



THE FUTURE  
OF THE AMERICAN  
**BOARD**

# RISK COMMITTEE BLUEPRINT

Guidance for Board Risk Oversight

In Partnership With  MarshMcLennan



## ABOUT NACD

The National Association of Corporate Directors (NACD) is the premier membership organization for board directors who want to expand their knowledge, grow their network, and maximize their potential.

As the unmatched authority in corporate governance, NACD sets the standards of excellence through its research and community-driven director education, programming, and publications. Directors trust NACD to arm them with the relevant insights to make high-quality decisions on the most pressing and strategic issues facing their businesses today.

NACD also prepares leaders to meet tomorrow's biggest challenges. The [NACD Directorship Certification](#)<sup>®</sup> is the leading director credential in the United States. It sets a new standard for director education, positions directors to meet boardroom challenges, and includes an ongoing education requirement that prepares directors for what is next.

With an ever-expanding community of more than 23,000 members and a nationwide chapter network, our impact is both local and global. NACD members are driven by a common purpose: to be trusted catalysts of economic opportunity and positive change—in business and in the communities we serve.

To learn more about NACD, visit [www.nacdonline.org](http://www.nacdonline.org).

## Marsh McLennan ABOUT MARSH MCLENNAN

**Marsh McLennan** (NYSE: MMC) is the world's leading professional services firm in the areas of risk, strategy, and people. The Company's more than 85,000 colleagues advise clients in 130 countries. With annual revenue of over \$20 billion, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses. **Marsh** provides data-driven risk advisory services and insurance solutions to commercial and consumer clients. **Guy Carpenter** develops advanced risk, reinsurance and capital strategies that help clients grow profitably and pursue emerging opportunities. **Mercer** delivers advice and technology-driven solutions that help organizations redefine the world of work, reshape retirement and investment outcomes, and unlock health and wellbeing for a changing workforce. **Oliver Wyman** serves as a critical strategic, economic and brand advisor to private sector and governmental clients. For more information, visit [marshmclennan.com](http://marshmclennan.com) and follow us on [LinkedIn](#) and [Twitter](#).



## ABOUT MYLOGIQ

The *Risk Committee Blueprint* leverages data from **MYLOGIQ** – Multidimensional Public Company Intelligence to create a snapshot of what boards look like. Their data has been cited as the source where utilized.

© Copyright 2023, National Association of Corporate Directors. All rights reserved.

Except as permitted under the US Copyright Act of 1976, no part of this publication may be reproduced, modified, or distributed in any form or by any means, including, but not limited to, scanning and digitization, without prior written permission from NACD.

This publication is designed to provide authoritative commentary in regard to the subject matter covered. It is provided with the understanding that neither the authors nor the publisher, the National Association of Corporate Directors, is engaged in rendering legal, accounting, or other professional services through this publication. If legal advice or expert assistance is required, the services of a qualified and competent professional should be sought.



# About the Future of the American Board

**What is the Future of the American Board Initiative?** NACD convened the Future of the American Board Commission—a diverse, influential group of seasoned board leaders from top private and public companies and notable governance practitioners from across the investor, regulatory, and academic communities—to help guide boards through an increasingly turbulent and unpredictable future.

The Commission's perspectives and experiences shaped a [comprehensive framework](#) for board governance centered on 10 Key Principles that boards can use and adapt to ensure they are fit for the future. This framework, released in the fall of 2022, is accompanied by a set of practical blueprints focused on the shifting roles of the key board committees, issued in the spring of 2023. Partners leading these working groups include KPMG (audit committee), Marsh McLennan (risk committee), Pearl Meyer (compensation committee), and Korn Ferry (nominating and governance committee).

**What are the main takeaways?** The report's 10 Key Principles provide guidance for boards that is rooted in progress American boards have made since NACD issued the first set of Key Agreed Principles in the wake of the global financial crisis of 2008. These updated principles are reflective of intensifying pressures and expectations that will affect companies and their governance in the coming years. Most important, in a world that seems less governable, the quality of board governance will be increasingly vital to the sustainability of our enterprises and trust in our market economy.

**How to use the report and the committee blueprints:** What is different about the report is that the Commission developed high-level principles with key questions that are meant to spur board discussion on critical improvements. The Commission understood that prescriptive, one-size-fits-all advice wouldn't be effective for individual boards and companies. The Commission expects that as boards confront these questions, they will come to different conclusions based on their level of maturity, the strategies they are pursuing, and the pressures they are facing. The four blueprints help translate the Commission's principles into practical guidance at the board-committee level.



# RISK COMMITTEE BLUEPRINT

## Introduction

**This blueprint is a call to action for boards to assess if their risk oversight is fit for purpose as they face an increasingly demanding risk agenda.**

Recent events, including the impacts of the global pandemic, supply chain issues, talent shortages, macroeconomic factors, and shocks in the financial sector, have challenged most organizations' risk management. Looking forward, organizations must respond to the impacts of long-term structural shifts, including climate change, demography, (de)globalization, and digitalization.

Against this backdrop, the demands and scrutiny placed on organizations' risk oversight and governance are expanding across three dimensions. First, the breadth and range of risks that boards must oversee continue to grow to include environmental impacts; artificial intelligence (AI); cyber risk; human rights; and employee mental health to list only a few. Second, boards must have a deeper and fuller understanding of how their organizations are responding to and managing individual risks, risk aggregation, risk concentration, and complex interconnections. Third, oversight perimeters are expanding to include risks inherited from the enterprise network—for example, cyber risks within critical third parties or environmental, social, and governance (ESG) performance within supply chains.

In response, boards and directors should focus on how, and if, they are prepared to execute these new expectations for risk oversight. This includes considerations of the board structure and coordination for a complex risk agenda, whether enabled by a board risk committee, other board committees, or the full board; directors' risk oversight expertise and skill sets; the necessary information flow for directors to perform their responsibilities; and the board agenda and calendars to ensure the right issues are discussed at the right time. (See Illustration 1.)

## ILLUSTRATION 1: KEY TAKEAWAYS

Directors should consider if the board and its committees have the mandate, members, information, and agenda to execute on their expanded risk oversight responsibilities



Source: Marsh McLennan

The *Risk Committee Blueprint* provides guidance for boards to elevate risk oversight. Report recommendations build on previous risk governance guidelines prepared by NACD and were guided by a Working Group of eight members with board roles on public and private companies and nonprofit organizations. In addition, the report includes insights and research from Marsh McLennan, the world's leading professional services firm in the areas of risk, strategy, and people, and research from NACD and elsewhere.

# The Evolving Risk Environment

An evolving business environment interacting with a growing focus on stakeholder capitalism is driving ongoing changes to many organizations' risk exposures:

- ▶ The magnitude of risk events that converge and compound one another are resulting in cascading and converging impacts that greatly exceed the sum of each part. Boards and organizations are facing a “polycrisis”<sup>1</sup>—a cluster of related familiar and “unfamiliar” disruptive risks, trajectories, and compounding impacts, and unpredictable consequences that organizations must navigate. In addition to managing the effects of mid-term and long-term trends, organizations must respond to real-time shocks and events. For example, within the past 18 months, organizations have had to respond to the effects of the war in Ukraine, a liquidity crisis and rising costs, and the rapid developments in AI.
- ▶ Risk velocity—driven by the interaction of external risks and a growing number and scope of operational risks, including digitization, social media, reliance on third parties, and disruptions in global supply chains—is increasing.
- ▶ Stakeholder expectations and requirements for enhanced board oversight, engagement, and disclosure of a wider range of traditional and “non-traditional” risk areas are increasing. Regulators, investors, employees, activists, and others are all placing higher risk management performance and transparency expectations on management and boards.

To meet the challenges and opportunities presented by these trends, boards must strengthen their governance and risk oversight approaches as noted in NACD's *The Future of the American Board* report. This *Risk Committee Blueprint* extends on principal six outlined in the report, which recommends: “Governance structures and practices should support the board as adaptive and agile, focused on strategy and risk, and prepared to take appropriate action in a crisis.” The guidance in this Blueprint enables boards to enhance their risk governance—either through a dedicated board risk committee or other board committees.

---

<sup>1</sup> The World Economic Forum, *The Global Risks Report 2023* (Geneva, Switzerland; WEF, 2023), p. 4.

# Board Risk Oversight Roles and Responsibilities

Risk can be defined as “the possibility that events will occur and affect the achievement of strategy and business objectives.”<sup>2</sup> From this definition, risk oversight includes considering the risks, or variance in outcomes, that could impact the organization’s strategy and operations; assessing the efficacy of the risk management framework implemented and maintained by the CEO and management team; and consideration of the alignment of the organization’s strategies, risk appetite, and risk capacity.

