Directors Quarterly

Insights from the Board Leadership Center

January 2024

Taking stock, looking ahead

The start of a new year is an important opportunity for boards to take a step back and reassess their agendas to help ensure that they are appropriately focused on the most critical issues for the company. Given the increasing breadth and complexity of issues that directors must oversee and the volatility and uncertainty of the business and risk environment, is the board—through its committee structure and allocation of oversight responsibilities—spending time on the right topics and in the most effective way? Leaving room on the agenda to consider future scenarios and address the unexpected (in addition to the must-dos) will be essential.

As directors fine-tune their board and committee agendas for 2024, our annual *On the agenda* messages highlight the mission-critical issues that should be considered in boardroom discussions throughout the year. In addition to reading excerpts from our board and audit committee publications, you can find our complete *On the 2024 agenda* series here.

This quarter, check out our financial reporting and auditing update for top takeaways from the AICPA & CIMA Conference on Current SEC and PCAOB Developments, questions to ask about ESG reporting obligations, and the impact of Pillar Two tax rules.

In this edition, we also share an interview with SEC Chief Accountant Paul Munter, including his views on audit committee expectations, oversight of risk management and the control environment, and audit committee and audit firm independence. Finally, we offer key areas of focus for boards as they oversee management's efforts to maintain effective third-party risk management programs amid the rapidly changing risk, regulatory, and compliance landscape.

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

What's inside

On the 2024 board agenda

Heading into 2024, companies face unprecedented disruption and uncertainty—wars in Ukraine and the Middle East, trade and geopolitical tensions, economic volatility, inflation and higher interest rates, technology and business model disruption, elevated cybersecurity risk, climate risk, domestic polarization, political gridlock in the US, and more. Advances in artificial intelligence (AI) and heightened regulation will add to the challenge.

In this volatile operating environment, demands—from investors, regulators, employees, and other stakeholders—for greater disclosure and transparency, particularly around the oversight and management of risks to the company's operations and strategy, will continue to intensify. The pressure on management, boards, and governance will be significant.

Drawing on insights from our survey work and interactions with directors and business leaders, our annual publication for boards of directors, *On the 2024 board agenda* includes nine issues to keep in mind as boards consider and carry out their 2024 agendas. We highlight four of these issues here:

Nine issues on the 2024 board agenda

- Link boardroom discussions on strategy, risk, and global disruption.
- Monitor management's efforts to design and maintain a governance structure for the development and use of generative AI.
- Maintain the focus on cybersecurity and data privacy and monitor management's preparations for compliance with the SEC's cybersecurity rules.
- Identify the company's material or strategically significant climate and ESG issues, and embed them in risk and strategy discussions.
- Keep abreast of management's preparations for new US, state, and global climate and sustainability reporting requirements.
- Enhance communication and coordination regarding risk oversight activities among the board and its committees.
- Clarify when the CEO/company should speak out on social issues.
- Make talent, human capital management (HCM), and CEO succession a priority.
- Think strategically about talent, expertise, and diversity in the boardroom.

Link boardroom discussions on strategy, risk, and global disruption.

Much has changed in the geopolitical and global economic environment. Companies face a deluge of risks, including the escalation of the wars in Ukraine and the Middle East; the continuing deterioration of the US–China relationship; the potential for massive political and social disruption caused by misinformation or disinformation; and the polarization of society. These and other risks, including supply chain disruptions, cybersecurity, inflation, interest rates, market volatility, and the risk of a global recession—combined with the deterioration of governance on the geopolitical level—will continue to drive global volatility and uncertainty.

At the same time, companies face potential disruption to business models and strategy posed by accelerating advances in digital technologies such as AI, including generative AI and blockchain.

Help management reassess the company's processes for identifying the risks and opportunities posed by disruption—geopolitical, economic, technological/digital, social, and environmental—and the impact on the company's long-term strategy and related capital allocation decisions. Does management have an effective process to monitor changes in the

external environment and provide early warning that adjustments to strategy might be necessary? That includes risk management as well as business continuity and resilience. It calls for frequent updating of the company's risk profile and more scenario planning, stress testing strategic assumptions, analyzing downside scenarios, considering the interrelationship of risks, and obtaining independent third-party perspectives.

Companies need to think about "events" and how they will impact the company's business model and strategy; however, it is also critical to understand the underlying structural shifts taking place—geopolitical, demographic, technological, economic, climate, global energy transition, societal, etc.—and the longer-term implications.

Monitor management's efforts to design and maintain a governance structure for the development and use of generative AI.

2023 saw major advances in the development and use of generative AI and its ability to create new, original content such as text, images, and videos. Indeed, generative AI has been the focus of discussion in most boardrooms as companies and boards seek to understand the opportunities and risks posed by the technology—a challenge given the pace of the technology's evolution.

The potential benefits of generative AI vary by industry but might include automating business processes such as customer service, content creation, product design, developing marketing plans, improving healthcare, and creating new drugs. The risks posed by the technology are significant, including inaccurate results, data privacy and cybersecurity risks, intellectual property risks (including unintended disclosure of the company's sensitive or proprietary information and unintended access to third-party IP), and compliance risks posed by efforts across the globe to regulate generative AI.

