EY Center for Board Matters

2024 Q3 audit committee update

EY Building a better working world

PRESENTED BY THE EY AUDIT COMMITTEE FORUM

This quarterly audit committee update provides a summary of key developments related to risk management, financial reporting, and regulatory developments. For Q3 2024, audit committees are focused on shifting macroeconomic trends along with geopolitical developments and related challenges. Many audit committees are considering how the US election outcome, recent and further interest rate cuts by the Fed and the outlook for potential recessionary risks could impact their business and strategies.

The recent disruptions from the global IT outage in July highlighted the pressing need for developing and stress-testing robust business continuity plans and building resiliency capabilities. We expect that audit committees will spend time discussing these matters and revisiting reliance on critical third parties and suppliers.

Meanwhile, audit committees are also closely monitoring Securities and Exchange Commission (SEC) activity and other regulatory developments. While there have been no developments relating to the litigation against the SEC's climate disclosure rules, audit committees are keeping an eye on those proceedings as well as on how companies will eventually comply with other new and emerging reporting requirements.

Risk management

Given the ongoing changes in the business environment, it remains essential for audit committees to stay focused on critical drivers of risk (e.g., political, economic, societal, technological, legal and environmental) to better assess the near- and longer-term risk implications.

Organizations have been acting cautiously this year, with many either selectively slowing down hiring and investment initiatives or freezing them altogether. This is primarily in response to the current economic, policy and geopolitical environment, in which inflation seems to be moderating but cost fatigue persists.

Key risks to watch this quarter include:

- Recent elections for European Parliament, Germany, France and the UK confirmed the surge of far-right populism has not gone away in Europe, increasing political fragmentation and policy uncertainty with various implications for businesses. Major sectors that may be affected by policy implications include government, financial services, energy, technology and life sciences.
- With the war in Ukraine seemingly unlikely to end soon, global companies should continue to monitor their exposure to evolving sanctions against Russia, which may expand in scope and geography to include third countries perceived to be supporting Russia's defense industry, possibly including China.
- Additionally, the ongoing unrest in the Middle East is posing challenges for the regional business environment. The conflict could result in impacts such as talent shortages, increased costs and reduced productivity for regional businesses. Companies dependent on regional production sites, suppliers or energy sources should revisit supplier resiliency or inventory management strategies.
- There continues to be elevated financial market volatility and softer economic data. While labor market conditions have visibly cooled, economic momentum appears positive. Households are being cautious as the labor market conditions and income growth soften. While businesses are being more judicious with their hiring and investment decisions in a high-interest-rate environment, some are offering discounts and incentives to draw more price-discriminating customers.
- With capital markets recalibrating to the realities of increased capital costs, activist investors are seizing the opportunity to question management's past capital allocation choices, particularly mergers and acquisitions (M&A) perceived as detrimental to shareholder value. This scrutiny is likely to continue as companies navigate a demanding economic landscape. In anticipation of potential critiques, numerous companies are taking the initiative to remedy business underperformance by shedding underperforming businesses. When overseeing strategic portfolio reviews and capital allocation discussions, boards and audit committees may want to press management on how the company is evaluating underperforming business units, non-strategic assets or business units that are not deserving of additional capital.
- One of the most important macro policy developments after the US elections will be around trade. Key global macro risks exist in the escalation of global trade tensions.
- As the US election draws near, the outlook for tax, trade and regulatory policy should be monitored closely.

Audit committees should consider discussing with management how these risks may impact financial reporting and related controls and disclosures. Additional conversations around scenario planning and risk mitigation plans may be prudent along with stress-testing assumptions surrounding these key risks.

In the spotlight

Spotlight on cybersecurity risks

Cybersecurity remains a top board and audit committee priority. The threat landscape continues to grow at an exponential rate globally with disruptive technologies such as generative AI, Internet of Things (IoT), 5G networks, and quantum computing, adding to an environment shaped by complex supply chains, greater scrutiny from stakeholders and evolving regulatory expectations.

