching consensus about those most critical to the organization?
- Is ownership and accountability for managing enterprise level risks clear to those involved?
- Does the senior executive team understand how the organization is responding to top risk exposures and are they confident those responses are actually implemented and effective?
- How often is management engaging in robust discussion with the board of directors about the top risks and is there agreement between management and the board about the most critical risks to the organization?

HOW IS THE OUTPUT FROM RISK MANAGEMENT USED IN STRATEGIC PLANNING?

Most executives understand the reality that the organization must be willing to take risks in order to generate higher returns. But unfortunately, our survey results find that only a small percentage of organizations view their risk management activities as providing important strategic value. Less than half of the organizations formally consider existing risk exposures when evaluating new possible strategic opportunities and less than one-fourth of the organizations have their boards of directors formally discuss risk exposures when they discuss the strategic plan.

QUESTIONS TO CONSIDER

- Why is the organizations' risk management process failing to provide important strategic information about risks on the horizon?
- Is the current risk management process focused too heavily on operational or compliance issues?
- Are the top risks identified by the risk management process mapped to the most important strategic initiatives?
- To what extent is the risk management process prompting management to look outside the entity for external events that might trigger risks for the enterprise?
- Does the existing risk management process frame the task of identifying risks from the organization's core value drivers and new strategic initiatives in the strategic plan?
- How frequently do risk management leaders and those leading the strategic planning process interact?
- Would most employees describe the organization's risk management process as bureaucratic and non-value adding?

DOES MANAGEMENT HAVE ACCESS TO ROBUST KEY RISK INDICATORS?

Our survey results find that a relatively small percentage of organizations have a robust set of metrics included in their management dashboards to help them keep an eye on shifting risk conditions. Most organizations have a tremendous amount of key performance indicators (KPIs) to help them monitor the performance of the business. However, it is important to remember that KPIs are historical in nature and they tend to focus on things internal to the enterprise.

QUESTIONS TO CONSIDER

- To what extent does management have metrics that are forward looking and that are based on monitoring both internal and external trends?
- How would management know that one of its top risk concerns is escalating?
- What would the warning signs be?
- Who among the management team is monitoring those signals?
- Are there clear "trigger points" that signal when action must be taken?
- How easy would it be for executives to override pre-established trigger points?

CALLS TO ACTION

IS OUR ENTITY SUFFICIENTLY PREPARED TO MANAGE A SIGNIFICANT RISK EVENT?

The worst time for an organization to discover a lack of risk management preparedness is during the risk event itself. Unfortunately, there have been a number of events impacting large, well-known organizations that seem to suggest that management was ill-prepared to navigate the risk event, causing tremendous brand and reputational harm. While a robust enterprise-wide risk management process cannot be expected to prevent all types of risks that might emerge, organizations that invest time and resources in engaging senior executives and boards in more robust risk management discussions and dialogue on an ongoing basis find that they are in a better position to deal with a significant risk event should one emerge.

QUESTIONS TO CONSIDER

- To what extent is the organization's risk management process helping to strengthen the organization's resiliency by preparing for the reality that disruption is inevitable?
- How confident are senior executives in their ability to navigate a significant risk event? What is the basis for that confidence?
- To what extent might management be "blindsided" by unexpected risk events? How vulnerable is the organization to blind-spots similar to those that led to other organizations' risk management failures?
- Does management and the board have a detailed "playbook" of how they will respond should one of the organization's top risk exposures emerge in a significant way?
- To what extent is the entity prepared to navigate a risk event that has gone viral over social medial platforms?

SUMMARY

This 14th Edition of **The State of Risk Oversight** provides extensive information about the current level of risk management capabilities in organizations in 2023 that shed important perspectives about opportunities to strengthen the value of risk insights for strategic decision making. It is our hope that this report highlights a number of ways entities can realize how proactive consideration of emerging risks can position an organization for competitive advantage.

While there are steady improvements in overall risk management practices over the 14 years we have conducted this study, our data suggests that business leaders still struggle to recognize and embrace the benefits that proactive and robust risk management can provide for creating strategic value for the organization. Given the speed of change and rapidly developing innovations in today's fast-paced global business environment, it is our conclusion that risk management is not getting easier, but more critical. Failing to address that reality may have serious strategic consequences for organizations who continue to take a status quo approach to risk management.

We hope that the extensive data in this report can prompt business leaders to identify gaps in their organization's risk management maturity that should be addressed. Engaging in serious consideration of the numerous questions we provide at the beginning of each section and honestly evaluating the Calls to Action (see page 60) will hopefully assist executives and boards in their efforts to strengthen the strategic value of their risk management practices. Hopefully, that will lead to enhanced risk intelligence that leaders can use for strategic decision making.

NC State ERM Initiative's web site and the AICPA's ERM website provide a number of resources to help executives and boards understand their responsibilities for risk oversight and effective tools and techniques to help them in those activities. We encourage executives and boards to take advantage of those resources provided.

APPENDIX A: OVERVIEW OF RESPONDENT DEMOGRAPHICS

This is the fourteenth 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 first few months of 2023 through an online survey instrument 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 454 fully completed surveys. This report summarizes our findings.

DESCRIPTION OF RESPONDENTS

Respondents completed an online survey consisting of over 40 questions that sought information about various aspects of risk oversight within their organizations. Most of those questions have been the same across all fourteen editions of the surveys that we have conducted each year from 2009-2023.

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 21% of respondents having the title of chief financial officer (CFO), 12% serving as chief risk officer (CRO), 7% as controller, and 10% leading internal audit, with the remainder representing numerous other executive positions.