Given the strategic importance of generative AI to most companies, boards should be monitoring management's efforts to design and maintain a governance structure and policies for the development and use of generative AI. Among the areas of focus are the following:

- 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 are the company's peers using the technology?
- How is management mitigating the risks posed by generative AI and ensuring that the use of AI is aligned with the company's values? What generative AI risk management framework is used? What is the company's policy on employee use of generative AI?
- How is management monitoring rapidly evolving generative AI legislation in the US and globally, and ensuring compliance?
- Does the organization have the necessary generative AI–related talent and resources, including in finance and internal audit?

Boards should also assess their governance structure for board and committee oversight of generative AI. In addition to the full board's engagement in overseeing AI, do (should) certain committees have specific oversight responsibilities, including perhaps taking deeper dives into certain aspects of generative AI?

Maintain the focus on cybersecurity and data privacy and monitor management's preparations for compliance with the SEC's cybersecurity rules.

Cybersecurity risk continues to intensify. The acceleration of AI, the increasing sophistication of hacking and ransomware attacks, the wars in Ukraine and the Middle East, and ill-defined lines of responsibility—among users, companies, vendors, and government agencies—have elevated cybersecurity risk and its place on board and committee agendas.

The growing sophistication of the cyber threat points to the continued cybersecurity challenge—and the need for management teams and boards to continue to focus on resilience. As Gurbir S. Grewal, director of the SEC's Division of Enforcement emphasized, "As opposed to cybersecurity, cyber resilience is a concept that recognizes that breaches and cyber incidents are likely going to happen, and that firms must be prepared to respond appropriately when they do. In other words, it's not a matter of if, but when." [1]

Regulators and investors are demanding transparency into how companies are assessing and managing cyber risk and building and maintaining resilience. In July, the SEC adopted final rules that require public companies to disclose material "cybersecurity incidents" on Form 8-K within four business days of a materiality determination. The rules also require companies to disclose detailed, material information regarding their cybersecurity risk management, strategy, and

[1] Gurbir S. Grewal, "Remarks at Financial Times Cyber Resilience Summit," June 22, 2023.

governance in their Form 10-K, beginning with the 2023 10-K. The rules greatly expand companies' cybersecurity disclosure obligations. Preparations to comply are a significant undertaking for management, and board oversight of management's final preparations for the Form 8-K and 2023 Form 10-K disclosures is essential.

While data governance overlaps with cybersecurity, it is broader and includes compliance with industry-specific laws and regulations as well as privacy laws and regulations that govern how personal data—from customers, employees, or vendors—is processed, stored, collected, and used. Data governance also includes policies and protocols regarding data ethics—in particular, managing the tension between how the company may use customer data in a legally permissible way and customer expectations as to how their data will be used. Managing this tension poses significant reputation and trust risks for companies and represents a critical challenge for leadership. How robust and up to date is management's data governance framework? Does it address third-party cybersecurity and data governance risks?

Identify the company's material or strategically significant climate and ESG issues and embed them in risk and strategy discussions.

Despite some recent anti-ESG sentiment, expect the intense focus on ESG to continue in 2024. How companies manage material climate and other ESG risks is seen by many investors, research and ratings firms, activists, employees, customers, and regulators as fundamental to the business and critical to long-term value creation.

The clamor for attention to climate change as a financial risk has become more urgent, driven by reports that the summer of 2023 was the hottest on record, with global temperatures expected to reach new highs over the next five years; the frequency and severity of floods, wildfires, rising sea levels, and droughts; growing concern about climate-related migration and displacement; and concern by many experts that the window for preventing more dire long-term consequences is rapidly closing. Regulators and policymakers globally are placing greater demands on companies to act—and climate disclosures are a priority for the SEC and global regulators.

The 2023 proxy season saw an increase in shareholder proposals on climate and a broad range of ESG and diversity, equity, and inclusion (DEI) issues, but a marked decrease in support. While there was an increase in anti-ESG proposals and "masked" ESG proposals, anti-ESG proposals continued to receive low levels of shareholder support. This anti-ESG sentiment has expanded to include state laws, regulations, and litigation. Some 20 state attorneys general have launched attacks against ESG in various state and federal courts.

Despite this push-back against ESG, most investors continue to view material ESG issues as important. As BlackRock Chairman and CEO Larry Fink wrote in his 2023 Letter to Investors: "Many of our clients also want access to data to ensure that material sustainability risk factors that could impact long-term asset returns are incorporated into their investment decisions."[2]

In this environment, several fundamental questions should be front and center in boardroom conversations about climate and ESG:

- Which ESG issues are material or of strategic significance to the company? In the context of ESG, the term "material" does not have the same meaning as it does in the securities law context. The ESG issues of importance will vary by company and industry. For some, it skews toward environmental, climate change, and emission of greenhouse gases (GHG). Others may emphasize DEI and social issues.
- How is the company addressing these issues as long-term strategic issues and embedding them into core business activities (strategy, operations, risk management, incentives, and corporate culture) to drive long-term performance?
- Is there a clear commitment with strong leadership from the top and enterprise-wide buy-in?
- In internal and external communications, does the company explain why ESG issues are materially or strategically important? Indeed, some companies are no longer using the term "ESG."

Find the full *On the 2024 board agenda* and more at kpmg.com/us/blc.

[2] BlackRock, "Larry Fink's Annual Chairman's Letter to Investors," March 2023.

On the 2024 audit committee agenda

The business and risk environment has changed dramatically over the past year, with greater geopolitical instability, surging inflation, high interest rates, and unprecedented levels of disruption.

