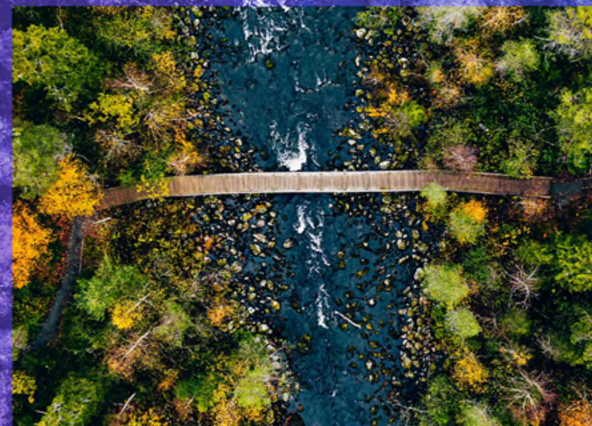
Directors Quarterly

Insights from the Board Leadership Center

October 2023



Geopolitical risk on the map

Geopolitical risks are a top concern for business leaders responding to our 2023 US CEO Outlook, reflecting an increasingly fragmented global economy that is more susceptible to external shocks. Given the global nature of many of the issues that companies are facing, from climate change and supply chains to data privacy and artificial intelligence, it's not surprising that geopolitical risks are top of mind for CEOs. In light of the operational, regulatory, and reputational implications of these global issues, it's clearer than ever that the US is not an island.

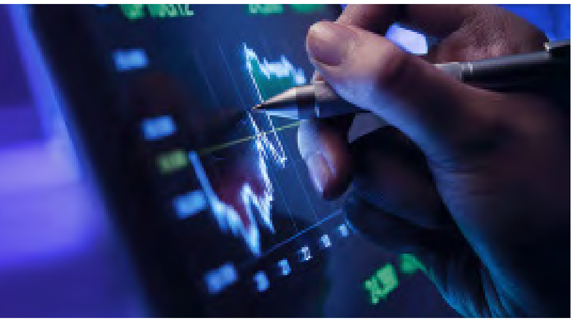
In this edition of *Directors Quarterly*, we detail steps to help boards take a holistic approach to the oversight of geopolitical risk. We also share insights from interviews with board members and business leaders about the changing board-management conversation on climate. Those discussions are increasingly focusing on value creation, risk, talent, and communication—all critical *business* issues.

In addition, we highlight financial reporting and auditing developments that audit committees should be paying attention to this quarter, including California's climate disclosure laws and recent updates from the SEC and PCAOB. Finally, we detail ways to enhance the audit committee–chief audit executive relationship, which is increasingly important for staying attuned to the company's changing risk profile.

John H. Rodi
Leader
KPMG Board Leadership Center (BLC)

What's inside

Financial reporting and auditing update



Below we summarize accounting and financial reporting developments potentially affecting companies in the current period or near term for audit committees to monitor.

ESG reporting update

Standard-setting activity has accelerated with the release of the State of California's Climate Accountability Package, the IFRS® Sustainability Disclosure Standards issued by the International Sustainability Standards Board (ISSB), and European Sustainability Reporting Standards (ESRSs) in the EU.

California's Climate Accountability Package

California Governor Gavin Newsom signed two landmark bills that will require companies to disclose their greenhouse gas (GHG) emissions and climate risks. The bills—SB-253 and SB-261—have national implications, affecting thousands of US companies that operate in California.

SB-253, the Climate Corporate Data Accountability Act, requires disclosure of GHG emissions data—Scopes 1, 2, and 3—by all US business entities (public or private) with total annual revenues in excess of $1 billion that do business in California. Disclosures will be in accordance with the Greenhouse Gas Protocol, with reporting for Scope 1 and 2 emissions to begin in 2026, and reporting for Scope 3 emissions to begin in 2027. Businesses will also be required to obtain assurance over their Scope 1 and 2 emissions, with Scope 3 potentially being added later.