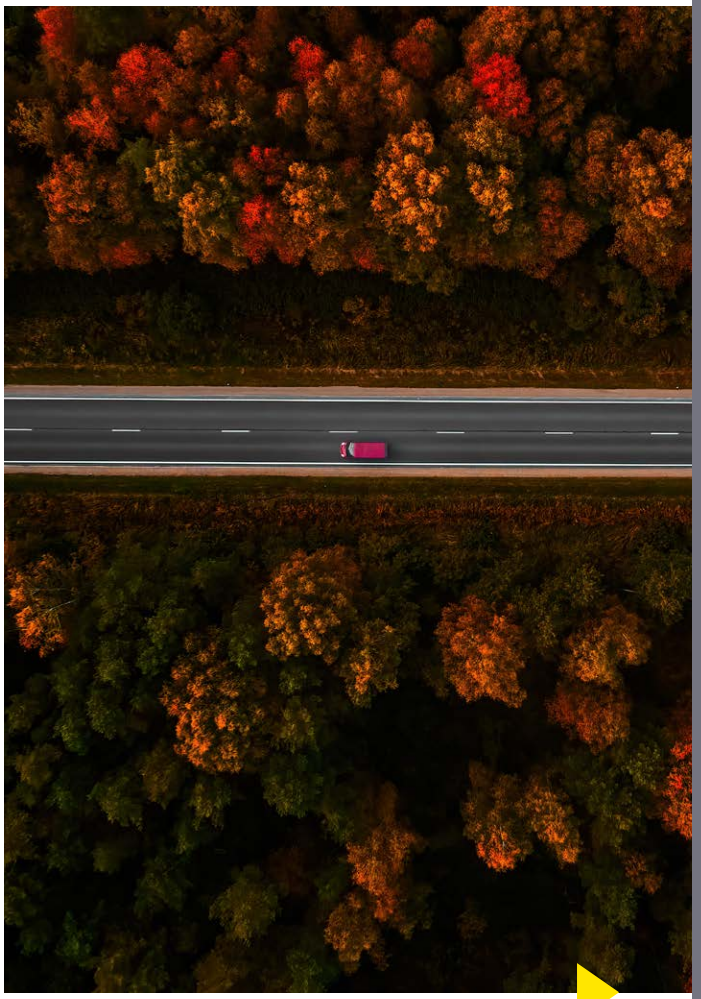
Tapestry Networks this spring convened audit committee chairs of large, multinational public companies to exchange views on the current threat landscape and the ways that cybersecurity practices are adapting. Tapestry's publication *Cybersecurity and data privacy: a dialogue with chief information security officers and data privacy leaders* explores some of the cyber and privacy challenges faced by companies along with ways to enhance oversight.

Following is a summary of key takeaways from that publication as well as themes we're hearing from audit committees[1]:

- **Assess impacts to the company's cyber risk profile from advanced technologies, tactics, and an exponential increase in attack surfaces.** Cyber adversaries are using advanced technologies, such as AI in phishing schemes, to amplify the sophistication and efficiency of attacks. More bad actors are also using identity theft tactics and other intrusion techniques that make it difficult to differentiate between normal activity and a breach — a concerning trend highlighted in the *CrowdStrike 2024 Global Threat Report*. Boards and audit committees should assess how companies are mitigating risks and how the company's risk mitigation efforts are evolving in light of the changing risk landscape.
- **Evaluate how geopolitical tensions and developments may amplify risks.** Active warfare in Ukraine and other areas heighten risks on top of existing tensions with China, North Korea and Iran.
- **Enhance the rigor of supply chain and third-party risk management.** Many companies find themselves increasingly reliant on third-party vendors, which brings additional risks. Audit committee chairs and chief information security officers (CISOs) note the proliferation of third-party vendors is one of their biggest challenges, especially since the vendors themselves face intensifying cyber threats but may have fewer resources to defend against them than their customers operating globally. Accordingly, leading companies are re-evaluating and simplifying the cyber technology stack (e.g., potentially reducing the number of vendors as low as possible) while helping partners strengthen their own security. Approaches to third-party risk management have evolved in the past few years — with some companies now completing pre-emptive assessments of potential breaches before vendor approval. Additionally, utilizing standardization and automation to reduce supply chain entry points that hackers could exploit has been an area of focus to improve cyber vigilance and continuously monitor performance without adding undue bureaucracy.