Audit committees can expect their company's financial reporting, compliance, risk, and internal control environment to be put to the test by an array of challenges—from global economic volatility and the wars in Ukraine and the Middle East to cybersecurity risks and ransomware attacks and preparations for US and global climate and sustainability reporting requirements, which will require developing related internal controls and disclosure controls and procedures.

Drawing on insights from our interactions with audit committees and business leaders, our annual publication for audit committee members, *On the 2024 audit committee agenda*, includes eight issues to keep in mind as audit committees consider and carry out their 2024 agendas. We highlight three of these issues here:

Eight issues on the 2024 audit committee agenda

- Stay focused on financial reporting and related internal control risks—job number one.
- Clarify the roles of management's disclosure committee and ESG teams and committees in preparations for new US, state, and global climate and other sustainability disclosures—and oversee the quality and reliability of the underlying data.
- Monitor management's preparations for and compliance with the SEC's cybersecurity rules.
- Define the audit committee's oversight responsibilities for generative AI.
- Focus on leadership and talent in the finance organization.
- Reinforce audit quality and stay abreast of proposed changes to PCAOB auditing standards, including its proposal relating to noncompliance with laws and regulations.
- Make sure internal audit is focused on the company's key risks—beyond financial reporting and compliance—and is a valued resource to the audit committee.
- Help sharpen the company's focus on ethics, compliance, and culture.

Stay focused on financial reporting and related internal control risks—job number one.

Focusing on the financial reporting, accounting, and disclosure obligations posed by the current geopolitical, macroeconomic, and risk landscape will be a top priority and major undertaking for audit committees in 2024. Key areas of focus for companies' 2023 10-K and 2024 filings should include:

Forecasting and disclosures. Among the matters requiring the audit committee's attention are disclosures regarding the impact of the wars in Ukraine and the Middle East, government sanctions, supply chain disruptions, heightened cybersecurity risk, inflation, interest rates, market volatility, and the risk of a global recession; preparation of forward-looking cash-flow estimates; impairment of nonfinancial assets, including goodwill and other intangible assets; impact of events and trends on liquidity; accounting for financial assets (fair value); going concern; and use of non-GAAP metrics. With companies making more tough calls in the current environment, regulators are emphasizing the importance of well-reasoned judgments and transparency, including contemporaneous documentation to demonstrate that the company applied a rigorous process. Given the fluid nature of the long-term environment,

disclosure of changes in judgments, estimates, and controls may be required more frequently.

In reviewing management's disclosures regarding these matters, consider the questions posed by the staff of the SEC's Division of Corporation Finance in its May 2022 sample letter pertaining to the Russia-Ukraine war and its July 2023 sample letter regarding China-specific disclosures. The sample comment letters may be instructive in considering the company's disclosure obligations posed by the wars in Ukraine, the Middle East (and the risk of a regional war), and the broader geopolitical, macroeconomic, and risk environment.

Internal control over financial reporting (ICOFR) and probing control deficiencies. Given the current risk environment, as well as changes in the business, such as acquisitions, new lines of business, digital transformations, etc., internal controls will continue to be put to the test. Discuss with management how the current environment and regulatory mandates—including new climate and cybersecurity rules—affect management's disclosure controls and procedures and ICOFR, as well as management's assessment of the effectiveness of ICOFR. When control deficiencies are identified, probe beyond management's explanation for "why it's only a control deficiency" or "why it's not a material weakness" and help provide a balanced evaluation of the deficiency's severity and cause. Is the audit committee—with management—regularly taking a fresh look at the company's control environment? Have controls kept pace with the company's operations, business model, and changing risk profile, including cybersecurity risks?

Importance of a comprehensive risk assessment. SEC Chief Accountant Paul Munter released a statement highlighting the importance of a comprehensive risk assessment by management and auditors—particularly, the SEC's concerns about auditors and management appearing to be 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. Munter's statement discussed management's obligations with respect to ongoing risk assessments and addressed auditors' responsibility as gatekeepers to hold management accountable in the public interest.

Committee bandwidth and skill sets. The audit committee's role in overseeing management's preparations for new US, state, and global climate and other sustainability reporting requirements, coupled with its role in overseeing new SEC cybersecurity disclosures, further expands the committee's oversight responsibilities beyond its core oversight responsibilities (financial reporting and related internal controls, and internal and external auditors). This expansion should heighten concerns about audit committee bandwidth and "agenda overload." Reassess whether the committee has the time and expertise to oversee the major risks on its plate today. Such a reassessment is sometimes done in connection with an overall reassessment of issues assigned to each board standing committee. For example, do cybersecurity, climate, sustainability, or "mission-critical" risks such as safety, as well as AI, including generative AI, require more attention at the full-board level—or perhaps the focus of a separate board committee? The pros and cons of creating an additional committee should be weighed carefully, but considering whether a finance, technology, risk, climate and sustainability, or other committee—and perhaps the need for directors with new skill sets—would improve the board's effectiveness can be a healthy part of the risk oversight discussion.

Clarify the roles of management's disclosure committee and ESG teams and committees in preparations for new US, state, and global climate and other sustainability disclosures—and oversee the quality and reliability of the underlying data.

As discussed in *On the 2024 board agenda*, an important area of board focus and oversight will be management's efforts to prepare for US, state, and global regulatory mandates that will dramatically increase climate and other sustainability disclosure requirements for US companies.

