



Midyear observations on the 2023 board agenda



In light of the high levels of ongoing disruption and uncertainty companies have faced in the first half of 2023—growing geopolitical risk and disruption, global economic volatility and inflation, a new phase of the Russia-Ukraine war, domestic polarization, risks posed by generative AI, regulatory developments, and more—we offer the following supplemental observations to our **On the 2023 Board Agenda** (issued in December 2022) as boards and their committees continue to calibrate their 2023 agendas.

Generative artificial intelligence (AI)

In the early months of 2023, major advances in the development and use of generative AI made headlines—including the promises and perils of the technology and its ability to create new, original content, such as text, images, and videos. Indeed, generative AI is being discussed in most boardrooms, as companies and their boards are seeking to understand its associated opportunities and risks—a challenge given the pace of the technology’s evolution.

We hear three recurring themes:

- The need for board education so that all directors have a basic understanding of generative AI, its potential benefits and risks, and how the company might use the technology.
- The importance of establishing and updating governance structure and policies regarding the use of the technology by the company and its employees.
- The need to reassess the governance structure for board and committee oversight of generative AI.

Board education. Many boards are asking management for a high-level training session—with third-party experts, as necessary—on generative AI and its potential benefits and risks.

The potential benefits of AI will vary by industry, but might include automating various business processes, such as customer service, content creation, product design, and marketing plan development, as well as improvements to healthcare, the creation of new drugs, etc.

The training session should include an overview of the major risks posed by generative AI—including additional reputational and legal risks to the company. For example:

- **Inaccurate results.** The accuracy of generative AI depends on the quality of the data it uses, which may be inaccurate or biased, and come from the internet and other sources. It is essential that management closely scrutinize the data results. Even so, an **explanation** of AI results is a challenge, as generative AI results are built on correlations and not causality.

- **Intellectual property risks** may include unintended disclosure of sensitive or proprietary company information to an open generative AI system by an employee, as well as unintended access to third-party intellectual property (IP) when an employee's prompt to an AI system generates the IP information.
- **Data privacy risk is a major concern with generative AI**, since user data is often stored to improve the quality of data.
- **Increased cybersecurity risks.** Cybercriminals can use the technology to create more realistic and sophisticated phishing scams or credentials to hack into systems.
- **Compliance risks** arising from the rapidly evolving global regulatory environment. Monitoring and complying with evolving AI legislation must be a priority for management.
- Finally, **bad actors** can create so-called **deepfake** images or videos with uncanny realism, which might negatively portray the company's products, services, or executives.

Generative AI governance structure and policies

Boards can begin to probe management as to what generative AI governance structure and policies are appropriate for the company. It's important to develop a governance structure and policies regarding the use of this technology early on, while generative AI is still in its infancy.

Key questions to ask may include:

- How and when is a generative AI system or model—including a third-party model—to be developed and deployed, and who makes that decision?
- How is management mitigating these risks—and what generative AI risk management framework is used?
- How is the company monitoring the legislative and regulatory proposals to govern the use of generative AI?
- Does the organization have the necessary generative AI-related talent and resources?

Board and committee oversight of generative AI

We hear from many directors that there is not necessarily one committee that has oversight responsibility for generative AI. Rather, given its strategic importance, oversight is often a responsibility for the full board. Board members also emphasize that director education is critical to help ensure that the board as a whole is up to speed on the topic. Whether the board has or seeks directors with generative AI expertise or uses outside experts is an issue for each board to consider. Some directors caution against bringing on a "specialist," but acknowledge that having board members with significant business technology experience could be helpful.

Geopolitical and economic risks and uncertainty

Much has changed in the geopolitical and global economic environment. From our conversations with economists and geopolitical advisors, it's clear that companies face an onslaught of risks. According to many advisors, at the macro level, the era of convergence has given way to one defined by fragmentation. From the end of World War II until a few years ago there was a "a coming together" on trade, capital flow, and accounting standards, but today is marked by divergence and de-risking. As one geopolitical observer noted during our June Board Leadership Conference, "China was expected to become more like the US, but that hasn't happened."

Other geopolitical factors and hotspots highlighted in our discussions with economists and geopolitical advisors include:

- **The escalation of the Russia-Ukraine war**, which is entering a dangerous phase with a Ukrainian counteroffensive underway and the possibility for more escalatory outcomes. Conditions appear to be in place for Western support of Ukraine for the immediate future, but prospects for a diplomatic resolution appear to be off of the table for foreseeable future.
- **The continuing deterioration of the US-China relationship**, described as one of "managed decline." While it appears that neither side wants escalatory incidents, they cannot be entirely ruled out.