SB-261, the Climate-Related Financial Risk Act, requires all US companies—public or private, with total annual revenues in excess of $500 million that do business in California—to disclose their climate-related financial risks and measures taken to reduce or adapt to such risks. The law excludes companies subject to regulation by the California Department of Insurance or that are in the insurance business in another state. Companies' disclosures will need to be made no later than January 1, 2026, and every two years thereafter, and be prepared in accordance with the Task Force on Climate-related Financial Disclosures (TCFD) or similar reporting standards (e.g., the IFRS® Sustainability Disclosure Standards issued by the ISSB).

In signing the bills, Governor Newsom noted some concerns that would be addressed by the state Administration and the legislature. Also see CA Climate Laws: GHG Emissions and Risk Reporting.

ISSB developments

On June 26, the ISSB issued its first two standards—the general standard (IFRS S1) and the climate standard (IFRS S2). The standards are effective for fiscal years beginning on or after January 1, 2024, but individual jurisdictions will need to decide whether and how to incorporate the standards into local requirements. Companies can also decide to adopt voluntarily.

The International Organization of Securities Commissions endorsed the standards in July 2023 and the list of countries considering adopting or incorporating them is growing. In addition, and notably for US companies, CDP (formerly, Carbon Disclosure Project) announced it will incorporate the climate standard into its disclosure system from 2024.

The ISSB published a comparison of the requirements in the climate standard and the TCFD recommendations, demonstrating that companies that apply the ISSB™ Standards will meet the TCFD recommendations. The TCFD announced that it is winding down operations and, beginning in 2024, the IFRS Foundation will take over monitoring of companies' progress on climate-related disclosures.

EU developments

On July 31, the European Commission (EC) adopted as a delegated act the first set of ESRSs. Compliance with the ESRSs, under the Corporate Sustainability Reporting Directive (CSRD), will be required as early as 2024 for some companies.

The first set of ESRSs includes two cross-cutting standards (general concepts and overarching disclosures) and ten topical standards (climate change, pollution, water and marine resources, biodiversity and ecosystems, resource use and circular economy, own workforce, workers in the value chain, affected communities, consumers

Continued

and end-users, business conduct). Companies will need to include information from their value chain and assess which topics (impacts, risks, and opportunities) to report using the double materiality concept, which requires information that is material from either a financial or an impact perspective.

Interoperability between the standards

Consistency in how companies report globally is important to supporting investor decisions and creating a level playing field for companies seeking investment. From a preparer's perspective, interoperability is important in easing the burden of reporting. Consistency runs deeper than equivalent disclosures—it also requires alignment of the inputs and in the basis of measurement.

The ISSB has been working closely with jurisdictional standard-setters to maximize interoperability between its standards and incoming mandatory reporting frameworks—e.g., the EC and EFRAG in the EU, and the SEC in the US. With the first set of ESRSs now issued, the work to analyze interoperability is underway.

EU supply chain acts

While companies are mostly focused on reporting obligations, more governments are seeking to regulate activities within supply chains with new laws aiming to prevent and mitigate environmental and social risks within company supply chains. Two such instances in the EU are the German Supply Chain Due Diligence Act, which took effect in January 2023, and the EU's proposed Corporate Sustainability Due Diligence Directive. See Impact of EU supply chain laws on US companies.

Compliance with such laws requires extensive due diligence and risk management throughout a company's supply chain. This may require embarking on new due diligence processes with other companies in the supply chain and in some cases parting ways with suppliers.

SEC developments

The SEC issued its final cybersecurity rules in July (see **SEC issues final cybersecurity rules**, below). Additionally, the SEC's Spring 2023 Regulatory Agenda targeted a final climate rule and a proposal for human capital management disclosures for October 2023; these targets now seem aggressive. In addition, a proposal for corporate board diversity is slated for April 2024.