[1] Adapted from "Cybersecurity and data privacy: a dialogue with chief information security officers and data privacy leaders," Tapestry Networks Audit Committee Leadership Network, April 2024.

- **Be wary of evolving data privacy regulations and increased enforcement.** Global companies face heightened data privacy risks due to stricter regulations and a greater focus on enforcement worldwide. When it became effective in 2018, the European Union's General Data Protection Regulation (GDPR) was often cited as a global standard for privacy programs: A company that complied with the GDPR was likely to be compliant with other regimes. However, the regulatory environment is evolving, particularly in the Asia-Pacific region, where countries are enacting more rigorous privacy laws on consent management and data localization. Some companies are also seeing more enforcement by regulators in the region. Global companies should be continuously evaluating their privacy program given these emerging regulations and the enhanced enforcement posture.
- **Revisit privacy policies.** Privacy regulation is becoming stricter in key jurisdictions, and global companies may need to reassess their policies around and approaches to compliance. A changing regulatory landscape may even drive companies to consider where they are doing business. Some companies are evaluating whether to continue to operate in certain countries, balancing factors such as unintended consequences or risks arising from providing sensitive information to foreign regulators about the company's information security network. Accordingly, audit committees may consider inquiring about regulatory expectations and compliance where the company has employees, operations, or data-processing activities in certain regions.
- **Enhance employee awareness and training to make the workforce more cyber-secure.** Audit committee chairs and CISOs are also re-evaluating approaches to employee training and awareness around cybersecurity and seeking ways to enhance the organization's culture around cybersecurity. Leading companies are making cybersecurity-related training accessible on devices such as smartphones, engaging younger employees through internal social media and incorporating gamification with a heightened focus around phishing and deepfakes.
- **Continue to have open dialogue with the CISO about ways to refine management's reporting of cybersecurity-related matters.** Audit committee chairs have varied views on the effectiveness of current management reporting on cybersecurity, whether it be through dashboards or other mechanisms. Audit committees should consider providing feedback on ways the CISO is being more intentional and purposeful on selected metrics. There is also a growing focus on the company's cybersecurity journey: how it has grown, how capabilities have improved, what the threat landscape looks like and how the company has either risen to the challenge or identified areas for further improvement.



Key lessons learned from the recent global technology outage

On July 19, an IT provider released a routine software update containing a flaw that affected approximately 8.5 million Windows devices and 674,620 subscribers in 1,200 unique industries.