- **The disruptive potential of generative AI.** From a political, social, and geopolitical perspective, there is potential for massive disruption caused by misinformation or disinformation.
- **The polarization of society.** As one observer noted, “The geopolitical risk I worry most about is the polarization of our society, and our country’s vulnerability to misinformation.”

These and other risks, including supply chain disruptions, cybersecurity incidents, inflation, interest rates, market volatility, and the risk of a global recession—combined with the deterioration of international governance—will continue to drive global volatility and uncertainty.

Assessing the company’s geopolitical risk awareness. As we hear from geopolitical advisors, this environment calls for a realistic assessment of the company’s capabilities in managing global geopolitical and economic risk and uncertainty—and that includes

risk management, as well as business continuity and resilience. A continual updating of the company’s risk profile and more scenario planning, stress testing strategic assumptions, and analyzing downside scenarios will be essential to staying agile. Boards need to hear diverse perspectives from a variety of sources.

In assessing management’s processes for identifying and managing geopolitical risks and their impact on the company’s strategy and operations, boards may ask:

- Is there an effective process to monitor changes in the external environment and provide early warning that adjustments to strategy might be necessary?
- How has the company’s risk profile changed as its supply chain has been reshaped?
- Is the company prepared to weather an economic downturn?

As one geopolitical advisor noted, risk events matter, but it’s much more important to think about the broader structural environment that raises and lowers the probability of each risk and to understand the different possibilities. Rather than reacting to events, taking a forward-looking approach—without trying to forecast specific risks—can be helpful.

Crisis readiness and resilience. Assessing management’s crisis response plans should be a board priority. Are crisis response plans robust, actively tested or war-gamed, and updated as needed? Do they include communications protocols to keep the board

apprised of events and the company’s response, as well as to determine if and when to disclose matters internally and/or externally?

Make business continuity and resilience part of the discussion. Resilience is the ability to bounce back when something goes wrong and the ability to stand back up with viable strategic options for staying competitive and on the offense in the event of a crisis. “Focus on resilience and prepare for the idea of disruption and practice dealing with disruption.”

Regulatory developments on climate, cybersecurity, HCM, and other ESG and sustainability disclosures

Demands for higher-quality climate and other ESG disclosures should be prompting boards and management teams to reassess and adjust their governance and oversight structure relating to climate and other ESG risks—and to closely monitor SEC and global regulatory developments in these areas.

SEC developments. In June, the SEC released its Spring 2023 Regulatory Agenda, which outlines the SEC’s rulemaking priorities over the next 12 months. Release of a final climate disclosure rule is now anticipated for October 2023. Significant questions about the final rule include the nature of the disclosures that might be required in the financial statements and the disclosure of greenhouse gas (GHG) emissions, in particular, Scope 3.

On July 26, the SEC adopted [final cybersecurity rules](#). The rules require SEC registrants that are subject to the 1934 Act to disclose information about a material cybersecurity incident “within four business days after the registrant determines that it has experienced a material cybersecurity incident.” Also see [“SEC finalizes cybersecurity rules”](#) and [“Public Company Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure.”](#)

October is also listed as the anticipated release of proposed amendments to the human capital management (HCM) disclosures. The HCM proposal could include detailed quantitative and qualitative disclosures on workforce-related topics like diversity, turnover, compensation and benefits, and training. It is unclear whether the proposal will also require more expansive disclosures regarding a company’s governance, strategy, and risk management for its HCM.

Global regulatory developments. Companies doing business abroad will also want monitor and maintain compliance with other climate and ESG regimes. For example, on June 26, the International Sustainability Standards Board published its first two IFRS® Sustainability Disclosure Standards: general requirements (IFRS S1) and climate (IFRS S2). Subject to adoption by local jurisdictions, the effective date of the standards is January 1, 2024. However, companies can elect to disclose only climate-related information in the first year of application. And on June 9 the European Commission released a near-final set of European Sustainability Reporting Standards (ESRSs) for consultation; the comment period ended July 7. The final standards—which comprise just the first set of ESRSs—will be issued by the end of August and the first wave of companies will adopt them from January 1, 2024.

The anticipated SEC, ISSB, and EU climate-related disclosure requirements will differ in a number of ways; however, the disclosure of GHG emissions is expected to be common. We expect this reporting to be heavily informed by the Greenhouse Gas Protocol, which has emerged as a nexus in the climate reporting ecosystem.