SEC issues final cybersecurity rules

In July, the SEC issued its final rules—effective September 5, 2023—that will require several new and enhanced disclosures on cybersecurity risk management, strategy, governance, and incident reporting. Under the final rules, companies must disclose new information based on two broad categories. Public companies subject to the Securities Exchange Act of 1934 are required to disclose material "cybersecurity incidents" on Form 8-K and disclose material information regarding their cybersecurity risk management, strategy, and governance in their annual reports on Form 10-K.

Public companies will be required to report information regarding a material "cybersecurity incident" within four business days after the company determines that the incident was material—not from the time of discovery of the incident. And companies must make materiality determinations "without unreasonable delay" after discovery of the incident. If the US Attorney General determines that immediate disclosure poses a substantial risk to national security or public safety, and notifies the SEC in writing, disclosure may be delayed for a maximum of 60 days (absent extraordinary circumstances). Updated incident disclosures on an amended Form 8-K are required for any new information about a previously disclosed material incident that was unavailable or undetermined at the time of the initial Form 8-K filing.

Companies must describe in Form 10-K their processes for assessing, identifying, and managing material risks from cybersecurity threats, as well as the material effects or reasonably likely material effects of risks from cybersecurity threats and previous cybersecurity incidents. While companies will not be required to disclose board-level cybersecurity expertise, they will be required to describe the board of directors' oversight of risks from cybersecurity threats and management's role and expertise in assessing and managing material risks from cybersecurity threats.

Companies—other than smaller reporting companies—must begin complying with the incident disclosure requirements on December 18, 2023. Smaller reporting companies must begin complying on June 15, 2024. All public companies will be required to make Form 10-K annual disclosures beginning with annual reports for fiscal years ending on or after December 15, 2023.

Other SEC headlines

SEC statement on the importance of comprehensive risk assessment by auditors and management

In a statement from the SEC, Chief Accountant Paul Munter highlighted the critical role of risk assessment—particularly, the SEC's concerns about auditors and management appearing to be

Continued

too narrowly focused on information and risks that directly impact financial reporting while disregarding broader, entity-level issues that may also impact financial reporting and internal controls. In view of these concerns, the statement discusses management's obligations with respect to risk assessments, and addresses auditors' responsibility as gatekeepers to hold management accountable in the public interest.

SEC staff sample comment letter: China-specific disclosures

The SEC Division of Corporation Finance posted an illustrative letter with examples of comments issued to companies regarding China-specific disclosures. In general, the Division is requesting more prominent, specific, and tailored disclosures about China-specific matters so investors have the material information they need to make informed investment and voting decisions. The sample letter expands on guidance previously issued by the Division on China-specific disclosures and focuses on three key areas: disclosure obligations under the Holding Foreign Companies Accountable Act; specific and more prominent disclosure about material risks related to the role of the government of the People's Republic of China in the operations of Chinese-based companies; and disclosures related to material impacts of certain statutes.

PCAOB proposal on noncompliance with laws and regulations

The PCAOB has proposed sweeping changes to auditing standards that would heighten auditors' responsibilities for detecting legal and regulatory noncompliance and alerting appropriate members of management and audit committees when instances of noncompliance with laws and regulations (NOCLAR) are identified. The PCAOB is also proposing to amend other auditing standards to better incorporate consideration of NOCLAR.

In addition to the impact on audits, the proposed amendments would likely also affect the company, its processes and controls and the level of effort required of management by, for example, creating or causing:

- a need to evaluate the design, implementation, and operating effectiveness of controls over compliance in addition to controls over financial reporting;
- increased inquiries of management regarding NOCLAR;
- a need for management to compile complete lists of relevant laws and regulations across the company and its operations, including across multiple jurisdictions, and expand its risk assessment process to consider this population;
- additional process documentation and resources for walkthroughs over identifying and investigating NOCLAR;
- tests over the relevance and reliability of information provided by management regarding NOCLAR; and
- increased costs that could be substantial, including additional resources, legal fees, auditor fees, and other costs.

According to the Center for Audit Quality (CAQ), "this is the most significant PCAOB proposal since their 2011 Concept Release on mandatory firm rotations." The CAQ is encouraging the PCAOB to further engage with all stakeholders—auditors, management, audit committees—to better understand the implications of the proposal and whether it will meet the PCAOB's objectives.