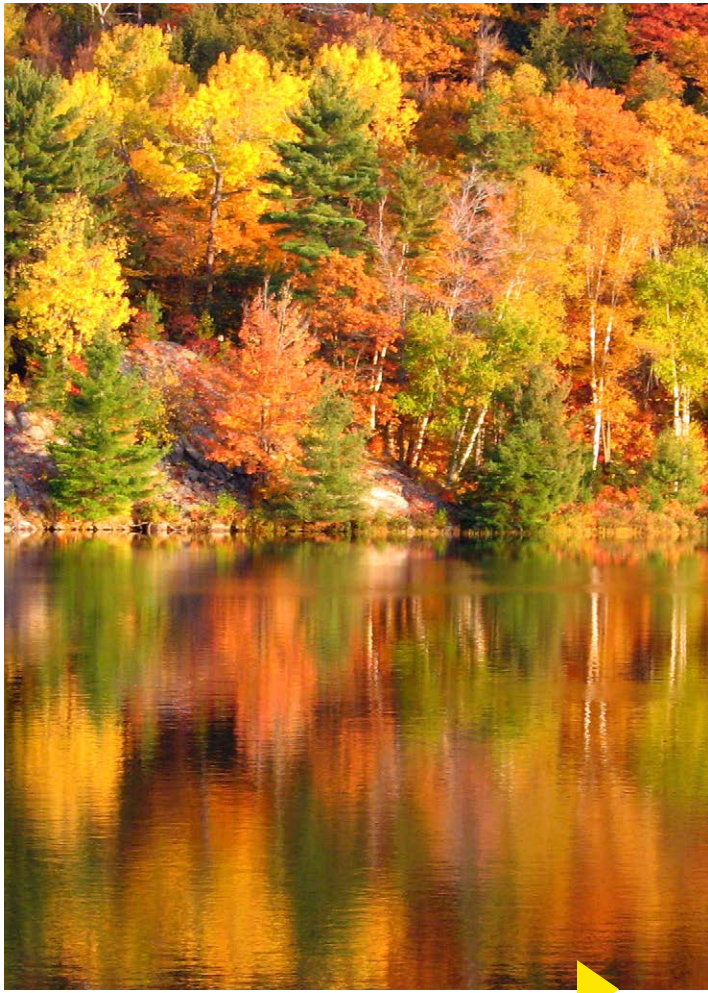
As organizations around the world continue to recover from what some have described as the biggest IT outage in history, the event illustrates the importance of developing IT resiliency strategies and robust business continuity planning. While it was not a cybersecurity incident, the disruptions bore resemblance to those caused by cyber attacks requiring the use of complex non-typical disaster recovery processes and well-coordinated communication across multiple teams. Key actions for audit committees to consider:

- **Reassess concentration risk.** This global IT outage exposed a few critical risks — in particular, the significant element of concentration risk at play. A vast majority of the world's IT systems run on a handful of provider platforms. Should any of them experience an outage, the results could extend beyond mere inconvenience and possibly compromise public health and safety. Audit committees and boards should acknowledge possibility of technology failures and understand management's plans to preserve function and provide services to customers in these scenarios.
- **Evaluate quality control mechanisms.** The outage has shone a spotlight on quality control in software updates, drawing attention to the urgent need for more rigorous scrutiny during the testing phase before deployment. It raises the question of whether there is a need for fundamental changes to the operations of essential technology service providers. Audit committees may want to inquire with CISOs as to whether: 1) new quality assurance protocols should be implemented to govern the rollout of updates and new software releases, and 2) patches should be risk rated to ultimately drive a decision on auto accept vs. manual intervention.

- **Continue to build resiliency.** The introduction of EU regulatory frameworks such as the NIS2 directive and the Digital Operational Resilience Act (DORA) make IT resilience and business continuity plans even more important. Among other things, these frameworks mandate that essential and important entities implement risk management measures including advanced threat detection and continuous monitoring. There are also requirements around the regular testing and updating of these measures to ensure effectiveness. Audit committees and boards should continue to challenge management teams to update risk management practices to strengthen resiliency capabilities.

Overall, this global outage highlights the importance of cultivating a culture of resilience that spans the key disciplines of business continuity, disaster recovery, cybersecurity, technology and crisis management. As organizations seek ways to bolster recovery abilities, key action steps include:

- Know business continuity plans and test them regularly.
- Know resilience gaps and identify corresponding workarounds.
- Know third- and fourth-party technology ecosystems.
- Know recovery strategies and establish a clear tiering system.
- Know the limits of key partners on which the business relies on (e.g., vendors, third parties, supply chain/ suppliers) through consistent testing.



> “Audit committees and boards should continue to challenge management teams to update risk management practices to strengthen resiliency capabilities.

Accounting and disclosures

Audit committees will continue to evaluate evolving impacts of the uncertain economic environment and other shifts in the business landscape on their financial reporting processes.