While US companies await final SEC climate rules, they are preparing to comply with California climate legislation signed into law in October 2023. US companies with international operations are also assessing the potential impacts of, and preparing for compliance with, European Sustainability Reporting Standards (ESRSs) issued under the EU's Corporate Sustainability Reporting Directive (CSRD)—which covers a broad range of sustainability issues beyond climate—and IFRS® Sustainability Disclosure Standards issued by the International Sustainability Standards Board (ISSB), as well as other foreign disclosure regimes. Countries are already announcing adoption of, or commitments to consider adopting, the final ISSB™ Standards, including Australia (climate only), Brazil, Japan, and the UK.

The California laws and international climate standards, as well as the anticipated SEC climate rules—which will likely vary in important respects and have different effective dates—are based in part on the standards

and frameworks of the Task Force on Climate-related Financial Disclosures (the TCFD) and the Greenhouse Gas (GHG) Protocol and are highly prescriptive and expansive. Detailed disclosures in a number of areas would be required, including GHG emissions data (Scopes 1 and 2, and in many cases, Scope 3), with third-party assurance, as well as detailed disclosures about the impacts of climate-related risks and transition risks on the business, financials, strategy, and business model.

In the near term, US companies must determine which standards apply, effective dates, and the level of interoperability of the applicable standards. Monitoring SEC, state, and international developments will be critical. A key area of board and audit committee focus will be the state of the company's preparedness—requiring periodic updates on management's preparations, including gap analyses, resources, and skills/talent requirements to meet regulatory deadlines. In addition to the compliance challenge, companies must consider whether disclosures are consistent, and the potential for liability posed by detailed disclosures—as well as the US implications of a company making more detailed disclosures in another jurisdiction (such as the EU or under state laws).

This will be a major undertaking, with cross-functional management teams involved, including management's disclosure committee and management's ESG team/committee—often led by an ESG controller at larger companies—with multiple board committees overseeing different aspects of these efforts. Given the scope of the effort, audit committees should encourage management's disclosure committee and management's ESG team/committee to prepare now by developing management's path to compliance with applicable reporting standards and requirements—including management's plan to develop high-quality, reliable climate and sustainability data. Key areas of audit committee focus should include:

- Clarifying the disclosure committee's role and responsibilities in connection with disclosures contained in SEC and other regulatory filings and those made voluntarily in sustainability reports, websites, etc., including coordination with cross-functional management ESG team(s) or committee(s). Since disclosures that are not filed still carry potential liability, management should have processes in place to review these disclosures, including for consistency with filed disclosures.
- Reassessing the composition of the disclosure committee. Given the US, state, and global climate and other sustainability reporting requirements and the intense focus on these disclosures generally, companies should consider expanding management's disclosure committee or creating a subcommittee to include appropriate climate and other sustainability functional leaders, such as the ESG controller (if any), chief sustainability officer, chief human resources officer, chief diversity officer, chief supply chain officer, and chief information security officer.
- Encouraging management's disclosure committee to work with management's ESG team/committee to identify gaps, consider how to gather and maintain quality information, and closely monitor US, state, and global rulemaking activities.
- Expanding management's subcertification process to support CEO and CFO quarterly 302 certifications regarding design and operational effectiveness of disclosure controls and procedures.
- Understanding whether appropriate systems are in place or are being developed to ensure the quality of data that must be assured by third parties.

Monitor management's preparations for and compliance with the SEC's cybersecurity rules.

The SEC's rules require several new and enhanced disclosures on cybersecurity risk management, strategy, governance, and incident reporting. Companies must disclose new information in two broad categories:

- Companies are required to **disclose material "cybersecurity incidents" on Form 8-K,** within four business days after the company determines that the incident was material—not from the time of discovery of the incident. Companies must make materiality determinations "without unreasonable delay" after discovery of the incident.
- Companies are required to **disclose material information regarding their cybersecurity risk management, strategy, and governance in their annual reports on Form 10-K.** 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.

As companies finalize their preparations for these disclosures, we highlight the following areas for the audit committee's attention:

Cybersecurity risk management, strategy, and governance disclosures on Form 10-K. The preparation of these disclosures will take time and care, as the disclosures are detailed and extensive and will likely require a reassessment, and perhaps modification, of the company's existing risk management and governance processes, including board oversight processes. Boards should be working with management now as management prepares for the upcoming Form 10-K disclosures.

Management's cyber incident response plan. Management's cyber incident response policies and procedures, including disclosure controls and procedures and internal controls, must be reviewed and updated to provide for the timely consideration of materiality—at the same time that management may be engaged in remediation and investigation efforts. This would include a clear delineation of the responsibilities of management's cybersecurity and risk management teams, management's disclosure committee, and the legal department, as well as escalation procedures for determining materiality and the preparation and review of disclosures. Escalation protocols should provide for information from the technology team to be promptly provided to the cross-functional team making materiality determinations, and also address when the board is notified and how internal and external communications are handled. Management and the board should conduct periodic tabletop exercises to test management's response plans and procedures, including protocols for documenting incidents, evaluating for materiality, and drafting Form 8-K disclosures—and refine response plans and procedures to reflect what is learned from those exercises. Incident response plans should also be updated to take into account the changing cyber risk landscape.