Board risk oversight responsibilities are based on fiduciary duties arising from common law as codified under state law and interpreted by courts and are also shaped by federal and state laws and regulations.<sup>3</sup> Key responsibilities have continued to expand over the past decade in recognition of evolving governance practices, complex business environments, and rising disclosure requirements—for example, evolving oversight and disclosure requirements around cyber risks.



## SOURCES AND DRIVERS OF THE BOARD’S RISK OVERSIGHT ROLE AND RESPONSIBILITIES

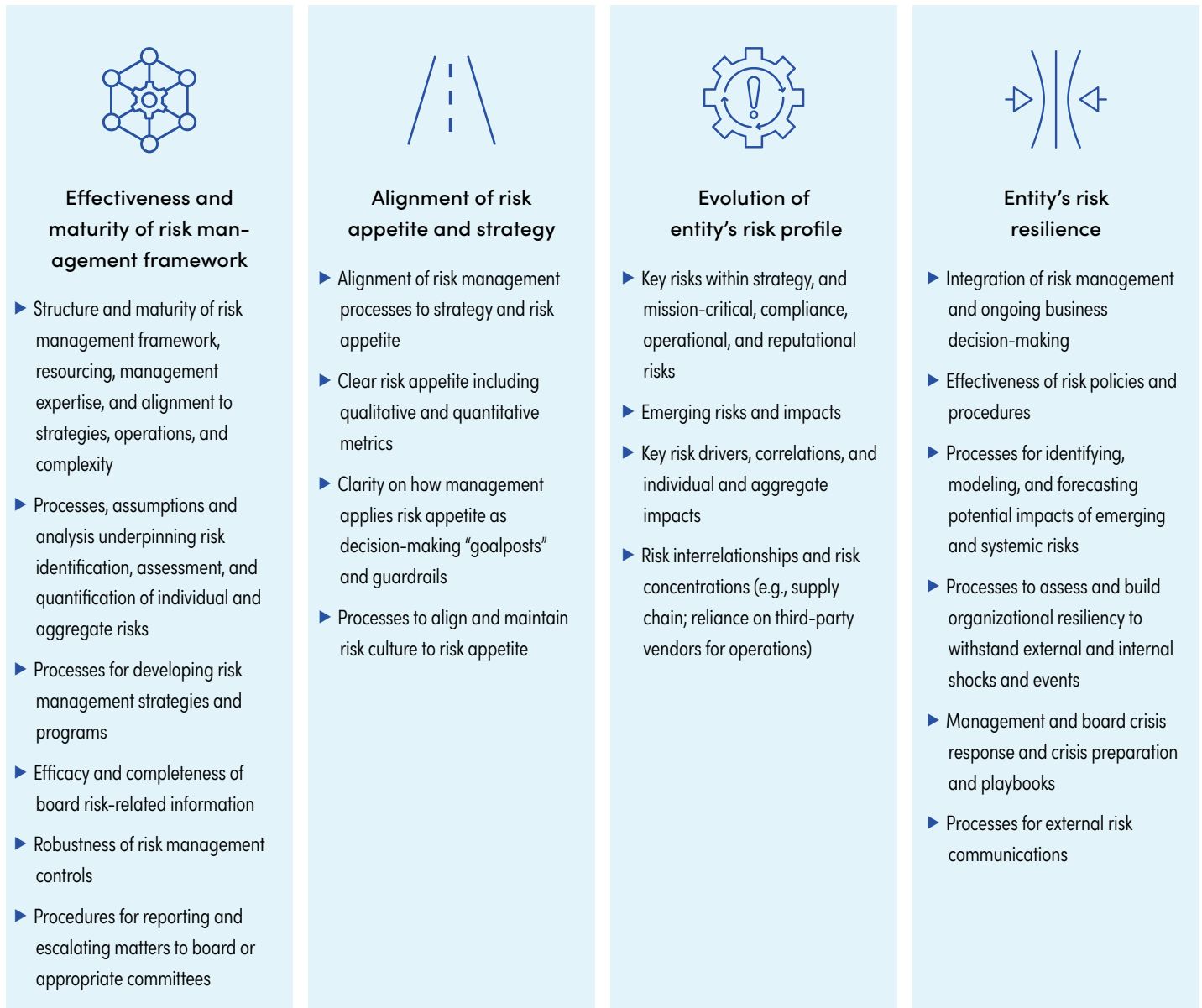
- ▶ **Fiduciary Duties:** The Delaware courts’ rulings have formulated many of the national legal standards for directors’ duties for risk management with the *Caremark* line of cases.
- ▶ **The Dodd-Frank Wall Street Reform and Consumer Protection Act:** The Dodd-Frank Act created federally mandated risk management procedures for financial institutions, requiring bank holding companies, and certain other non-bank financial companies, to have a separate risk committee which includes at least one risk-management expert.
- ▶ **The Securities and Exchange Commission (SEC) and other regulators:** Recent and proposed disclosure requirements are expanding the breadth, depth, and focus of board risk oversight.
- ▶ **NYSE Listing Guidelines:** The guidelines require a listed company to have a written audit committee charter that includes oversight of risk exposure policies and the processes to govern risk management.
- ▶ **Third-Party Guidance on Best Practices:** This includes reports by NACD and the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

<sup>2</sup> *Enterprise Risk Management: Integrating with Strategy and Performance* (COSO, 2017), p. 9.

<sup>3</sup> See also, “[Risk Management and the Board of Directors](#),” posted by Martin Lipton, Sebastian V. Niles, and Marshall L. Miller, Wachtell Lipton Rosen & Katz, on Tuesday, March 20, 2018, *Harvard Law School Forum on Corporate Governance*.

The board’s core risk oversight responsibilities have been outlined in previous NACD risk governance reports, and the key elements remain.<sup>4</sup> The responsibilities can be grouped into four key areas as outlined below. (See Illustration 2.)

## ILLUSTRATION 2: BOARD RISK OVERSIGHT RESPONSIBILITIES



Source: Marsh McLennan

<sup>4</sup> *Risk Governance: Balancing Risk and Reward* (Washington, DC: NACD, 2009) and *Strengthening Risk Oversight* (Washington, DC: NACD, 2016).



The challenge now facing boards is the execution of responsibilities to meet rising governance demands. To meet this challenge, the board should focus on the following four governance areas to ensure directors are enabled to provide oversight:



- ▶ The board's risk oversight structure, including consideration of a risk committee, and clear assignment and alignment of risk oversight responsibilities to avoid overlaps or "gaps"



- ▶ Risk oversight expertise and the composition of the board and committees to ensure expertise matches the organization's evolving risk profile and risk management framework



- ▶ Management's risk reporting and communications with the board and other sources of information to enable effective independent oversight



- ▶ Annual calendar for risk oversight and committee agenda to ensure the board can prioritize focus

# Board’s Risk Oversight Structure

The expanding board risk agenda requires boards to consider how to allocate risk oversight for more risk issues across the committees and the full board and focus on the coordination of risk oversight.

The “right” board risk oversight structure will depend on factors specific to each organization. (The exception are financial services organizations where board risk committees are governed under the Dodd-Frank Act). Regardless of how risk oversight responsibilities are allocated across the board, it is vital that directors and management teams reporting to the board have a clear and robust understanding of the responsibilities, and how they will be executed and coordinated. As one director stressed, *“Clear governance around risk oversight and oversight of risk management is in many ways more important than any particular board structure.”*<sup>5</sup>

In practice, risk oversight responsibilities are generally distributed across committees, and boards leverage a combination of approaches. Five approaches are presented below. (See [Illustration 3](#).) Further, as noted below, even if a board risk committee is established and tasked with oversight of key risks impacting the organization’s performance, aspects of risk oversight responsibilities will likely be distributed across committees. For example, the compensation committee will provide oversight of executive compensation and any risks within that process, and the audit committee will provide oversight of the internal controls around the risk management framework.