Below is a summary of some of the latest developments in financial reporting:

Disclosure considerations on segment reporting

- The SEC staff said that it will focus closely on segment reporting, including compliance with the additional disclosure requirements in Accounting Standards Update (ASU) 2023-07, in its review of 2024 annual financial statements.
- The FASB issued ASU 2023-07 amending the guidance in Accounting Standards Codification (ASC) 280, Segment Reporting, to require a public entity to disclose significant segment expenses and other segment items on an annual and interim basis and provide in interim periods all currently required annual disclosures about a reportable segment's profit or loss and assets. Public entities with a single reportable segment are required to provide the new disclosures and the disclosures currently required under ASC 280.
- Another aspect of ASU 2023-07 is that it allows public companies to disclose more than one measure of segment profit or loss, provided that such measures are used by the chief operating decision-maker (CODM) to assess performance and allocate resources. Under ASC 280, the segment profitability measure that is most consistent with US GAAP is required to be reported. All other segment measures used by the CODM represent additional measures of segment profitability.
- The SEC staff said in response to the FASB's issuance of the guidance that additional segment profitability measures a public entity chooses to disclose that are not determined in accordance with US GAAP would be considered non-GAAP financial measures because ASC 280 does not (1) require their disclosure or (2) expressly permit their disclosure by prescribing or otherwise specifying the additional measures that may be disclosed.

> "As companies prepare to adopt the FASB's new guidance on segment reporting, it will be important that management consider all sources of information.

- Although Item 10(e) of Regulation S-K prohibits the inclusion of non-GAAP measures on the face of the financial statements or in the accompanying footnotes, based on recent discussions with the SEC staff, we understand that they will not object to the disclosure of additional non-US GAAP segment profitability measures in the footnotes if it otherwise complies with Regulation G, Item 10(e) of Regulation S-K and the related SEC staff's compliance and disclosure interpretations (C&DIs), including the requirement that the non-GAAP measure not be misleading. We encourage companies to carefully consider this staff guidance, and engage with their legal counsel and independent auditors, when considering disclosure of additional non-GAAP segment measures of profit or loss in the financial statements.
- The FASB's guidance is effective for all public entities for fiscal years beginning after 15 December 2023 and interim periods beginning after 15 December 2024 and should be applied retrospectively to all periods presented in financial statements.

Texas federal judge blocks Federal Trade Commission (FTC) rule on noncompete arrangements

- A federal judge in Texas recently blocked the FTC rule generally prohibiting employers from enforcing the terms of previous noncompete arrangements made with workers. The rule, which was supposed to take effect on September 4, 2024, also would prohibit employers from entering certain new noncompete arrangements. The FTC said it is weighing an appeal, and companies should continue to monitor developments.
- The rule would have broad accounting and financial reporting implications for companies in industries regulated by the FTC. Companies that have recognized on their balance sheet a finite-lived intangible asset related to noncompete arrangements that would be affected by the rule would need to consider the impact on the subsequent accounting of the asset. Companies would also need to evaluate the remaining useful life of the asset each reporting period and review the asset for impairment in accordance with ASC 360-10, *Property, Plant, and Equipment – Overall*, when events or changes in circumstances indicate that its carrying amount may not be recoverable.

SEC rulemaking and other regulatory considerations

The pace of rulemaking by the SEC has slowed in recent months.The government agency slowdown typically expected ahead of a presidential election may be compounded by recent legal developments, including the recent Supreme Court decision in Loper Bright v. Raimondo, which overturned the decades-long "Chevron" deference of courts (under Chevron USA, Inc. v. Nat. Res. Def. Council) to the reasonable interpretation of statutes by agencies.Among other impacts, the decision may open the door to increased court challenges asserting regulatory overreach and have a chilling effect on regulatory agendas, as agencies reconsider their authority in light of the ruling, especially where there is not clearly stated legislative authority to act. Observers have suggested that SEC rulemaking relating to climate-related disclosures, digital assets and AI could be at risk due to the decision. Meanwhile, litigation relating to the SEC climate disclosure rule remains pending and the timing for a decision remains unclear.

