AUDIT COMMITTEE PRIORITIES FOR 2023

Audit committees (ACs) continue to be charged with significant oversight responsibilities. As **directors enter 2023**, it is important to identify and communicate realistic priorities for the ACs and ensure they have adequate resources and experience to match the evolving roles and oversight of increasingly complex areas.

Evolving Oversight of Financial Reporting and the Audit

FINANCIAL REPORTING

Financial reporting continues to present challenges based on the dynamic macroeconomic environment — e.g., inflation, supply chain constraints, the war in Ukraine and COVID-19 — as well as emerging trends — e.g., use of digital assets, increased cybersecurity threats and climate change impacts. BDO's publication **2022 AICPA SEC & PCAOB Conference Highlights** provides insight into these matters and other accounting and reporting issues. The companion publication, **2022 SEC Reporting Insights**, may also be referenced for a more comprehensive discussion of SEC rulemaking, developments and related staff activities.

The AC will want to consider how management accounts for and discloses the individual impacts of inflation and rising interest rates, particularly on assumptions and judgments it makes about specific accounts and transactions. For example, a continued rise in interest rates may impact fair value measurements resulting in asset or goodwill impairments; while increasing inflation may negatively impact costs and demands for products and services which may affect, among other analyses, going concern, already a target topic of the **PCAOB's inspections of 2021 audits**. Additionally, ACs should exercise professional skepticism when reviewing managements' key assumptions and estimates and auditor conclusions as well as ensure transparent communication within the company's reporting and disclosures.

The SEC staff continues to **emphasize** the importance for disclosures that provide decision useful information to investors, including how changes and uncertainties may affect the predictive value of historical financial information. The SEC also reminds registrants to consider disclosures relative to valuation and qualifying accounts, which are likely to be affected by the current environment; in addition to seeking explanation of sensitivities in estimates and assumptions, revisions to prior assumptions, together with early warnings of potential impairments and updates on past predictions.

The use of digital assets, if applicable, is an emerging area of complexity and regulatory focus, likely requiring education and expertise. Specifically, the **SEC provides examples** in the areas of registered offerings of crypto assets, safeguarding of crypto assets and lending arrangements to illustrate the unique risks and complexities in this area. The SEC has recently expanded its Division of Enforcement's **Crypto Assets and Cyber Unit** to support investors in this area including a **sample comment letter** on disclosures regarding crypto asset market developments.

We continue to see comment letters from the SEC related to non-GAAP financial measures. The SEC staff recently released **updates** to the Compliance and Disclosure Interpretations (C&DIs) for non-GAAP financial information, aimed to clarify reporting considerations of potentially misleading non-GAAP measures.

As environmental, social and governance (ESG) risks and impact are becoming more material to the business, it ultimately falls to the Board to ensure that management is acting in the interest of a broader set of stakeholders with respect to the sustainability of the organization, which includes **overseeing ESG** reporting processes and related controls. ACs should further be actively considering the implications of SEC existing and anticipated ESG-related disclosure requirements, including **cybersecurity**, climate, compensation and human capital:

- Cybersecurity rules remain in the proposal stage, but registrants should refer to the previously published staff **interpretive release** and **guidance** when considering cybersecurity disclosures. Mike Stiglianese, a former Managing Director in BDO's Technology Advisory Services Practice, recently **discussed** the SEC's proposed rules on cybersecurity risk management, strategy, governance and incident disclosure and their related impacts and considerations.
- Climate-related disclosures have garnered increased SEC comments over the past year, especially following the release of the SEC staff's **sample comment letter** in late 2021. Registrants should also consider the **staff's guidance** on climate change released in 2010. BDO's Tim Kviz, National Managing Partner – SEC Services, recently **discussed** preparation for implementation of the SEC's **proposed rules** to standardize climate-related disclosures for public companies.
- Recent Dodd-Frank Act rule-making includes **pay vs performance** and **policies related to the recovery of erroneously awarded compensation** (aka clawbacks)
- Anticipated SEC rulemaking related to **human capital disclosures** is currently being considered to enhance publicly reported information and reduce the current **heterogenous nature** of such disclosures.