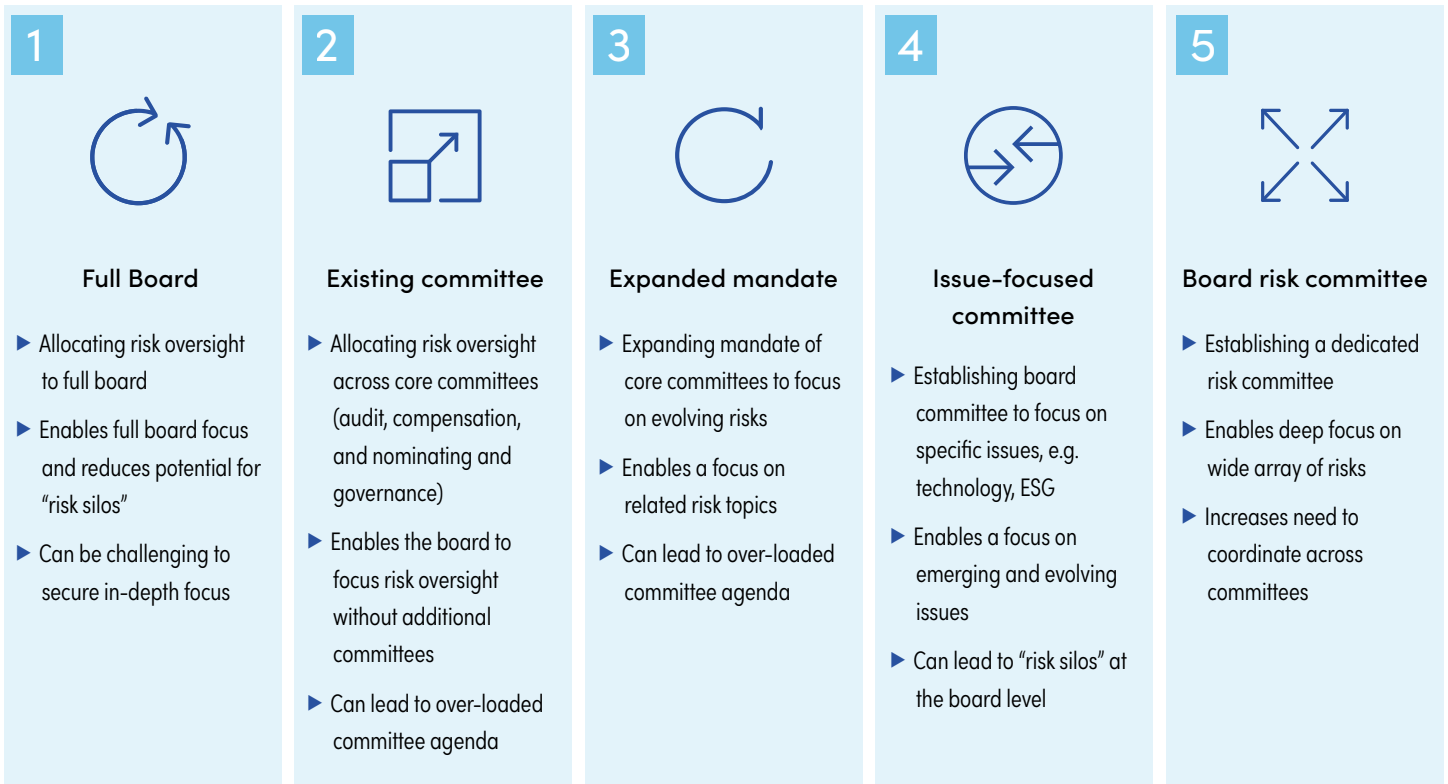
Clear committee charters that define risk oversight responsibilities, roles, and the management structure and processes to support those responsibilities are vital to align different areas of risk oversight—for example, clarity on the links to the audit committee to align disclosure and risk oversight practices. Robust charters, supplemented by effective communications between the committees and full board, will minimize overlapping or “under-lapping” responsibilities. This is particularly important as the mandates of long-standing board committees (e.g., the compensation committee) are evolving.

Committee chairs also play a critical role in ensuring effective alignment and coordination of the board’s risk oversight. The chairs will shape and structure committee calendars and agendas and drive coordination and information flows between committees and the full board. (See more in the section, [“Annual Calendar for Risk Oversight and Committee Agenda.”](#)) This will ensure risk insights on cross-cutting issues are integrated as part of overall oversight.

---

<sup>5</sup> Participants’ quotes (italicized) have been anonymized.

## ILLUSTRATION 3: BOARD RISK OVERSIGHT STRUCTURES



Source: Marsh McLennan

Efficient allocation of risk oversight responsibilities to committees allows boards to schedule more time for higher-level, exploratory risk discussions. Directors should consider three key factors in assessing their risk oversight approach and whether to establish a board risk committee.

- ▶ **Organization’s current and evolving risk profile:** Consider how the existing risk oversight allocation and board committee structure and composition align to the entity’s current and evolving risk profile. External developments, such as emerging oversight expectations or requirements on areas such as ESG factors may prompt changes in the allocation of the board’s responsibilities. A rapidly evolving industry, or an uptick in the velocity of changes affecting a sector, can also shift the entity’s risk profile.

Internal factors should also be considered—for example, a large merger, acquisition, or divestiture that creates significant disruptions in strategy and the organizational culture. Significant changes in key operational backbones such as a transformative technology implementation will also impact the overall risk profile.

Finally, the maturity of the overall organization is a factor. A start-up or rapidly expanding organization may benefit from a dedicated board risk committee. As one director noted, *“If you are a new company, or going through a major organizational transformation, then you really need a risk committee.”*

- ▶ **Board capacity:** Consider the board’s capacity and if there are sufficient board resources—time, members, and expertise—to support a new committee. Boards must balance increasing governance requirements and a proliferation of committees to address emerging issues. Boards should also consider the issue of risks being “siloeed” at the board level if there are too many board committees addressing aspects of risk oversight.
- ▶ **Management’s risk management capacity:** Consider if management’s risk structure can support a board risk committee. This can be a function of the maturity and robustness of management’s risk configuration. For example, a chief risk officer (CRO) and/or a robust executive risk committee can play a critical role in ensuring appropriate matters are escalated to the board and can help shape the board risk committee agenda. In contrast, the lack of a robust risk structure at the management level may signal the need for a board risk committee. Research suggests that only about 30 percent of organizations have a mature enterprise risk management (ERM) program.<sup>6</sup>

---

<sup>6</sup> *The State of Risk Oversight: An Overview of Enterprise Risk Management Practices*, AICPA and NC State, 13th edition, 2022, p. 17.



# The Value of a Board Committee

Establishing a board risk committee can be a very effective structure to enable boards to meet their expanding risk oversight responsibilities. This is particularly the case when the agenda of the audit committee—which is often tasked with risk oversight—or other committees is becoming crowded or too cumbersome.

Data show that the risk committee is the third most prevalent “nonstandard” board committee, but this data is skewed upward due to the regulatory requirements for financial services.<sup>7</sup> A recent NACD survey suggested that 7 percent of respondents were considering adding a standing risk committee to the board.<sup>8</sup> It is interesting to note that dedicated board risk committees are uncommon outside of the financial sector. (See Illustration 4.) However, a review of the Russell 3000 shows that a number of organizations have committees with mandates such as “Finance and Risk” and “Security and Risk.”

## ILLUSTRATION 4: PREVALENCE OF BOARD RISK COMMITTEES

BOARD RISK COMMITTEES BY INDUSTRY RUSSELL 3000	2022	BOARD RISK COMMITTEES BY MARKET CAPITALIZATION RUSSELL 3000	2022
Energy & Mining	2.8%	<\$100M	4.4%
Entertainment, Media & Communications	2.4%	\$100M–500M	3.3%
Financial Services & Insurance	28.2%	\$500M–1,000M	6.6%
Health Industries	0.0%	\$1,000M–10,000M	11.0%
Industrial Products	2.0%	>\$10,000M	8.4%
Pharmaceutical & Life Sciences	1.7%		
Retail & Consumer	1.8%		
Technology	3.7%		

n=2,912

Data Sourced from  


A risk committee enables a substantive focus on risk and risk analysis, including emerging and non-defined risks, optimizing risk management, and links to strategy. The risk committee can also serve as an aggregator of risks overseen by the different board committees and can ensure all risks receive thorough oversight. This enables the audit committee to provide oversight to the processes and internal control framework for risk management and disclosure.

A review of risk committee charters in nonfinancial organizations reveals a common focus on oversight of the entity’s risk management, but the alignment of risks and oversight responsibilities to the risk committee varies—often reflecting the organization’s industry. The responsibilities overseen by the risk committee can include the effectiveness and maturity of the overall ERM process and specific risk areas such as ESG, cybersecurity, supply chain, geopolitical risks, commodity risks, security risks, or regulatory risks. One commonality across the charters was a requirement that members must be independent, but only one charter specified the necessary expertise of the members (noting at least one member to have a finance or accounting background).