Additionally, the SEC staff published C&DIs relating to the materiality assessment and disclosure of cybersecurity incidents involving ransomware attacks. Among other things, the C&DIs emphasized that the materiality of a cybersecurity incident cannot be determined based on a singular factor (e.g., whether a ransomware payment was made, the size of a ransomware payment).

PCAOB developments

The SEC approved the amended standard issued by the Public Company Accounting Oversight Board (PCAOB) related to the use of technology assisted analysis in conducting an audit and the ethics rule governing the liability of an associated person. It also approved the PCAOB's new auditing standard, AS 1000, *General Responsibilities of the Auditor in Conducting an Audit*, and related amendments to "modernize, clarify, and streamline" concepts of auditing. Audit committees may want to inquire with their audit engagement team as to whether there would be impacts on the company's audit arising from these standards.

Last quarter, the PCAOB issued a spotlight report on topics that its staff discussed with audit committee (AC) chairs. Overall, the report indicated that AC chairs were satisfied with their communications with their auditor on a range of topics, including economic and geopolitical risks, interest rates, inflation and critical audit matters (CAMs). Separately, recent PCAOB board member remarks have raised concerns about low numbers of CAMs being reported. The PCAOB has indicated that CAMs will be a priority in 2024 inspections of audit firms.

Another PCAOB staff report discusses how auditors report they are using technology and AI in audit procedures to enhance audit quality. The recent PCAOB GenAI spotlight report on discussions with major US audit firms indicates they are applying generative AI (GenAI) to administrative (memos and presentations) and research (internal accounting and auditing guidance) activities in audit procedures. As the adoption of GenAI increases, including its integration into financial reporting processes and auditing, audit committees should consider assessing how their related oversight practices may need to evolve to keep pace.

Additional resources:

- SEC in Focus, July 2024
- 2024 proxy season review: Five takeaways, July 2024
- How boards can embrace and oversee AI with curiosity and care, July 2024

Questions for the audit committee to consider

In discussions with management, compliance personnel and internal and external auditors, audit committees should consider the following in addition to standard inquiries:

Risk management-related inquiries:

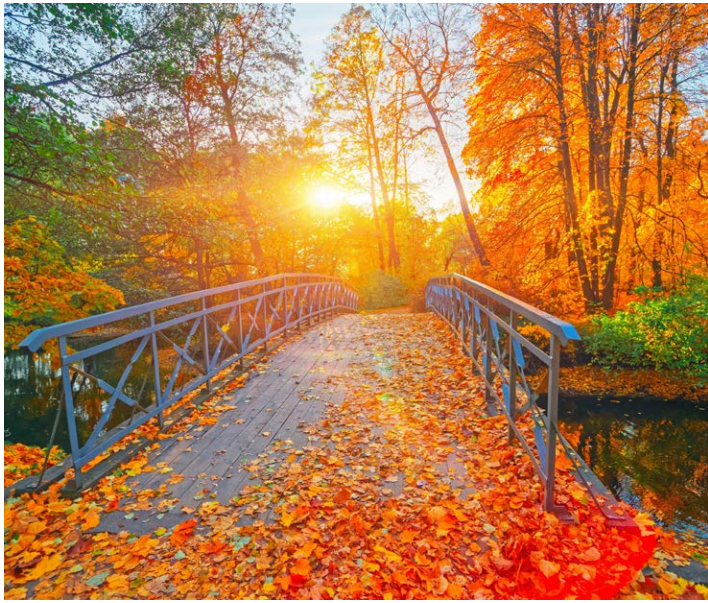
- How strong are the organization's capabilities to be highly informed about the internal and external environment, and risks, events and opportunities that may influence or compromise enterprise resilience?
- How effective is the board's oversight of emerging risks and other evolving external risks such as geopolitical developments, uncertain economic conditions and climate risk? Does it have the information, expertise and professional skepticism it needs to challenge management in these areas?
- Does the organization perform stress tests to confirm that its financial reserves can absorb distress in the economy? Does the organization have confidence in the financial strength of its counterparties?
- Does the organization deploy future scenario planning to inform its long-term planning process to enable rapid adaptation during changing circumstances?
- Who (individual or group) in the company is responsible for oversight of the use of GenAI? Has management developed a framework for responsible use of GenAI? Has management established policies regarding the acceptable and ethical use of GenAI?
- How does the company track and monitor GenAI usage, including through third-party service providers, and assess its impact on various groups?
- What laws, regulations and contractual agreements affect the company's use of GenAI and how does the company ensure compliance? How does the company assess and monitor compliance, especially concerning potential biases in GenAI technologies that could lead to noncompliance?
- Has the company identified specialized skills or knowledge needed to assist with oversight, development, deployment, operation and monitoring of GenAI technologies?
- How has management considered GenAI technologies in its fraud risk assessment? Has the company identified new incentives, opportunities or pressures to commit fraud it ties to the deployment of GenAI technologies?
- How does management consider data privacy risks when selecting or developing GenAI technologies? Does the company use a public instance of GenAI technologies that tracks and saves inputs and data that are accessible by third parties or a private instance where inputs and data are tracked and saved only by the company?
- How does the company consider cybersecurity risks when selecting or developing GenAI technologies? Has the company performed a cybersecurity risk assessment to evaluate threats and safeguards?
- How does the company monitor the ongoing effectiveness of GenAI technologies for their intended purpose? How does the company monitor changes to GenAI technologies? How does the company determine the appropriate level of human-in-the-loop involvement with GenAI technologies? How does the company consider the explainability and interpretability needs of users to enable effective human-in-the-loop involvement with the GenAI technology?