The comment deadline ended August 7. ■

For more updates, visit Financial Reporting View.

Shifting geopolitics and the role of the board

The pace and impact of geopolitical developments have raised the stakes on a company's ability to systematically identify and prioritize a broad range of geopolitical threats and to assess their impacts in a targeted way.

Nearly three-quarters of companies surveyed said that their boards discuss geopolitical issues more frequently now than they did just two or three years ago.[1] In a 2023 survey, directors indicated that key geopolitical factors would have "a significant or some" impact on the company's strategy, including supply chain disruptions (88%), the political environment (80%), the war in Ukraine (70%), and trade policies.[2]

"Companies recognize they can no longer operate above the fray of international relations," says Alex Kazan, chief commercial officer, Eurasia Group. "Understanding the far-reaching impacts of geopolitics on the business is imperative, and it requires a disciplined process."

Despite an increasing board-level focus on various geopolitical issues and risks, many boards continue to wrestle with how best to oversee the company's efforts to manage geopolitical risks and opportunities holistically and proactively.

"Boards can often understand and digest the macro implications of world events," says John Rodi, leader of the KPMG Board Leadership Center, "but it can be difficult to translate those developments into clear strategic and operational implications for the business."

Understanding the interplay of certain risks, monitoring international developments and structural shifts, gaming out scenarios, and connecting critical dots requires an astute and focused geopolitical lens. Boards have a pivotal role to play in assessing how effectively the company is monitoring and managing geopolitical risk, identifying gaps, and strengthening the board's own geopolitical acumen and risk oversight processes, with the endgame being a robust geopolitical risk governance framework.

While every business will face unique challenges operating in a global environment, several basic steps can help boost every board's effectiveness in helping the company navigate geopolitical risk and opportunities more systematically and cohesively.

In collaboration with Eurasia Group, our paper describes three areas of focus for assessing the company's governance structure and processes for managing geopolitical risk:

- Helping to ensure that management has robust processes in place to manage geopolitical by:
  - Identifying the key geopolitical risks and their potential impacts to the business.
  - Establishing clear responsibility for developing a mitigation plan for each risk to a specific individual and hold those individuals accountable.
  - Providing robust, periodic reporting to the board on the company's key geopolitical risks—including current risks, future scenarios, and crisis-readiness plans.
- Obtaining a diversity of perspectives, including third-party expert views, regarding the company's geopolitical risks and management of those risks.
- Considering the board's own geopolitical acumen and oversight framework.

The approaches described in the paper can help boards deepen their engagement, including helping management establish or strengthen a geopolitical risk governance framework and processes to respond to geopolitical events and turbulence, and understand the unfolding structural changes that are reshaping the geopolitical landscape and the implications for the company's future. ■

Read Shifting geopolitics and the role of the board.

[1] "Geopolitical and economic risks: Board oversight in an evolving world," Corporate Secretary, January 5, 2023.

[2] What Directors Think 2023 Survey, Diligent and Corporate Board Member, February 2, 2023.

Advancing the board-management conversation on climate communication

This excerpt is adapted from Boardroom climate competence: Advancing the board-management conversation, the third paper in a series by the KPMG BLC and Plan C Advisors. Building on our prior work, which discussed boardroom imperatives and processes for climate-related oversight, our latest paper offers insights on how boards of directors and executives can engage one another on the topics of value creation, risk, talent, and communication.

Insights from interviews for our recent paper, Boardroom climate competence: Advancing the board-management conversation, indicate that board members and management are engaging more frequently and in a more detailed way in discussions that factor in climate change to value creation, risk, and talent. In addition, changes in the regulatory landscape and investor expectations are driving enhanced board scrutiny and a focus on clear and consistent climate-related communication.