<sup>7</sup> NACD, *2022 Inside the Public Company Boardroom* (Arlington, VA: NACD, 2023), p. 22.

<sup>8</sup> NACD, *2022 NACD Public Company Board Practices and Oversight Survey* (Arlington, VA: NACD, 2022), p. 43.

A benefit of allocating risk oversight responsibilities outside of the audit committee is the opportunity to apply differing perspectives and expertise. Outside of the financial services sector, there are currently no specific expertise requirements for board risk committee members. In an era of risk convergence, the insights of diverse directors with an array of expertise and experience (including legal, technology, marketing, human capital, etc.) can provide powerful, cross-cutting, unique perspectives. (See more under the section, “[Risk Oversight Expertise](#).”)

Creating a board risk committee also signals and clarifies the importance of risk oversight and risk management to the organization’s internal and external stakeholders. External stakeholders, including regulators, investors, community leaders, analysts, and activists, are increasingly pushing for greater transparency on risk oversight. For internal stakeholders, establishing a board risk committee can stimulate the organization to develop its risk management and ERM maturity and provide clear sponsorship for the function and robust risk management. The risk committee also helps set the “tone at the top” necessary for a healthy “speak-up” risk culture.<sup>9</sup>

## CASE STUDY: RISK COMMITTEE STRENGTHENS RISK OVERSIGHT

In one organization, a push by the CEO to revitalize the CRO role and the ERM team prompted the establishment of a board risk committee. Along with this revised board structure, there has been a mutual evolution of the ERM team and Risk Committee in terms of a focus on proactive risk management. As one director noted: “*There has been a shift in the risk conversation in the boardroom from formulaic risk register reviews to a substantive conversation on how risks manifest.*” In addition, assigning the heads of business and corporate functions to the management team’s risk committee has driven better linkages between strategy and risk and embedded a stronger risk culture.

While risk committees can provide significant value, the structure can face two challenges. In some instances, the risk committee portfolio can become full and unmanageable, as it may be chartered to provide oversight to too many risk areas. In such cases, it can be hard to discern the most important risks to focus on. In others, the committee tends to focus on silos of specific risk, such as financial risk, and may not be able to integrate risk issues across critical strategic decisions.<sup>10</sup>

As noted in the [Nominating and Governance Committee Blueprint](#), the decision to create a new committee ultimately rests with the full board, but the nominating and governance committee can shape the discussion. For example, the nominating and governance committee can take the lead in determining the new committee’s purpose, scope, composition, guidelines, and procedures, including defining the committee’s responsibilities and reporting structure.<sup>11</sup>

<sup>9</sup> [Identifying and Responding to a Dysfunctional Culture: Key Actions for Boards](#), Women Corporate Directors and Marsh McLennan, 2019, p. 10 and p. 23.

<sup>10</sup> “[Effective Risk Oversight Demands Board Structure Evolution](#),” Mark Pellerin and Til Schuermann, *NACD BoardTalk™*, September 2, 2021.

<sup>11</sup> NACD, [The Future of the American Board: Nominating & Governance Committee Blueprint](#) (Arlington, VA: NACD, 2023), p. 15.



## KEY QUESTIONS FOR DIRECTORS TO ASSESS THE ALLOCATION OF RISK OVERSIGHT RESPONSIBILITIES

1. How does the current board risk oversight structure enable a focus on key risks and risk management, including strategic, mission-critical, and operational risks and other risk categories as identified through the risk management framework?
2. Does the current board oversight structure support a focus on emerging risks, potential scenarios, and the organization's overall risk resilience?
3. In what ways does the current risk oversight structure need to be adjusted to meet internal and external stakeholder expectations?
4. Does the current board committee allocation enable a diversity of views in risk discussions?
5. How does the board's risk oversight structure support the organization's desired risk culture?
6. How does the board's risk oversight structure align to management's risk structure?
7. Has the board recently assessed if there are any redundancies between committee responsibilities or management reporting in the current risk oversight structure?
8. Do committee charters specify the process and frequency of assessing any necessary updates to ensure alignment of the board's risk oversight responsibilities and the entity's risk profile?

# Risk Oversight Expertise

The breadth and depth of risk oversight continues to expand, requiring new or evolving director expertise. For example, the list of board oversight responsibilities now includes emissions reduction; diversity, equity, and inclusion; cybersecurity; digital transformation; supply chain continuity; and issues around AI and the metaverse. In addition, boards also need experience with risk management and implementing risk management programs.

Boards should assess the necessary and desired director expertise and board composition against the risk landscape, the entity's risk profile, and the organization's risk oversight matrix to identify any gaps. The nominating and governance committee can help the board consider how to close any risk oversight gaps, including whether to evolve the board's composition, increase board education, or add a board advisor.

As noted earlier, there are currently no defined listing or best practices requirements for the composition of a board risk committee in nonfinancial services. Further, given the range of risk oversight responsibilities documented in risk committee charters, "best practices" in risk oversight expertise have not yet been established.

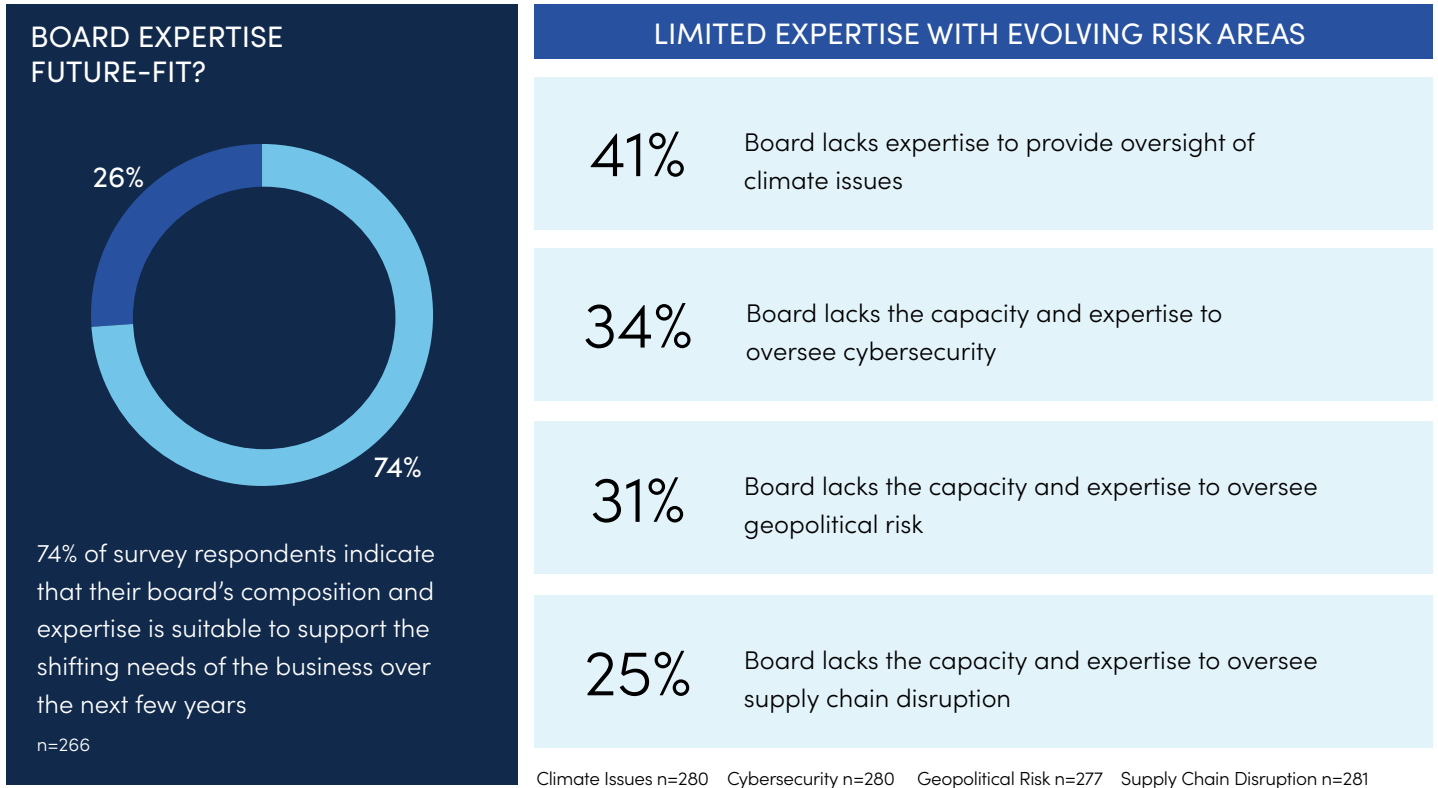
Based on research and interviews, boards should consider the following:

- ▶ Risk committee members should reflect a wide diversity of experience and capabilities. (See [Illustrations 5](#) and [6](#).) Directors have noted that diversity of expertise is vital for effective oversight of a complex, interconnected risk environment. One director observed that, *"Board recruitment practices haven't yet caught up with the complex and changing risk landscape. Over the next few years, boards will really want to have some members with deep expertise in areas such as technology, security, or operations who understand how to prevent, mitigate, and report out on vulnerabilities."*
- ▶ Boards should consider if they have the expertise to probe management on the maturity of its risk management framework and complex processes around management's risk identification, assessment, quantification, and modeling. Experience with management's governance structures around risk quantification, model development, and data management are areas of increasingly important expertise as organizations build risk quantification capabilities and leverage new technologies including AI. Individuals who have served as CROs may increasingly be a target of board recruiting.
- ▶ Given the expansion of risk issues and the typical size of most boards (10–12 individuals), no board can have an expert on each risk topic. Boards should thoughtfully consider the right mix of approaches to build and maintain knowledge and expertise on evolving issues, including adding board advisors or a regular session with outside experts.



NACD survey research shows that most respondents believe that their board’s composition and expertise is aligned to evolving challenges. However, when specific drivers of emerging risks are considered, many boards are less confident. (See Illustration 5.)

## ILLUSTRATION 5: BOARD EXPERTISE WITH EMERGING RISK AREAS



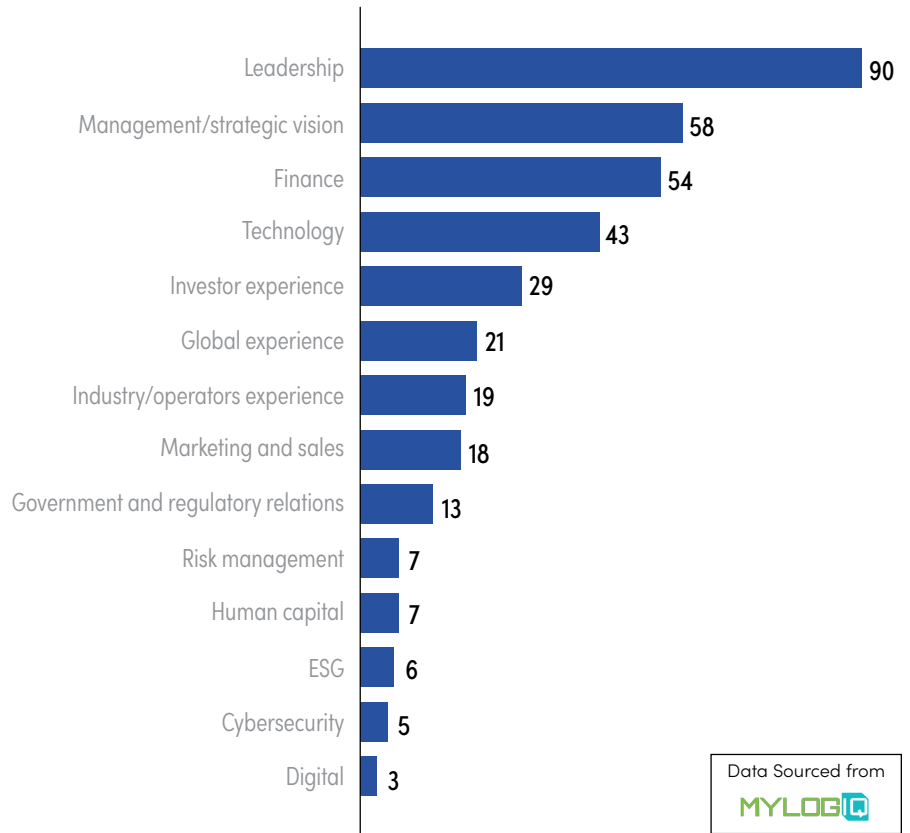
Source: NACD, *2023 Governance Outlook: Projections on Emerging Board Matters* (Arlington, VA: NACD, 2022), p. 6, Figure 5 and Figure 6, and unpublished data from the *2023 Board Trends and Priorities Survey*.

Data also suggest a gap between the prevalence of director skills and experience and the top issues that could impact organizations over the next three to five years, such as digitalization. (See Illustration 6.)

Ultimately, regardless of director background or expertise, as one director noted, *“Intellectual curiosity is the most important expertise for effective risk oversight.”* Boards must commit to a culture of continuous learning and inclusivity of diverse experiences, expertise, and insights on evolving topics to support an active and effective risk oversight. In short, since boards cannot be know-it-alls, boards must become learn-it-alls.<sup>12</sup>

As noted above, the nominating and governance committee plays an important role in aligning board composition with the organization’s risk profile, enabling continuing education for the board and individual directors, and driving processes for board and committee evaluations to ensure board risk expertise is aligned to the organization’s risk profile.

ILLUSTRATION 6: INCOMING DIRECTOR SKILLS  
(Percentage of directors)



n=1,375

Source: 2022 *Inside the Public Company Boardroom*, p. 7.

Data Sourced from  
**MYLOG**



## KEY QUESTIONS FOR DIRECTORS TO ASSESS RISK OVERSIGHT EXPERTISE

- ▶ Has the board recently mapped its expanding risk oversight responsibilities against a matrix of current expertise to assess if the board has necessary experience to provide oversight to critical and emerging risks?
- ▶ How is risk expertise and risk management experience factored into board refreshment plans?
- ▶ How are the needs for expanding risk expertise and experience integrated into directors’ continuing education programs?

<sup>12</sup> Also see “Increasing Board Agility Is Critical to Risk Oversight,” Margarita Economides and David Gillespie, in *Evolutions in Risk Oversight: Lessons Learned for the Decade Ahead* (NACD and Marsh McLennan, 2021), p. 16.

# Management’s Risk Reporting and Communications with the Board

Effective reporting and information flows to the board lie at the core of enabling directors to execute risk oversight responsibilities and provide independent judgment and oversight. The board must have a fundamental clarity about its risk responsibilities and the organization’s risk appetite as these, in turn, guide the necessary content, structure, and cadence of information flow to the board. (See [Illustration 7](#).)



## IMPORTANCE AND VALUE OF DEFINING RISK APPETITE


*The Future of the American Board* report notes that “The board and management [should] have an agreed and clearly defined risk appetite which provides guardrails for risk activity.”<sup>13</sup> An organization’s risk appetite is an articulation of the risks the organization wants to take (e.g., geographic expansion or new product launches) and how much risk it can take (e.g., risk-taking capacity as defined in terms of the organization’s performance such as capital requirements, earnings volatility, or liquidity).

A clear risk appetite is an essential risk oversight and governance tool. It is the yardstick that helps the board and management to identify risks (events with impacts that exceed the risk appetite) and better understand the relative impacts of risks and what constitutes a “big risk” for the organization. It drives the “translation” of risk analyses (e.g., critical and high cyber vulnerabilities or high staff turnover) into information and metrics expressed in quantitative measures on the organization’s performance. It is key to risk-enabled, strategic decision-making. It guides decisions around investment and resources for risk mitigation to align to risk appetite. Finally, risk appetite structures add rigor to risk discussions and management’s risk reporting, including risk thresholds and risk forecasts.