Consideration of "materiality." While the definition of materiality has not changed, applying that standard in the context of a cybersecurity incident is not straightforward. In its final release, the SEC said that companies should consider qualitative factors in assessing the material impact of an incident, and indicated that harm to a company's reputation, customer or vendor relationships, or competitiveness, and the possibility of litigation or regulatory investigations or actions, may be examples of material impacts. Audit committees should confirm that management has in place policies and procedures for the cross functional team making materiality determinations, including procedures for the identification of significant cyber incidents that should be escalated and discussed with management's disclosure committee and legal team for final materiality determination, and documenting its materiality determinations. Companies may want to consider, in advance, what might constitute a material incident.

The role of management's disclosure committee. Consider the role and responsibilities of management's disclosure committee in developing and maintaining cybersecurity-related disclosure controls and internal controls and procedures. What resources and processes does the committee require to make a timely determination of materiality in the event of a cyber incident?

Find the full *On the 2024 audit committee agenda* and more at kpmg.com/us/blc.

Financial reporting and auditing update

2023 AICPA & CIMA Conference highlights

In December, the AICPA & CIMA hosted their annual Conference on Current SEC and PCAOB Developments, featuring speakers from the SEC, PCAOB, FASB, and other key players in the financial reporting infrastructure. We summarize some of the top takeaways from the conference below.

- **The importance of culture.** SEC representatives stressed the significance of an audit firm's culture in maintaining trust, while PCAOB representatives highlighted the shared responsibility of the audit committee, management, and others in the financial reporting ecosystem in upholding the auditor's gatekeeper role.
- **Risk assessment drives good reporting.** Properly assessing and communicating risks is crucial to the financial reporting process. It is essential for companies to take a holistic approach to risk assessment, considering entity-level risks and those that directly impact financial reporting. Audit committees should help ensure that management's risk assessment processes and disclosures are robust and the company's disclosures adequately communicate the risks and uncertainties the company faces.
- **Audit committees play a crucial role.** Staff from the SEC Office of the Chief Accountant encouraged audit committees to engage directly with the independent auditor (formally and informally)—instead of through management—to promote and encourage the auditor's exercise of professional skepticism, particularly in the areas of risk assessment and cybersecurity.
- **New segment reporting ASU raises questions.** Weighing in on the FASB's new segment reporting standard, SEC staff cautioned that additional measures of profit or loss disclosed in the financial statements may be non-GAAP measures to which SEC regulations apply.
- **Concerns about the cash flow statement.** SEC representatives delivered the message that not all companies have the same rigorous processes and controls around preparing the cash flow statement as other financial statements—and reinforced that classification errors in the statement should be evaluated like other financial statement errors.
- **GenAI is here and its pervasive.** GenAI promises amazing improvements in financial reporting speed, quality, and insights, but it comes with new demands on corporate governance, internal control and auditing techniques to ensure it is used responsibly.

The SEC staff also addressed frequently asked questions about its new rules on pay versus performance and compensation clawback and revisited familiar themes on topics such as non-GAAP financial measures and MD&A disclosures.

Also see *Top 10 Highlights: 2023 AICPA & CIMA Conference.*

ESG reporting update

In the absence of a final climate rule from the SEC, there are plenty of questions US companies should be asking about ESG reporting, including whether they are subject to the new California climate disclosure laws, have statutory reporting obligations outside the United States, or have EU operations.

Do you do business in California?

California Governor Newsom signed the following into law in October, which affect both public and private companies.

- Effective January 1, 2024, specified disclosures are required by business entities marketing or selling voluntary carbon offsets in California, and by entities purchasing or using voluntary carbon offsets that make claims regarding the achievement of net zero emissions or other similar claims.

- Beginning in 2026 (2025 data), US business entities with total annual revenues > $1B that do business in California must disclose Scope 1, 2, and 3 GHG emissions. Assurance over Scope 1 and 2 is required, with Scope 3 potentially being added later.
- Beginning no later than January 1, 2026, US companies with total annual revenues > $500M that do business in California must disclose their climate-related financial risks and measures taken to reduce or adapt to such risks.

Do you have statutory reporting obligations outside the US?

Individual jurisdictions are now deciding whether and how to incorporate the ISSB Standards into local requirements. Countries that have announced their support include Brazil, Japan, Canada, and the UK. The ISSB Standards require comprehensive sustainability reporting of risks and opportunities to primary stakeholders such as investors.

Do you have EU operations?

Many US and other non-EU based companies are in the scope of the CSRD—by virtue of having securities listed on an EU-regulated market or substantial activity in the EU. The related sustainability reporting under the ESRSs is effective for the first wave of companies starting from January 1, 2024. The ESRSs require comprehensive sustainability reporting of impacts, risks, and opportunities to a broad range of stakeholders based on both financial materiality and impact materiality (so-called double materiality).

For a discussion of these and other questions US companies should be asking about their ESG reporting obligations, see the KPMG BLC *On the 2024 agenda* publications.

Closing in on the Pillar Two tax rules

The Pillar Two, Global Anti-Base Erosion (GloBE) tax rules go into effect for many jurisdictions in January. These rules require complicated and data-intensive calculations of a new effective tax rate measure (the "GloBE ETR") for every single jurisdiction in which the company has operations. The GloBE ETR calculation is based on a unique hybrid of tax and financial accounting concepts, which will effectively require companies to create a third set of books. Therefore, Pillar Two is expected to have a significant impact on companies beyond their tax department, including disruption to finance and controllership, IT, and internal audit.