“How does the company track and monitor GenAI usage, including third-party service providers?

- Does the organization have a clear and comprehensive understanding of the relationships and interdependencies between the company's critical business services, third parties including suppliers, business processes and supporting technology?
- How aligned is the company in meeting its recovery time objective (RTO) and does it have alternative business strategies to manage any gaps in the RTO?
- Is there an appropriate level of robustness and redundancy provided for critical third parties to reduce service disruption(s)?
- How does management evaluate and categorize identified cyber and data privacy incidents and determine which ones to escalate to the board?
- Has the board participated with management in one of its cyber breach simulations in the last year? How rigorous was the testing? What changes were implemented by the organization as a result?
- Has the company leveraged a third-party assessment to validate that its cyber risk management program is meeting its objectives? If so, is the board having direct dialogue with the third party related to the scope of work and findings?
- As a result of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 adding a new govern function, how have the organization's risk management strategy, expectations and policies evolved?
- What actions has management taken to ensure that the company's cybersecurity policies, procedures, risk assessment and practices align to NIST CSF 2.0?
- Has management performed a gap analysis of its cybersecurity program against the new NIST CSF 2.0 and communicated the results and remediation items to the board?
- Given NIST CSF 2.0's emphasis on utilizing a risk-based approach, how has this impacted the company's cybersecurity risk assessment process, appetite and risk posture?
- Is the organization equipped to respond to any crisis scenario and operate/deliver services at the minimum acceptable levels? Does the organization test/flex its resilience against a range of operational and strategic scenarios?
- Should management perform more real-time tabletop exercises to help build the muscle memory to respond to gray swan events? More importantly, should the organization incorporate more live testing vs. relying on traditional tabletop?
- How has the company identified environmental and social factors that are material to the business? Has it conducted a recent sustainability materiality assessment and disclosed the results?
- How has the company integrated material environmental, social and governance (ESG) factors into strategy development and enterprise risk management? Do company communications successfully tie those ESG factors to strategic and financial results?
- Have there been any meaningful changes to the company's key policies, any material exceptions granted or any unusual allowances to any compliance provisions?