---

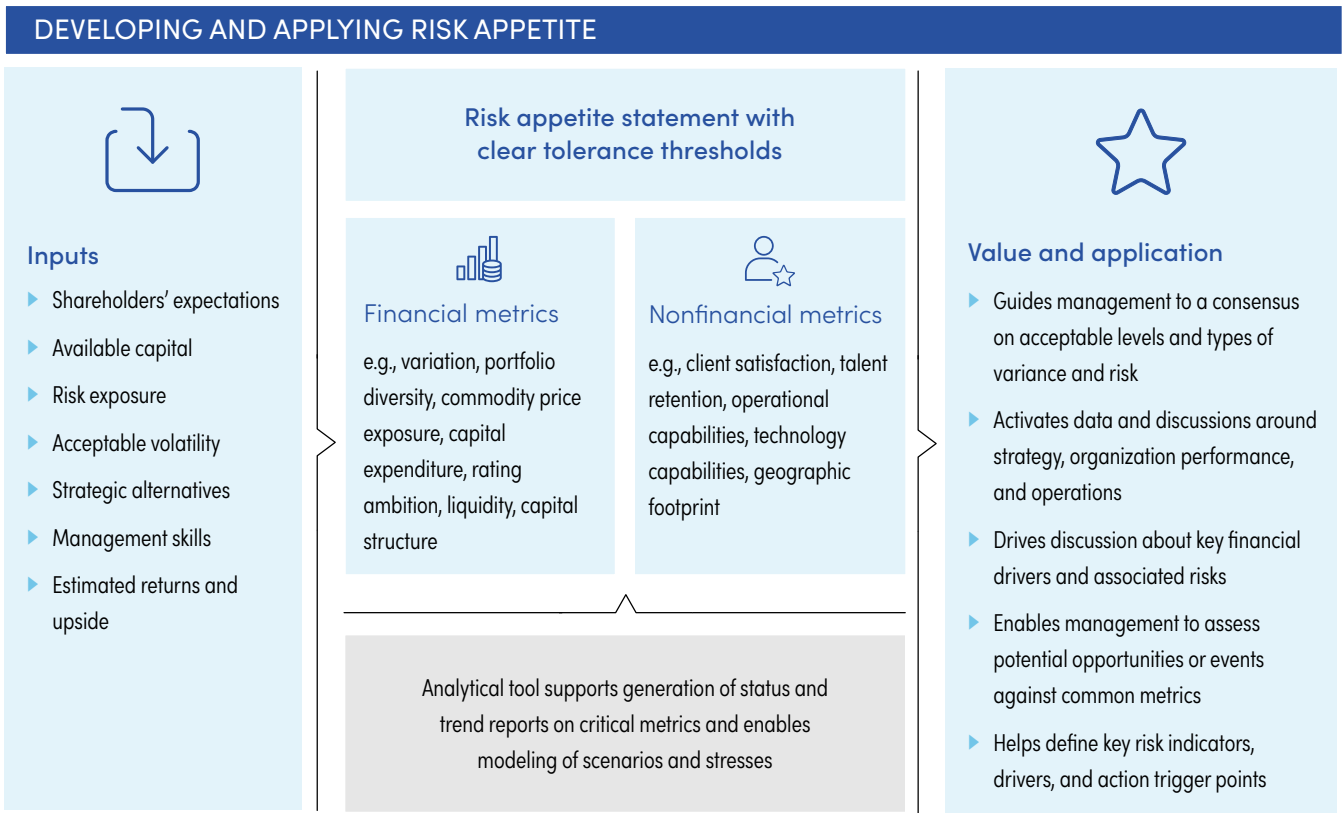
<sup>13</sup> NACD, *The Future of the American Board* (Arlington, VA: NACD, 2022), p. 36.

## ILLUSTRATION 7: COMPONENTS OF RISK APPETITE



### RISK APPETITE STATEMENTS NEED THREE CHARACTERISTICS TO BE EFFECTIVE

- ▶ A quantitative and qualitative foundation based on a comprehensive, strategic view of the key drivers of value creation and destruction for the organization
- ▶ Relevance to a broad swath of stakeholders at different levels in the organization
- ▶ A connection to key decision-making processes across the organization to increase the value derived from risk management



Source: Marsh McLennan

As noted in NACD's *Future of the American Board* report, "Information and reporting systems are key to the board's ability to provide oversight of management performance generally, including compliance and risk management and mission-critical risks more specifically."<sup>14</sup> The risk information that must be reviewed by the board is an evolving area, and guidance is expected to be forthcoming (for example, evolving requirements on cyber risk and disclosure).

<sup>14</sup> NACD, *The Future of the American Board* (Arlington, VA: NACD, 2022), p. 37.



In a recent NACD survey, director respondents rated “Information flow issues between management and the board” as the second-highest barrier to a board’s high performance, and over 60 percent have communicated with management about the types of risk information the board requires.<sup>15</sup> Directors’ challenges with management’s risk reporting can be summarized as insufficient information or insights on the impacts of dynamic risks on the entity’s strategy and performance. Looking closer, directors’ frustrations include these:

- ▶ **Reworked management data that is not effective for directors’ oversight role. For example, voluminous material with excess focus on details.** Typical risk dashboards are static, backward looking, too high-level, or too granular with information expressed in technical terminology that is difficult to access, understand, and interrogate by a nonexecutive audience.
- ▶ **Excess focus on individual risks or risk categories with snapshots of exposures and the estimated impacts of mitigation plans that too often stop short of outlining the potential impacts on key processes, organizational performance, or strategy.** For example, cyber risk reports that flag the number of incidents but do not outline the cost of cyber events on vital business processes.
- ▶ **Under-developed or limited insights as commonly used risk tools, such as a risk register or a “heat map.”** These tools do not highlight risk and risk driver concentrations, correlation, and interdependencies across risks.
- ▶ **A focus on “known” and quantifiable risks.** Put differently, boards may receive excess data on known risks with known impacts, and too little information and analysis of potentially high impact and uncertain risks.
- ▶ **Short focus:** Insufficient consideration of differing timeframes, and direct and indirect implications (second- and third-order implications) of risks.
- ▶ **Limited focus on resilience.** Reports that do not allow the board to consider the entity’s responsive capabilities, maturity, and progress toward greater resilience in the face of complex multipart crises that demand a variety of levers to be deployed in combination.<sup>16</sup>
- ▶ **Information that is “circular” and limited to internally generated information with insufficient external benchmarking or inputs.** For example, the board focuses on the risk issues identified by management as critical. Often, risk management improvements are based on improvements over time but are not based on industry or other best practices.

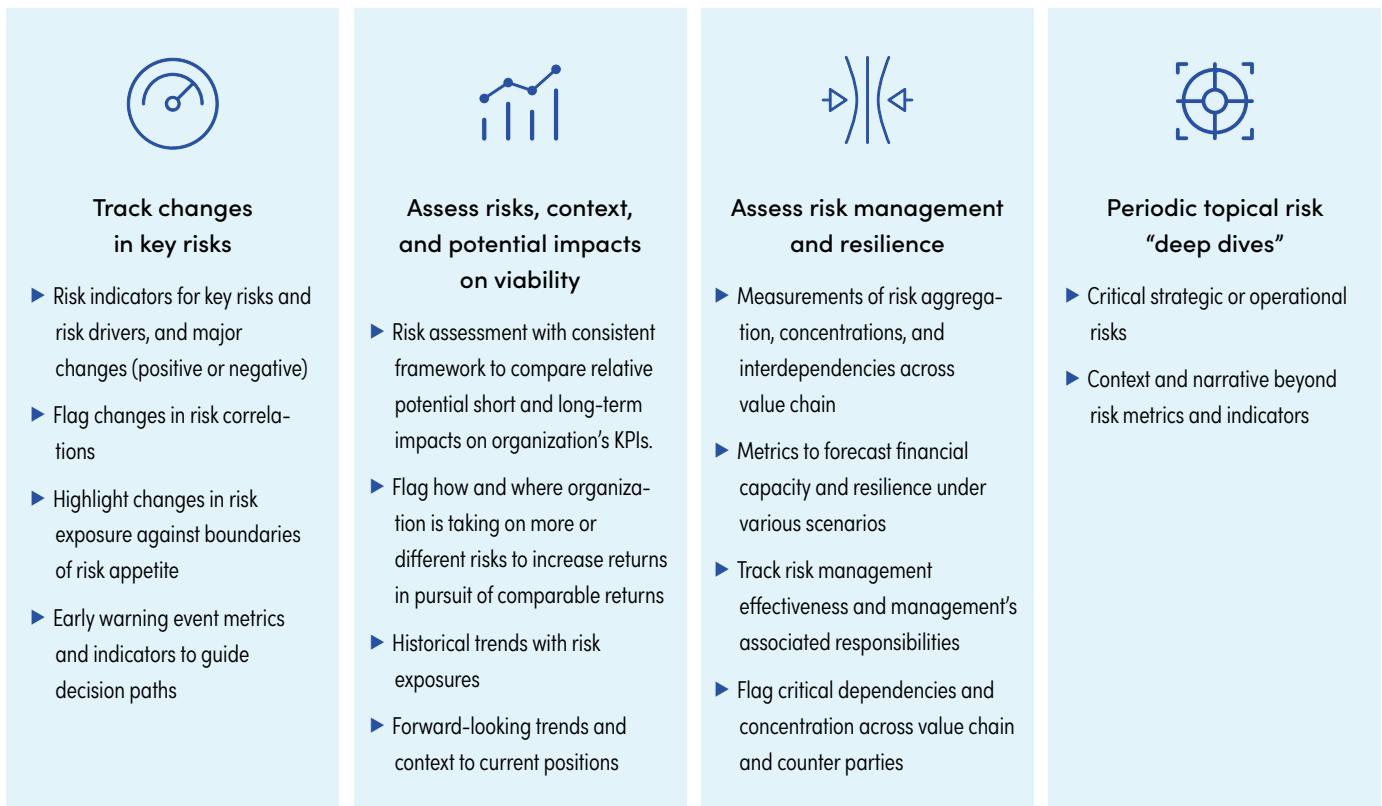
The content, format, and process supporting board risk reporting will be unique to each organization and aligned to the risk profile. However, reporting should move beyond siloed, single-risk information to identify risk drivers and impacts across risk categories and should include metrics that support board-level decisions around the dynamics of systemic and emerging risks across the complete value chain. Effective risk reporting should enable the board to capture changes in key risks and trends. It should offer forward-looking perspectives into the entity’s evolving risk profile and provide indicators that will help the board to determine whether the organization is within its risk appetite. (See [Illustration 8](#).)