Accountability for disclosures is being shared among committees of the Board and collaboration is critical to ensure consistent messaging supported by oversight of controls, policies and procedures around the information shared publicly. ESG reporting, encompassing the above-mentioned cybersecurity, climate, compensation and human capital disclosures, is a prime example. The AC, along with the other committees of the Board, are reminded that oversight of disclosures should take into account the consistency of relevant information contained in public reporting beyond the financial statements — e.g., proxy statements, sustainability reports, webpages, marketing materials, etc.

THE AUDIT

The PCAOB **reminds** AC members of the importance of considering audit execution, auditor independence and the audit firm's quality control system in driving audit quality for the protection of investors. The PCAOB shares in the role of auditor oversight, therefore, the AC should remain abreast of the regulator's activity including:

- PCAOB's **2023 strategic plan**, which includes modernizing standards, enhancing inspections, strengthening enforcement and improving organizational effectiveness.
- 2021 **inspection results**, which identified a collective increase in the number of audits with deficiencies compared to the prior year with common deficiencies identified in auditing Internal Control over Financial Reporting (ICFR), revenue, estimates, inventory, equity and digital assets.
- PCAOB **standard-setting projects**, where the PCAOB is working actively to update more than 30 standards within 10 projects.
- Recently released PCAOB guidance, particularly, the proposed risk-based **quality control standard**, which would amend **AS 1301, Communications with Audit Committees**, to require the auditor to communicate to the AC about the firm's most recent evaluation of its quality control (QC) system.
- **PCAOB 2022 inspection cycle**, where the PCAOB staff has continued its focus on audit risk factors driven by the current economic and geopolitical environment, including financial statement areas that are complex, require significant **judgment**, and may be susceptible to change, for example, Fraud, Initial Public Offerings (**IPOs**) and Merger and Acquisition (**M&A**) activity among other auditor-centric topics.

Auditor communications with ACs are critical to auditor oversight and audit quality. This is an area where the PCAOB continues to find inspection deficiencies, specifically around;

- The auditor's use of other auditors,
- Critical accounting policies and practices used by the company, including reasons certain policies and practices are considered critical, and
- Written communications with management, including the representation letter.

These communications are designed to inform ACs in their oversight role and directors should remain aware of their value and make inquiries as necessary. Continual two-way dialogue regarding risks identified, audit procedures (including areas where common deficiencies are found), internal controls, Critical Audit Matters (CAMs) and audit firm QC systems will continue to enhance audit quality.

Risk Management Oversight

The AC is often charged with oversight of the company's enterprise risk management (ERM) function. The Dodd Frank Act federally mandates certain bank holding companies to establish a separate risk committee to execute this responsibility, but proxy data shows that only about 12% of S&P 500 companies have a separate risk committee. As discussed in our **2022 publication**, risk oversight remains a high priority for Boards, and risks identified as significant or impactful are often further assigned to other committees of the Board for detailed oversight. In some instances, the identification of a risk may require the Board to engage an advisor to assist in oversight, or at a minimum educate the Board in a certain area. While delegation of detailed risk oversight is essential to efficient Board operations, it is important to remember that the full Board, and each individual director has a fiduciary duty around the oversight of risk.

The AC should ensure that it understands the ERM processes and practices adopted by the company to identify and prioritize risk in accordance with the company's unique risk appetite and tolerance. Simply identifying, assessing and reporting on risks, while part of the process, is not in and of itself an evolved ERM program. James MacDonnell and Joe Casey, Managing Directors and Leaders within BDO's Risk Insurance and Risk Advisory groups, recently **discussed** the role of the Board in ERM, trends in ERM and opportunities to maximize the value of ERM programs.

Efficient and effective risk oversight requires frequent and clear communication of roles and responsibilities, collaboration between directors, committees, the full Board, management and other departments and individuals, and timely reporting and review by the full Board. The ERM process should be ongoing and as changes in risks are identified, the oversight allocation, documentation and reporting should be updated accordingly. Additionally, Boards should note there is a renewed focus by the SEC on Board leadership structure and risk oversight **disclosure** under item 407 of Regulation S-K. Comment letters have been issued asking registrants to disclose why the current leadership structure is appropriate and how the Board administers its oversight function and has referred companies to the **adopting release** of the rule as helpful guidance.