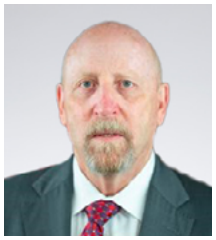
Calendar-year public companies will be required to report on the forecasted effects of Pillar Two in their Q1 2024 income tax provision and consider SEC disclosure obligations in their 2023 10-K. Therefore, it is critical that multinational companies have a gameplan to comply with these requirements including: (1) identifying which legal entities and jurisdictions will be impacted, (2) evaluating whether any of those jurisdictions will qualify for the transitional country-by-country safe harbor, and (3) determining if any top-up taxes will be owed based on forecasted results.

In addition, Pillar Two implementation will likely have an effect on the external audit process. The external auditor may ask about an implementation gameplan (including the three items mentioned above), internal controls, and data and technology, including whether any Pillar Two–specific models have been used or developed. Also expect the external auditor to perform independent procedures to test the information and amounts used to determine the impact to the financial statements.

For more detail about these and other financial reporting and auditing issues, see the Q4 2023 Quarterly Outlook and On the 2024 audit committee agenda.

Focus on independence, risk assessment, and cash flows, says SEC chief accountant

Jackie Daylor
Audit partner
KPMG LLP



Paul Munter
Chief accountant
US Securities and Exchange Commission

In December, Jackie Daylor, audit partner at KPMG LLP and a member of the Women Corporate Directors (WCD) Foundation board, interviewed Paul Munter, SEC chief accountant, for the WCD Audit Committee peer exchange series. They discussed Paul's views on audit committee expectations, oversight of risk management and the control environment, and audit committee and audit firm independence, among other issues. The following discussion highlights have been edited for length and clarity.

Paul Munter's comments below are provided in his official capacity as the Commission's Chief Accountant but do not necessarily reflect the views of the Commission, the Commissioners, or other members of the staff.

Jackie Daylor: The audit committee plays a critical role in the oversight of the audit. How do you frame the role of the audit committee from your vantage point as chief accountant?

Paul Munter: The SEC has a three-part mission—to protect investors, to facilitate capital formation, and to ensure fair, orderly, and efficient markets. If you go back to the Congressional hearings that led to the enactment of the Securities Act of '33 and the Securities Exchange Act of '34, high-quality financial reporting was an integral part of those proceedings. When considering financial reporting, it is not just important that financial statements are accurate, but that investors believe that those statements are accurate and complete. For this, high-quality audits are critical.

We only have to go back a couple of decades to several high-profile accounting frauds and audit failures. As a result, the Sarbanes–Oxley Act further empowered the audit committee as a primary gatekeeper to the financial reporting process and made its oversight of the external audit explicit. So, it is important that audit committees, collectively, and audit committee members, individually, take ownership of their responsibilities—that they're the ones engaging the auditor, determining the compensation of the auditor, and evaluating whether audit quality is at an appropriate level to serve the investors. It's also very important for the audit committee to transparently explain to investors how they are fulfilling their gatekeeper responsibilities and overseeing the external audit process.

JD: Last summer, you issued a statement on the importance of comprehensive risk assessment by management and the auditors. How should the audit committee think about its role in that process?

PM: In my view, audit committee members have an important role to play in terms of their oversight and understanding of management's process for risk assessment. The audit committee is looking to ensure that it is exercising oversight of the financial reporting process, the internal control structure, and that it understands how business risk management processes are integrated into financial reporting and internal control effectiveness assessments. That statement evolved from several conversations we had with issuers. We had seen a number of circumstances where the risk management process was viewed as separate and apart from the financial reporting process. But when you think about financial reporting—reflecting financial position, results of operations, and cash flows for the period—business risks that manifest

themselves in the company's operations will impact the financial statements now or at some point in the future. It also cascades to the auditor, which should start the audit by doing a robust risk assessment and identifying where within operations there is potential for material misstatements to the financial statements.

JD: Regarding internal and external factors impacting the control environment—from AI to cyber to geopolitical risk—what do you see as critical for audit committees to focus on as they carry out their oversight of controls over financial reporting?

PM: Audit committees need to understand that the control environment is not static, and risk assessment has to be a continuous activity. It is important to have that mindset. One of the things that is really dangerous is what I'll call a "SALY mentality"—"same as last year." The audit committee should be continually probing, engaging with management, and discussing with the external auditor ... what the risks are, specifically what is new or emerging. How might those risks impact the issuer and what processes is management using to identify and manage them? This requires a culture of continuous assessment. From a disclosure standpoint, those risks are often communicated first outside of the financial statements, in risk factors or management's discussion and analysis (MD&A). So, it's important for audit committees not only to engage, but also to think through what those risks mean for the financial reporting process. How can those risks be conveyed transparently and clearly to investors who are making their own capital allocation decisions and pricing risk?

JD: Investors spend a lot of time on income statements and balance sheets, but those of us who read your statement in December know that you have a view on the utility of the cash flow statement and how it could be improved. Could you share a little more on that?

PM: The cash flow statement is equally important to the other financial statements. I think the audit opinion underscores its importance: it says that the financial statements present fairly the financial position, results from operations, and cash flows for the period. Anecdotally, we've seen circumstances where issuers don't seem to have the same robust processes and controls around the preparation of the statement of cash flows as they do around the other financial statements. We've also seen instances where it doesn't receive the same amount of attention as the other financial statements from an audit perspective. If you look at sources of restatements over a number of years, statement of cash flow issues are consistently at or near the top of the list.