---

<sup>15</sup> NACD, *2022 NACD Public Company Board Practices and Oversight Survey* (Arlington, VA: NACD, 2022), p. 15 and p. 43.

<sup>16</sup> Richard Smith-Bingham, “Building Enterprise-wide Resilience in an Age of Permacrisis,” posted on *NACD BoardTalk*™, January 31, 2023.

## ILLUSTRATION 8: CRITICAL ELEMENTS AND FEATURES OF EFFECTIVE BOARD RISK REPORTING



### KEY FEATURES OF EFFECTIVE RISK REPORTING

- ▶ Update at a frequency consistent with pace of risk evolution and severity of risk
- ▶ Information at a level of detail consistent with the director's risk oversight responsibilities
- ▶ Avoid unnecessary jargon and complexity and tailored to a non-executive audience
- ▶ Appropriate qualitative or quantitative metrics for risk type with impacts measured in terms of organizational performance
- ▶ Consistency in format and delivery
- ▶ Supported by processes assuring the accuracy, timeliness, completeness, and relevance of management's risk information

Source: Marsh McLennan

Effective and concise risk reporting enables robust risk dialogue with management. As one director noted, *"Great reporting is no substitute for a good working relationship within the risk committee and effective dialogue with management."* All updates on risks and risk management should not be funneled solely through the CEO; the management team's risk structure should have direct access to the board's risk oversight. For example, ensuring that the chief information officer, if tasked with enabling cybersecurity, has regular and direct reporting access to the board committee chartered with cyber-risk oversight.

Risk dialogue helps management “see around corners” and uncovers risks within the entity’s value chain by asking challenging questions to probe what-if scenarios and to query assumptions, interpretations, and options. This is particularly true for emerging, complex, and transformative risks that are seldom effectively captured on a risk dashboard, an annual risk register, or commonly used operational risk taxonomies. One director of an organization with a mature risk management approach noted, “We now are focusing more on what could be a disruptive risk and asking: are we war-gaming those, are we capturing the learnings from events, and how can we use those learnings to improve future resilience? In that way, the risk committee really provides value to the organization.”

Improving board risk reporting may require the management team to strengthen and improve risk identification, assessment, and mitigation. For example, research by Marsh shows that relatively few organizations conduct scenario-based modeling to evaluate the potential financial impacts of risks.<sup>17</sup> This is especially the case for evolving and emerging risks. Scenario modeling and table-top exercises lead to a new appreciation of risks embedded within the organization’s value chain, the organization’s resiliency, and its capacity to respond. These forms of analysis also help create the “muscle memory” to respond in a crisis.

## CASE STUDY: IMPROVING BOARD RISK REPORTING

In one organization, the risk committee was quite prescriptive in defining its information needs and necessary changes to risk reporting. The process of improving risk reporting took several iterations with the management team and within the board to achieve informative and consistent formats. As one director determined, “It is our responsibility as the board to manage the information flow coming to us and to make it clear what we need and don’t need.” The committee’s goal was to move beyond siloed volumes of risk information based on risk categories to information supporting board-level decisions around the dynamics of top risks and systemic and emerging risks across the complete value chain.

The process helped create consistency in the reporting materials, including the underlying process, cadence, format, content, and key performance indicators (KPIs) required for oversight, that allowed the board and management to better identify important developments in the organization’s risk profile. “Consistency in the reporting package is really helpful in reviewing the quantities of information and enables improved risk dialogue with management,” observed the director.

As part of the shift to a greater use of scenarios, war-gaming, and other assessment tools, boards must actively foster courage and confidence within senior leadership teams and risk functions. This will enable teams to adopt new forms of risk analysis, bring forward issues despite incomplete or imperfect data and analysis, and facilitate exploratory dialogue on issues for which there may not yet be a consensus or perfect data for risk estimates.<sup>18</sup> As one director noted when speaking about risk forecasting, “It takes a thoughtful approach and a lot of CFOs are uncomfortable putting a dollar

<sup>17</sup> *Risk Resilience Report*, Marsh, 2021, p. 8.

<sup>18</sup> “Improve Your Board’s Risk Visibility with One Critical Factor: Courage,” Michelle Daisley and Lucy Nottingham, in *Evolutions in Risk Oversight: Lessons Learned for the Decade Ahead*, NACD and Marsh McLennan, 2021, p. 12.

*value on such scenarios, but the risk committee needs to push a dialogue on how an event or shock could impact the company and the relative potential impacts of different scenarios.”*

The board also needs external risk insights—especially on evolving and emerging issues that are unfamiliar to the management team or board and could impact the organization’s risk profile. The cadence and process for accessing external insights should be defined in the committee’s annual calendar to prevent overreliance on management’s view of risks.



## KEY QUESTIONS FOR DIRECTORS TO ASSESS RISK REPORTING

- ▶ Do risk reports highlight key internal and external drivers of change and illustrate changes in risk parameters?
- ▶ Do reports identify how risks are impacting the organization’s aggregated risk profile, how impacts are correlated, and scenarios where the overall business is more or less exposed?
- ▶ Are risks measures and metrics evolving from qualitative to quantitative terms to better highlight relative impacts in terms of the organization’s priorities and key performance indicators?
- ▶ Do reports outline the first, and potentially second and third, risks’ impact on key strategic objectives (e.g., potential variability in earnings and by how much)?
- ▶ How is the organization stress testing, measuring, and modeling the impacts of critical risks and forecasting the impact on the organization? What reports does the board receive on these processes?
- ▶ What measures and metrics are used to monitor risk profile and projections against risk appetite parameters?
- ▶ Do the reports include issue/action tracking, and align specific actions with strategic KPIs?
- ▶ Where and how are dependencies and risks related to critical suppliers and third parties reported?
- ▶ Do reports outline how risk impacts are being mitigated (e.g., diversification, new investments, MA&D, supply chain reorientation) and the overall effectiveness of risk management efforts?
- ▶ What is the data management and model governance structure for the analysis supporting risk identification, assessment, and management?
- ▶ Do the risk reports provide insights into the entity’s capacity to absorb shocks and overall resilience?

# Annual Calendar for Risk Oversight and Committee Agenda

Careful consideration of the full board and committee annual calendar and agendas enables directors to prioritize their focus, meet governance responsibilities, and allow time for review of dynamic events and information from a range of sources. It is vital that the board risk committee agenda is not overly absorbed by focus on “check-the-box” or formulaic reviews at the expense of meaningful strategic discussions around risk / return trade-offs. As one director noted, *“A key skill is knowing how to structure the agenda to get the right information and not just what the management team may want the board to hear.”*

Agenda structure is particularly important with regard to risk oversight where topics are addressed across board committees and the information flow and activities of committees must be sequenced (e.g., risk and audit committees). In the face of crowded board agendas, directors stressed two points:

- ▶ Ensure the calendar blocks time for discussion on emerging and evolving risks and impacts. For example, what key macroeconomic issues does management see that could influence the long-term viability of the firm, not just specific strategies or quarterly performance. Along with this, it should be expected that the risk committee agenda may be somewhat dynamic, with adjustments throughout the year to allow time for a shifting risk landscape.
- ▶ The risk committee should ensure calendars and agendas allow independent insight from external experts, such as academics and industry specialists. They can provide insights into emerging trends and risks and the evolution of best risk management practices at other organizations, helping committees to upgrade their fact base, challenge the management team’s “conventional wisdom,” and guard against groupthink.<sup>19</sup> Boards may use “education sessions” before risk committee meetings, such as a dinner the night before, to create time for such sessions and reduce pressure on the committee agenda.