Accounting, disclosures and other financial reporting-related inquiries:

- Are there any nonrecurring events and/or circumstances that have transpired in the past quarter? If so, what are the related financial reporting and disclosure implications?
- Are the company's nonfinancial disclosures fit for purpose given current investor stewardship priorities, investing trends and related investor data needs?
- Does the company have robust internal controls and procedures in place to identify cybersecurity risks and incidents promptly and communicate them to the parties responsible for oversight and disclosure? How does the company assess the materiality of cybersecurity incidents and what is the protocol for determining when to disclose such incidents?
- Has the company continued to prepare to comply with the SEC climate-related disclosure rules?
- How is the organization proactively assessing the opportunity to enhance stakeholder communications, including corporate reporting to address changes in operations and strategies as well as changing stakeholder expectations?
- How is management progressing with its analysis of the impact of the OECD Pillar 2 global minimum tax model? In particular, what impact do the rules have on the estimated annual effective tax rate (ETR) for 2024 and is management monitoring proposed tax legislation for potential impact on the projected ETR in those countries that have yet to adopt the Pillar 2 rules?
- How is the company progressing in its systems and control enhancements required to calculate the Pillar 2 impacts, including analyzing the safe harbor rules and producing separate entity financial statements for the calculations. Is management planning any internal restructuring transactions to mitigate the increased worldwide taxes that may be occurring as a result of the Pillar 2 impacts on the entire group?
- Has management analyzed the impact that the Pillar 1 tax regime may have on its intercompany transfer pricing policies, and will it be an early adopter of the OECD transfer pricing regime inherent in Pillar 1?
- Does management have the resources within the tax function to keep pace with, and evaluate quarterly the impacts to the company of, the OECD global minimum tax and new environmental/carbon taxes being legislated globally?
- Have there been any material changes to internal controls over financial reporting or disclosure controls and procedures to address the changing operating environment?
- How is the company evaluating any initiatives (e.g., cost-saving initiatives) that may impact resources and/or processes that are important to internal controls over financial reporting or disclosure controls and procedures?



> "Is the company continuing to prepare to comply with the SEC climate-related disclosure rules?

Inquiries to auditors:

- External auditors:
  - Does the engagement team expect significant changes in hours or staffing mix from previous audits? Why or why not?
  - Did the engagement team notice any red flags arising from management responses? How has the engagement team considered changes to the incentive, opportunity and rationalization of the fraud triangle?
  - What plans does the auditor have to assess the company's accounting for Pillar 2 taxes and testing relevant internal controls this quarter?
  - What audit challenges does the team anticipate in relation to the newly adopted SEC climate rules or other applicable ESG-related reporting requirements (e.g., California climate laws, European Commission's European Sustainability Reporting Standards)?
- Internal auditors:
  - How should audit plans be adjusted to address the newly released NIST CSF 2.0 framework? What changes and implementation challenges are expected from the application of this updated framework?
  - If the company is subject to Pillar 2, what processes and controls will it need to capture the data necessary to calculate the taxes under the new regime? Has the company begun internal testing of those processes and controls?
  - What is the company's state of readiness to comply with the newly adopted SEC climate rules?
  - What action(s) is internal audit taking to align with the Global Internal Audit Standards? Has the organization conducted a gap assessment to understand the magnitude of change to conform with the standards?
  - What internal audit processes need to change or adjust due to the new standards?
  - Does internal audit currently have the resources and capabilities to conform with the new standards?
  - Is there a plan to upskill the internal audit function to understand the new standards and related impacts?
  - When will internal audit be ready to demonstrate conformance with the new standards?
  - What changes can the board expect to see during the implementation period?

RETURN HOME

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

About the EY Center for Board Matters
Effective corporate governance is an important element in building a better working world. The EY Center for Board Matters supports boards, committees and directors in their oversight role by providing content, insights and education to help them address complex boardroom issues. Using our professional competencies, relationships and proprietary corporate governance database, we are able to identify trends and emerging governance issues. This allows us to deliver timely and balanced insights, data-rich content, and practical tools and analysis for directors, institutional investors and other governance stakeholders.

US SCORE no. 24627-241US
CS no. 2408-84429-CS

ED None

ey.com/us/boardmatters

Looking for more?

Access additional information and thought leadership from the EY Center for Board Matters at ey.com/us/boardmatters.