When we get engaged in discussions with issuers where an error in the cash flow statement has been identified—as to whether it is material and therefore warrants a big 'R' versus a little 'r'—we tend to hear comments like, "Well, it's quantitatively big, but there are all these qualitative factors as to why it's not material," starting with the fact that it's just about classification. But that's at the heart of the cash flow statement. Investors want to understand where an issuer is generating its cash from. The other part of the December statement focused on the utility of the direct method (vs. the indirect method) for conveying information about cash flows to investors. And, if companies don't feel that they can use the direct method, are there additional disclosures that they could make to help investors' understanding of cash flow information? This goes back to viewing financial reporting as more than just a compliance exercise, but also one of communication.

JD: Switching gears slightly, in the US, there are requirements for audit committee independence at public companies, clearly articulated in the exchange guidelines. Auditor independence is also mandated and just as important for the company and its stakeholders. How does the audit committee help to uphold these aspects of independence?

PM: The audit committee plays a critical role in how investors get information about the company. Its ability to exercise oversight of both the financial reporting process and the external audit would obviously be hindered if management or former management had a seat at the table. That transitions to auditor independence, which is a shared responsibility of the external auditor and the issuer. If the auditor is not independent, then the issuer has a problem because it now has a deficient filing.

It is very important for audit committees to understand the external auditor's process for maintaining its independence and whether that permeates throughout the firm's culture. In terms of audit and assurance, it is the firm that is required to be independent—not just the audit practice. So having a culture of the highest level of professional conduct and a commitment to auditor independence and audit quality must be resident at the very top of an audit firm. Audit committee members would be well served by having conversations with the leader of their engagement team about the firm's culture of compliance and its commitment to independence and audit quality.

JD: Lastly, what are the concerns that keep you up at night that audit committees should have top of mind?

PM: This really gets back to the risk questions we've been talking about. First, are risks properly identified? Second, does the company have a process in place to properly manage those risks? Third, is the company communicating those risks to investors?

In the current environment, relatively high inflation triggered action by central bankers around the world to increase interest rates. That resulted in exchange rate volatility and shifts in commodity prices and other uncertainties throughout the supply chain. One of the things I worry about is that those who are responsible for identifying and managing risk and, from an audit perspective, risk assessment over those processes, may not have previously managed their way through an environment of high interest rates or inflation. From an audit committee perspective, I would want to understand not only the processes, but also the skills of the people who are doing that and what kinds of steps the issuer has taken to make sure that those responsible for risk assessment and risk management have the appropriate skills. I would also engage the audit team about what it is doing to make sure that it too has the skills to make an appropriate risk assessment and execute an effective audit in light of those risks and uncertainties.

JD: On behalf of KPMG and WCD, I want to thank you for your time and your insights.

Board oversight of third-party risk management

by John H. Rodi and Greg Matthews

In recent years, as a result of reputational harm caused by the failure of third parties to deliver goods and services in line with expectations, management has had to sharpen its focus on third-party risk management (TPRM) programs. These third parties—including vendors, suppliers, cloud service providers, consultants, sales and distribution channels, and partners, as well as fourth, fifth, and nth parties—pose the same complex and evolving array of risks the company faces.

In a KPMG survey on TPRM, three-quarters of respondents said their company experienced a major business disruption because of a third party in the prior three years, and that business disruptions caused by third parties have exposed their companies to reputational risks. As many companies are increasingly seeing firsthand, cybersecurity and data privacy, geopolitical risk, compliance, climate and other environmental and social risks, and business continuity issues can quickly impact business operations and the brand.

While many companies have robust TPRM programs in place as a strategic imperative today, ensuring that TPRM programs keep pace with the rapidly changing risk, regulatory, and compliance environment is a significant challenge. As boards oversee management's efforts to maintain effective TPRM programs, key areas of focus should include the following:

Third-party cybersecurity and data privacy risks

According to the KPMG third-party cybersecurity and data privacy risks rank among the top third-party risks today, and the level of risk is increasing given the growing sophistication of hackers, including their use of generative AI. As noted in a recent World Economic Forum report,[1] a key challenge for companies is to maintain continuous monitoring and real-time visibility to identify potential third-party cybersecurity risks and issues. That requires leveraging automation, aligning the company's and third-party's internal and external control assessments, and understanding how management is improving its monitoring of third-party cybersecurity threats on a real-time basis.

Given the importance of cybersecurity risks, the SEC's recent cybersecurity disclosure rules require greater disclosure in this area, including whether the company "has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider." The final rules do not exempt companies from providing disclosures regarding cybersecurity incidents on third-party systems they use. However, as stated in the SEC's adopting release, companies are not required to conduct additional inquiries outside of their regular channels of communication with third-party providers and in accordance with the company's disclosure controls and procedures.[2] Nonetheless, boards will want to confirm that management has effective communication plans in place with third-party service providers to enable timely assessment and disclosure of material cybersecurity incidents.

Cybersecurity also poses compliance risks if third parties have access to personal data. Many countries have already enacted privacy and personal data protection laws and regulations, and more are in the process of drafting legislation. Companies should be monitoring global legal and regulatory data privacy developments. If third parties have access to personal data, then the company needs to ensure these parties have controls in place to manage that data in accordance with the laws and regulations as well as the company's data privacy policies.

[1] Global Cybersecurity Outlook 2023, World Economic Forum, January 2023.

[2] US Securities and Exchange Commission Final Rule, "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," July 26, 2023.