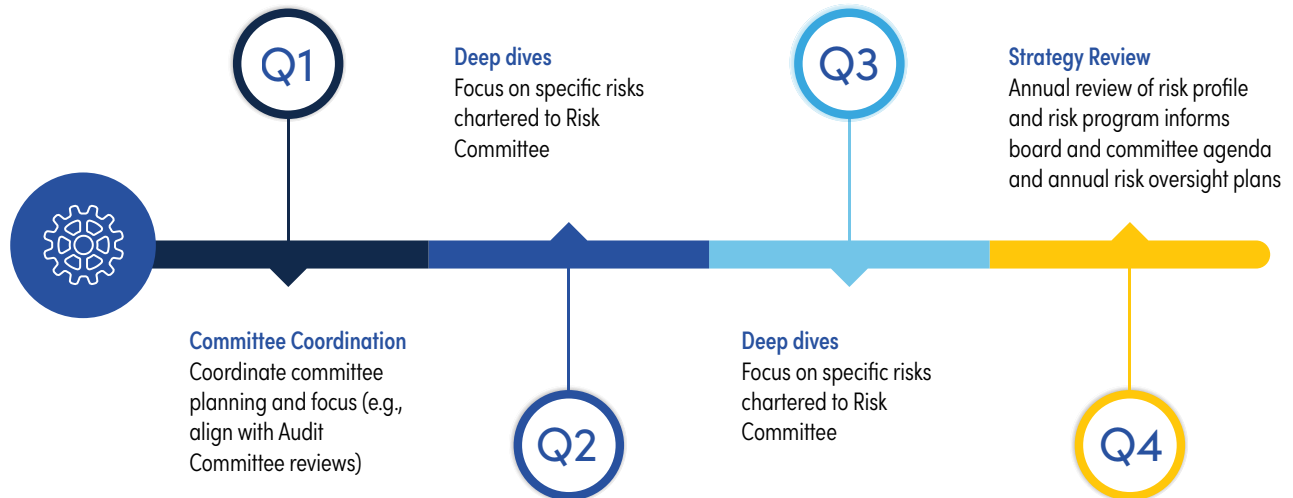
Committees must assess if their established annual rolling calendars encompass the evolving risk agenda and must remain in-synch with internal processes and external reporting requirements. Well-structured and efficient meetings will include regular agenda items (e.g., risk profile reporting); standing agenda items (e.g., risk appetite setting, reviewing outputs of stress testing); and rolling agenda items (e.g., business/support area or risk type drilldowns).

Clear calendars improve management’s engagement with the board and risk committee as requests for information and analysis can complement rather than add to ongoing work. The rolling calendar can be linked to board and committee charters and calibrated with internal processes and external reporting requirements. (See [Illustration 9](#).) In addition, the risk committee chair; CRO (or other executive leadership of risk management, such as the CFO); the corporate secretary; and CEO may meet two to four weeks before the meeting to review a proposed agenda (including a mixture of standard items, rolling topics, updates, and hot risk issues) to ensure prioritization of committee time.

---

<sup>19</sup> *The “Bored” Risk Committee? Less Ticking Boxes, More Meaningful Oversight*, Oliver Wyman, 2018.

## ILLUSTRATION 9: SAMPLE ANNUAL RISK OVERSIGHT CALENDAR



Source: Marsh McLennan

The committee chairs play a critical role in managing the increasingly complex board risk oversight agenda through their role in shaping committees and designing agendas. In terms of skill sets, chairs need to be capable of driving consensus on sensitive points, facilitating effective challenge and debate within committees, and running tight agendas with very focused sessions.

Chairs also support information flows to the full board and other committees, including the process for communicating and discussing urgent issues between committee meetings. This role should be defined in the committee charters with clarity on the cadence and content of communications. Informal liaison communications and discussions with other committee chairs in-between meetings also helps avoid “information silos” at the board level and manage and minimize overlapping committee agendas.

Beyond formal and information roles for the chair, boards are using other approaches to ensure risk information flow between committees. For example, some organizations have assigned the chair of each board committee to the risk committee to help identify issues that should be considered by another committee or the full board. Thoughtful consideration of director committee-membership overlap is another approach to use. Other organizations open risk committee meetings to all directors to educate and update directors on risk issues and oversight.



## **KEY QUESTIONS FOR DIRECTORS TO ASSESS THE ANNUAL CALENDAR AND THE RISK AGENDA**

- ▶ How does the board update and align the overall board and committee agenda to ensure clear and comprehensive risk oversight?
- ▶ Does the risk oversight calendar need to be adjusted to support emerging risk disclosure requirements?
- ▶ Are committees' calendars and agendas becoming overly cumbersome and too crowded to effectively cover risk oversight responsibilities? Does this signal a need to revise the agenda approach and the process supporting board meetings (e.g., information flow from management)?
- ▶ Do the committee agendas strike the right balance between necessary administrative elements (e.g., reviewing minutes), substantive review of risk issues, and time for dialogue and exchange between directors and with management?



# Conclusion

The risk landscape continues to evolve and become more complex. Boards play a vital role in helping their organizations navigate through complexity by enhancing and strengthening their risk oversight. This, in turn, will influence and shape the management team's approaches and risk management framework. Directors can use this blueprint guidance to assess whether the board and its committees have the members, mandate, information, and agenda that allow them to execute on their expanded risk oversight responsibilities.

## RISK COMMITTEE WORKING GROUP\*

Marsh McLennan and NACD are grateful to the Risk Committee Working Group participants for lending their time and expertise to help frame the issues for discussion and articulate key considerations and actions for board risk oversight.



**RICO BRANDENBURG**

Partner, Risk & Public Policy and Digital Practices, Oliver Wyman



**BARBARA DUGANIER, NACD.DC™**

Arcadis NV, McDermott International, MRC Global, Pattern Energy, Texas Pacific Land Corp., NACD Texas TriCities Chapter, John Carroll University



**DEBORAH DIAZ, NACD.DC™**

CEO, Catalyst ADV  
Archer Aviation, Primis Financial, Section IO



**MICHAEL EMBLER**

American Airlines, Ventas, NMI Holdings



**LINDA GOODEN**

GM, Home Depot, Bright Health Group, American Heart Association, University System of Maryland Board of Regents



**GEORGETTE KISER**

Aflac, NCR, Jacobs, Adtalem



**MARTIN PFINSGRAFF**

PNC Financial Services Group, PNC Bank



**MANOLO SANCHEZ**

FannieMae, Stewart Information Systems, BECU, Rice University



**REID SAWYER**

Managing Director and Head, Emerging Risk Practice, Marsh Advisory



**TIL SCHUERMAN**

Partner and the Cohead of the Americas Finance, Risk and Public Policy Practice, Oliver Wyman



**BOB SWAN**

Operating Partner, Andreessen Horowitz  
Ebay, GoTo, Nike, Flexport

\* With Primary Organization Affiliations and Selected Board Seats

## ACKNOWLEDGMENTS

The Commission recognizes, with appreciation, the contributions of the Marsh McLennan and the NACD Future of the American Board teams for their work on this initiative:

### John Colas

Partner and Vice Chairman, Financial Services Americas, Oliver Wyman

### Michelle Daisley

Partner, Oliver Wyman

### Alina Lantsberg

Partner, Head of Retail and Business Banking Oliver Wyman

### Andrew Medland

Partner, Oliver Wyman

### Lucy Nottingham

Director, Marsh McLennan Advantage

### Jason Wells

Managing Director, Marsh

### Mallory Bucher

Associate Director, Corporate Governance Content, NACD

### Ellen Errico

Art Director, NACD

### Sarah King

Senior Project Manager, Board Advisory Services, NACD

### Friso van der Oord

Senior Vice President, Content, NACD

### Dylan Sandlin

Digital and Cybersecurity Content Lead, NACD

### Ted Sikora

Project Manager, Survey and Business Analytics, NACD

### Margaret Suslick

Manager, Copy Editing and Knowledge Management, NACD





National Association of Corporate Directors  
1515 N. Courthouse Road  
Suite 1200  
Arlington, VA 22201  
[nacdonline.org](http://nacdonline.org)