A web of reporting and regulatory disclosure frameworks dots the globe and makes consistent information and messaging its own challenge. Companies increasingly face the task of managing voluminous and sometimes competing requests for information from multiple stakeholders, including the pending SEC climate rules, the EU's CSRD, the Greenhouse Gas Protocol, ISSB standards, the TCFD, and the new California climate disclosure laws.

"With each of these [disclosure frameworks], there's more data and more qualitative assessments that the company has to do," said one director. "We have added staff and a data analyst just to prepare. And we're conducting a gap analysis. What do we have? What do we not have and what have we budgeted for? How are we going to bring it all together?" Another director put it more bluntly: "There's one rule: Don't lie. And as a board, we have to consider how the company is responding to investor questions. Are we getting ahead of it? We may be able to avoid contentious shareholder fights through better communication."

Oversight of disclosure as a matter of compliance

While voluntary sustainability reports may have received a light board or committee review, existing government scrutiny and upcoming mandatory disclosures in the EU (and, eventually, in the US) require a deeper level of oversight, comparable to oversight of financial disclosure. This begins with clarity as to who on the board or which committee has responsibility for oversight, and which communications that draw on the company's climate goals and metrics will be reviewed—earnings releases, quarterly and annual reports, proxy statements, investor presentations, promotional material, and more. "Is what we are currently disclosing precise enough to withstand SEC scrutiny?" asked one director. "The audit committee needs to know that the data is consistent and reportable."

Beyond compliance—moving toward alignment

Cutting through the noise across regulatory filings, sustainability reports, analyst days, marketing and advertising, and customer and employee relations, the company must communicate its approach on climate in a manner that is coordinated with strategy, verifiable by third parties, transparent to all stakeholders, and, above all, consistent. "Having the leader of the company driving the message makes all the difference," said one executive.

Boards should engage with management and ask the following questions:

- Is the company's message clear, concise, and consistent?
- Is company leadership, including the board, able to articulate how the company's strategy incorporates climate risk and opportunity?

Continued

- What is the nature of reported and disclosed climate data? How has it been validated, assured, or audited?
- Who is the company sharing information with (third parties, employees, customers) and is that information consistent with what is being shared publicly?
- How does the board organize itself to set the tone and review (as needed) climate-related communications?

How the board and management approach climate-related issues will vary from company to company, influenced by the specific issues of the business and the culture of the organization and of the board. But as we've seen through our interviews, no matter how each company addresses climate, it can only benefit from increased dialogue.

"You have to talk about it thoughtfully and it has to be completely tied to your business strategy," said one director. "You can't ignore it—that's at your peril."

Susan Angele is a senior advisor at the KPMG Board Leadership Center. Amanda North is the founder and CEO of Plan C Advisors.

Staying in sync with internal audit and the chief audit executive

Understanding a company's strategic and operational risks in an increasingly complex business environment is both a top priority and a top challenge—and internal audit has a vital role to play. Staying attuned to the company's changing risk profile—including its control environment, culture, and crisis readiness—has put a premium on internal audit being in sync with the audit committee.

This year alone, major shifts in the regulatory and business landscape are demanding more agility from internal audit. New cybersecurity disclosure rules for public companies have arrived, and final climate disclosure rules and proposed human capital management disclosure rules could follow shortly. The use and experimentation with artificial intelligence is becoming pervasive as well.

The chief audit executive (CAE) can help audit committees monitor these trends, understand what's happening at every level of the company (as the committee's eyes and ears), and connect the dots.

As panel members suggested during the KPMG Audit Committee Leadership Forum in June, keys to the CAE's value-add to the audit committee include the following:

- Recognizing how dramatically the business and risk landscape is changing and having a "healthy concern" about any claims of a static risk and internal control environment
- Understanding the importance of a robust, disciplined, process-oriented risk assessment that is not adversarial as the basis for the audit plan
- Developing an audit plan that is risk-based, adapts to the changing operating environment, and aligns with the organization's strategy and risk profile
- Being objective, process-oriented, and disciplined
- Maintaining robust two-way communication with the audit committee and making executive sessions regular and structured

"Internal control is a team sport," said one audit committee chair at a recent KPMG-sponsored event. "As an audit committee, you have to have a CAE whom you can rely on, who is agile, and who can adjust to changes in both reporting expectations and the risk environment."