The proliferation of new and complex disclosure mandates is challenging companies' ability to update their disclosure processes and internal controls and adequately staff their finance functions to ensure compliance. For multinationals facing differing ESG reporting requirements around the world, there is even more complexity. At the same time, companies are being pressured by investors, employees, and customers for more disclosure. Given the scope of the undertaking, boards and audit committees should encourage management to prepare—as many companies are—by assessing management's path to compliance, and closely monitoring the rulemaking process.

2023 proxy season results

On June 29th, Pamela Marcogliese, a partner at Freshfields, joined KPMG Board Leadership Center (BLC) Senior Advisor Stephen Brown to discuss 2023 proxy results and key takeaways for management teams and directors. During the recent proxy season, shareholders submitted more than 800 proposals, with S&P 500 companies receiving 80 percent of those proposals. Relatively few shareholder proposals received majority support. Highlights from the discussion included the following:

- **ESG proposals** accounted for 90% of all shareholder proposals; however, only 1% of environmental proposals and 1.2% of social proposals received greater than majority support. Proposal topics continue to follow cultural trends, with increased attention on reproductive rights, workers' rights, human rights, environmental considerations, and political contributions.
- **Climate change proposals** made up a quarter of all environmental and social proposals, with a number of proposals focused on adopting GHG emission targets in line with goals set by the Paris Agreement, but average support for these proposals is down year over year. Only two environmental proposals received majority support.
- **Anti-ESG proposals** and "masked" ESG proposals were submitted on a variety of topics and a number of these proposals were submitted for effect (e.g., requesting companies rescind prior shareholder proposals).
- **Universal proxy** did not unleash an increased numbers of proxy fights; settlements increased, and hundreds of companies amended their advance notice bylaws in the wake of universal proxy rule effectiveness.



Looking behind this proxy season data, the webcast presenters highlighted important messages for directors, particularly regarding ESG. While support for voted ESG proposals decreased, investors and companies still view ESG as important—and as a risk. When the ESG movement started, neither side fully understood what ESG meant. Today when people say ESG, they are referring to material operational and business risks, and how the company is going to respond.

These material business risks should be the focus of shareholder engagement. And given the anti-ESG currents today, companies may need to refine their messaging around ESG concepts, including the “S” or social topics the country is grappling with.

View the webcast replay and presentation from Freshfields at boardleadership.kpmg.us.

Communication and coordination among board committees

As the issues and topics highlighted above suggest, the increasing complexity and fusion of risks unfolding simultaneously requires a more holistic approach to risk management and oversight. Rarely does a risk fit neatly into a single, siloed category, and risks are often interrelated. A siloed approach to managing risks—such as generative AI, environmental, social, and other ESG risks, compliance risks, and geopolitical risks—is no longer viable. Investors, regulators, ESG rating firms, and other stakeholders are demanding higher-quality disclosures about a variety of risks and how boards and their committees are overseeing their managements.

In this challenging environment, many boards are reassessing the risks assigned to each standing committee; in the process, they are often assigning oversight responsibility to multiple committees for various aspects of a particular risk. For example, in the oversight of climate, HCM, and other ESG risks, the nom/gov, compensation, and audit committees may have some overlapping oversight responsibilities. While cybersecurity and data governance oversight may reside in a technology committee (or other committee), the audit committee may also have oversight responsibilities. Other examples of risks for which multiple committees may have oversight responsibilities include culture, talent, and compliance.

Given these overlapping committee oversight responsibilities, a challenge for boards is to encourage more effective information sharing and coordination. We see boards taking various approaches:

- Identify areas where committee oversight responsibilities may overlap and develop a process for frequent communication and discussion of activities in these areas.
- Maintain overlapping committee memberships or informal cross-attendance at committee meetings.
- Conduct joint committee meetings when an issue of strategic importance to multiple committees is on the agenda.
- Hold periodic meetings of committee chairs to discuss oversight activities.
- Insist on focused, appropriately detailed, and robust committee reports to the full board.

About the KPMG Board Leadership Center

The KPMG Board Leadership Center (BLC) champions outstanding corporate governance to drive longterm value and enhance stakeholder confidence. Through an array of insights, perspectives, and programs, the BLC—which includes the KPMG Audit Committee Institute and close collaboration with other leading director organizations—promotes continuous education and improvement of public and private company governance. BLC engages with directors and business leaders on the critical issues driving board agendas— from strategy, risk, talent, and ESG to data governance, audit quality, proxy trends, and more. Learn more at kpmg.com/us/blc.

Contact us

kpmg.com/us/blc

T: 800-808-5764

E: us-kpmgmktblc@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization. USCS002965-4A