The respondents represent a broad range of industries. The most common industries responding to this year's survey were finance, insurance, and real estate (26%) and services (26%). Just over one-quarter of the respondents work in not-for-profit organizations. The mix of industries is generally consistent with the mix in our previous reports.

The respondents represent a variety of sizes of organizations. As shown in the table on the next page, 44% of organizations have revenues $100 million or lower while 32% have revenues over $1 billion. So, there is nice variation in organization size in our sample. Almost all (89%) of the organizations are based in the United States.

INDUSTRY (SIC CODES)	PERCENTAGE OF RESPONDENTS
For-Profit Entities:	
Finance, Insurance, Real Estate (SIC 60-67)	**26%**
Services (SIC 70-89)	**26%**
Manufacturing (SIC 20-39)	**11%**
Retail (SIC 52-59)	**3%**
Wholesale/Distribution (SIC 50-51)	**2%**
Transportation (SIC 40-49)	**2%**
Construction (SIC 15-17)	**1%**
Mining (SIC 10-14)	**1%**
Agriculture, Forestry, Fishing (SIC 01-09)	**1%**
Not-for-Profit (SIC N/A):	
Government Agencies, Universities, Non-Profits	**27%**

APPENDIX A: OVERVIEW OF RESPONDENT DEMOGRAPHICS

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 94 publicly traded companies, 119 financial services entities, and 121 not-for-profit organizations included in our sample.

RANGE OF REVENUES IN MOST RECENT FISCAL YEAR	PERCENTAGE OF RESPONDENTS[2]
$0 <x < $10 million	**25%**
$10 million < x < $100 million	**19%**
$100 million < x < $500 million	**15%**
$500 million < x < $1 billion	**9%**
$1 billion < x < $2 billion	**8%**
$2 billion < x < $10 billion	**14%**
x > $10 billion	**10%**

2 Forty-two of the 454 respondents did not provide information about revenues. The data reported in this table reflects the percentages based on the 412 that provided revenue information.

APPENDIX B: ASSESSING CULTURE AND LEADERSHIP SUPPORT FOR ERM

Assessing the focus and commitment to risk management by the organization's leadership team is critical for ensuring that an appropriate environment and tone at the top is being communicated about the strategic importance of ERM. Consider having several members of management or the board of directors individually answer the following questions. Ask them to think about the organization's enterprise-wide approach to risk management as they answer each question. Then, have them meet to discuss differences in answers to facilitate a conversation about the effectiveness of the organization's approach to risk oversight.

	YES	NO
Does the organization's risk management process mostly focus on pockets or silos of risks impacting particular business functions or operations without leading to a top-down, holistic view of the entity's most critical risks impacting its strategic objectives?		
Is the coordination and implementation of risk management activities across the organization mostly *ad hoc* or informal?		
Does the organization's risk management process help executives and boards see related risks emerging across different silos of the business that might snowball into bigger, enterprise-wide issues?		
Does the existing risk management process tend to focus on already known risks mostly linked to internal operations and compliance issues?		
Would most employees describe the organization's risk management process as bureaucratic and non-value adding?		
Is that process effective in prompting management to think outside the status quo to pinpoint unknown, but knowable risks?		
Does the senior executive team engage in dialogue about the top enterprise-level risks and reaching consensus about those most critical to the organization?		
Is ownership and accountability for managing enterprise level risks clear to those involved?		
Does the senior executive team understand how the organization is responding to top risk exposures and are they confident those responses are actually implemented and effective?		
Does the board of directors engage in robust discussion about the top risks and is there agreement between management and the board about the most critical risks to the organization?		
Is the organizations' risk management process providing important strategic information about risks on the horizon?		
Is the current risk management process focused too heavily on operational or compliance issues?		
Are the top risks identified by the risk management process mapped to the most important strategic initiatives?		
Does the risk management process prompt management to look outside the entity for external events that might trigger risks for the enterprise?		
Does the existing risk management process frame the task of identifying risks from the organization's core value drivers and new strategic initiatives in the strategic plan?		
Do risk management leaders and those leading the strategic planning process interact frequently?		
Does management have metrics that provide forward looking insights about emerging risks that are based on both internal and external trends?		
Does management's dashboard include data to help them know that one of the entity's top risk concerns is escalating?		
Are key members of management assigned responsibility for monitoring those emerging risk signals?		
Are there clear emerging risk "trigger points" that signal when action must be taken?		
Can pre-established risk limits or risk trigger points be easily overridden by executives?		
Are senior executives adequately prepared to navigate a significant risk event?		
Does management have "blindspots" that are keeping them from recognizing vulnerabilities that would lead to significant risk events for the organization?		
Does management and the board have a detailed "playbook" of how they will respond should one of the organization's top risk exposures emerge in a significant way?		
Is the organization adequately prepared to navigate a risk event that has gone viral overnight over social media platforms?		
Does the board challenge senior management by asking probing questions about competence, internal controls, incentives, labor relations, regulations, sustainability and other related issues and trends?		
Does management have a process in place to assess risk proactively as significant changes, such as entering new markets, disruptive innovations, regulatory, economic/geopolitical shifts, and other events occur?		
Does the entity design the ERM process to proactively address emerging significant risk areas (i.e. sustainability)?		
Is the organization's leadership focusing both on near-term (e.g., next 2-3 years) and long-term risks (e.g., a decade from now)?		
Is the organization's risk management process helping business leaders prepare for the realities of ongoing disruptions that impact organizational resiliency?		

TABLE OF CONTENTS

AUTHOR BIOS

Both authors serve in leadership positions within the Enterprise Risk Management (ERM) Initiative at NC State University (https://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 Alan T. Dickson Distinguished Professor of Accounting 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 100 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.

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

NC STATE Poole College of Management
Enterprise Risk Management Initiative