Given the increasingly complex risk environment and the intense focus of regulators, investors, and other stakeholders, the audit committee should closely monitor internal audit's risk assessment process and its development of the audit plan. The committee should ask, for example, the following questions:

- To what extent does the CAE and internal audit participate in management committees responsible for the company's various strategic initiatives, including the identification and management of risks and related controls associated with those initiatives? How does internal audit interact with the company's risk management and compliance functions?
- As the company prepares to comply with new regulatory disclosure requirements for climate, cybersecurity, human capital management, and sustainability, does internal audit have a seat at the table? Does internal audit participate as a member of management's disclosure committee?
- Does internal audit have the talent, resources, and expertise to conduct a robust risk assessment and to develop and execute an audit plan that aligns with the company's risks?

Currently, CAEs view cyber, information technology, and sustainability risks at opposite ends of the risk spectrum in terms of the time and attention that internal audit devotes to them. According to the 2023 North American Pulse of Internal Audit, from the Institute of Internal Auditors, 78 percent of internal audit professionals viewed cybersecurity as a high or very high risk, with 57 percent responding the same for broader technology issues. By comparison, only 9 percent said the risk level for the range of sustainability risks was high or very high.

Continued

While climate and sustainability may be a long-tail or distant risk for some companies (and nearer for others), new regulatory mandates for climate disclosures both in the United States and globally—as well cybersecurity, human capital management, and other sustainability disclosures—will require an increased focus by internal audit.

"The chief audit executive needs to be comfortable with a risk environment that is rapidly changing," said another audit committee chair. "When significant shifts are needed in the audit plan—for example, with new disclosure requirements—flexibility is key."

Stephen L. Brown is a senior advisor at the KPMG Board Leadership Center. Michael A. Smith is a partner and internal audit leader at KPMG LLP.

This article originally appeared in the Fall 2023 issue of NACD Directorship *magazine.*

Mark your calendar

BLC-Eurasia Group webcast: The board and geopolitical risk

October 31, 11:00 a.m.–12:00 p.m. (EDT)

Join the KPMG BLC and Ian Bremmer, founder and president of Eurasia Group and GZERO Media, for a timely dialogue on the forces reshaping the geopolitical landscape and the implications for business and the boardroom.

To register, visit watch.kpmg.us/BLCwebcast.

KPMG Annual Accounting & Financial Reporting Symposium

November 30–December 1, Las Vegas

Designed for financial executives, the Symposium will include insights and information on trending topics like emerging technology, cybersecurity, and the latest on financial accounting and reporting developments. A separate one-day course on ESG Reporting will take place the day before the Symposium.

To register, visit execed.kpmg.com.

WCD Europe Institute 2023

October 26–27, Frankfurt, Germany

The 2023 Women Corporate Directors (WCD) Europe Institute, sponsored by KPMG, features discussions on corporate governance topics such as ESG, artificial intelligence, leading through a crisis, and geopolitical considerations. The event is complimentary for WCD members.

To register, visit wcdinstitutes.org.

KPMG Board Insights Podcast

On demand

Conversations with directors, business leaders, and governance luminaries to explore the emerging issues and pressing challenges facing boards today.

Listen or download now at listen.kpmg.us/BLCpodcast.

Selected reading

KPMG 2023 US CEO Outlook
KPMG LLP

Dealing with activist investors
Wachtell Lipton

The compensation committee's role in HCM
Semler Brossy

KPMG ESG assurance maturity index
KPMG International

NIST releases Cyber Framework 2.0
Mayer Brown

CEO tenure rates
Equilar

To receive articles like these from Board Leadership Weekly, register at *kpmg.com/blcregister*.

About the KPMG Board Leadership Center

The KPMG Board Leadership Center (BLC) champions outstanding corporate governance to drive long-term 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: 1-800-808-5764
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