Risks posed by use of third-party AI tools

Companies are quickly recognizing the need to address the growing risks associated with their use or integration of third-party AI tools. As discussed in an April 2023 MIT Sloan Management Review article, "Third-party AI tools, including open-source models, vendor platforms, and commercial APIs [application programming interface], have become an essential part of virtually every organization's AI strategy in one form or another, so much so that it is often difficult to disentangle the internal components from the external ones."[3]

As a result, companies need to reassess their AI governance structure and processes regarding the development, use, and protection of AI systems and models, how and when an AI system or model—including the use of third-party generative AI tools—is to be developed and deployed, and who makes these decisions. What regulatory compliance and reputational risks—including biases—are posed by the company's use of third-party generative AI tools? How is management mitigating these risks? (Also see *Assessing the risks and opportunities of generative AI*.)

Third-party climate, sustainability, and other ESG risks

Stakeholder demands for higher-quality climate and other ESG disclosures should be prompting boards to sharpen their focus on the company's efforts to manage a broad range of climate and sustainability risks in the supply chain. As part of the effort, boards should closely monitor SEC, state, and global regulatory developments in these areas and management's plans to comply with new disclosure mandates. Key areas include mandated disclosures regarding the impact of climate change on the supply chain; the disclosure of Scope 3 GHG emissions data; and disclosures regarding a range of sustainability and "S" risks in the supply chain, such as human rights and forced labor.

Even as they await the SEC's final climate disclosure rules, companies doing business abroad will also want monitor and maintain compliance with other climate and sustainability regimes, including the ISSB's global sustainability disclosure standards and the European Union's ESRSs.Collection and calculation of Scope 3 GHG emissions data will pose a significant challenge for many companies, given the number of third parties in the supply chain and the fact that the emissions data reside outside of the company's control. Companies need to plan now as to how they will collect and calculate quality Scope 3 emissions data.

Management's projects to address business operations vulnerabilities and improve resilience and sustainability

For the past several years, companies have been navigating unprecedented business operational stresses and strains, with failures often glaringly public. Many are undertaking major initiatives to "de-risk" the supply chain—i.e., to understand the role third parties play in the delivery of goods and services, to identify and address vulnerabilities on these dependencies, and to improve resilience and sustainability by taking a risk-based approach. The projects vary by company and may include updating business continuity and disaster recovery plans, diversifying the supplier base, re-examining supply chain structure and footprint, reducing dependency on China and developing more local and regional supply chains, deploying technology to improve business operations visibility and risk management, improving cybersecurity to reduce the risk of data breaches, and developing plans to address future disruptions.

In the near term, the board will want to help ensure that significant projects being undertaken by management to rethink, rework, or restore critical business operations are carried out effectively. Importantly, given the complexity of business operations, it is critical that the company maintain an overarching vision and strategy to manage the supply chain in the context of the company's broader business operations risks. Focused leadership, connecting critical dots, and clear accountability are essential.

Core questions for the board

As the issues and elements highlighted above suggest, the increasing complexity and range of third-party risks poses a significant oversight challenge for boards. Investors, regulators, ESG rating firms, and other stakeholders are demanding higher-quality disclosures about third-party risks and how boards and their committees are overseeing the management of these risks. In this challenging environment, many boards are reassessing how, through their committee structure, they can effectively oversee third-party risk.

[3] Elizabeth M. Renieris et al., "Responsible AI at Risk: Understanding and Overcoming the Risks of Third-Party AI," MIT Sloan Management Review, April 20, 2023.

Among the core questions for boards and board committees to keep in mind:

- Do the management team members responsible for specific risks understand the scope and magnitude of the risk being managed by third parties and whether that risk is appropriately managed and controlled in line with the company's policies?
- Does management have a complete risk-ranked inventory of critical services provided by third parties, including subcontractors?
- How often does the board want updates on third-party risk from management? How is the information provided? Is data available in real time?
- Where should board oversight of third-party risk be housed—full board, risk committee, or another committee? Does the audit committee have responsibility for supply chain risks by design or by default?
- Is the TPRM program approached holistically, as an enterprise-wide activity (versus silo-driven) and effectively integrated with risk management and compliance functions?
- Do the TPRM team and other functions have sufficient skills/talent, funding, and technology to keep pace?
- When should the board be involved in the oversight and approval of large or complex services involving third parties?

John H. Rodi
Partner, Audit, KPMG LLP
Leader, KPMG Board Leadership Center

Greg Matthews
Partner, Advisory, KPMG LLP

Mark your calendar

BLC Quarterly Webcast

January 25, 11:00 a.m. EST

Join us for the first KPMG BLC quarterly webcast of 2024 as our KPMG Board Leadership team discusses the critical challenges and priorities driving board and committee agendas in the year ahead.

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

Corporate Directors Forum Summit 2024

February 15–16, San Diego, CA

Corporate Directors Forum hosts its 2024 Directors Summit. Gain insights on the future of modern leadership, navigating disruptive technology, addressing activism inside and outside the boardroom, and the state of the global economy.

To register, visit conference.directorsforum.com

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

Risk oversight: Reassessing board and committee structure
KPMG BLC

Audit committee transparency barometer
The Center for Audit Quality

Geopolitical hotspots on the board agenda: A discussion with Eurasia Group *KPMG LLP*

Evolving human capital disclosures
Gibson Dunn

AI in the financial reporting function
KPMG LLP

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: 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.

The views and opinions expressed herein are those of the interviewee and do not necessarily represent the views and opinions of KPMG LLP.

kpmg.com/socialmedia