Core responsibilities around oversight of financial reporting and audit quality, coupled with the prevalence of overseeing risk management and cybersecurity, contribute to the AC's "kitchen sink" moniker. The Center For Audit Quality (CAQ) has recently released a joint academic **study** that addresses these concerns and provides insight into effectively allocating oversight responsibilities to the AC, supporting AC members in keeping up with an ever-evolving workload, all while improving AC oversight disclosures.

Evolving Risk

While risks will vary by company, several broadly applicable risks involving technology, innovation, cybersecurity, fraud, human capital and macroeconomic factors have risen to the top in terms of prioritization and impact.

DIGITAL TRANSFORMATION AND CYBER RISK

Digital transformation is everywhere, and ACs should be aware of the impacts of technology on audit firms and the audits they perform. The PCAOB has a short-term standard setting **project** dedicated to considering how auditing standards should be revised to address certain aspects of designing and performing audit procedures using technology-assisted data analysis. Technology-enabled audits can provide increased data analytics and allow auditors to focus more closely on higher risk areas, therefore increasing audit quality. ACs should discuss with the auditor the use of **technology** in their audits and understand the benefits provided to their company. The PCAOB's recent **Spotlight: Audit Committee Resource** provides considerations for ACs in their engagement on this topic.

With digital transformation and continued technological innovation come increased importance for oversight of cyber assets and **data protection**, which should be on the agenda at every Board meeting. Geopolitical activity continues to enhance these risks. **The Cybersecurity & Infrastructure Security Agency** recently released its **Shields Up** initiative, including recommendations for corporate leaders and CEOs around security including ransomware responses. The Board, or the designated committee, should consider the following:

- Continually evaluate knowledge and experience in this area, identify gaps, and determine where advisors and/or succession planning may be necessary.
- Identify and document responsibility for Board oversight and development and maintenance of programs within management.
- Understand the company's data protection policies and procedures and the mechanisms in place to support them to ensure they are up to date and in line with best practices, laws and regulations.
- Help set the scope of a company's compliance and ethics program, including performing a timely review of policies and procedures and reviewing periodic reporting to ensure adherence to those objectives.

Consider the following resources in the Board's oversight of data protection:

- **Questions** Boards should be asking in their oversight of cybersecurity.
- Director Oversight of Cybersecurity in Today's Digital Environment **archived webinar**.
- Data Privacy and Governance **Checklist** for the Board.
- Board's Role in Data Protection **interactive article**.

Boards need to be wary of becoming desensitized to cybersecurity risk. **Security Magazine** reports that the global average cost of a data breach increased 2.6% from $4.24 million in 2021 to $4.35 million in 2022 — the highest it has been in the history of **IBM Security's** "The Cost of a Data Breach Report." Recent high profile breaches — e.g., Medibank, The Los Angeles Unified **School District**, Uber, **Twitter** and the **Costa Rica Government** — remind Boards that risk goes beyond financial to encompass legal, reputational and consumer trust concerns, and supports the need for "zero trust cybersecurity frameworks." The SEC's proposed cybersecurity **disclosures** aim for greater transparency to allow investors to accurately evaluate cybersecurity concerns.

REVISITING FRAUD

The recent FTX bankruptcy reminds Boards of the imminent risk of fraud and the importance of strong governance and controls to protect companies. Unfortunately, the likelihood of fraudulent activities is increased by the current environment which aptly supports the three dimensions of the fraud triangle: motive/pressure, rationalization and opportunity. Boards can combat this by limiting opportunity for unethical activity via strong internal controls and culture. In October, the SEC's Acting Chief Accountant Paul Munter issued a **public statement** reminding independent auditors of their role in financial statement fraud detection, estimated by The Association of Certified Fraud Examiners (ACFE) to be 5% of revenue each year, or an estimated $4.7 trillion loss on a global scale. (See ACFE's 2022 annual **Occupational Fraud Report** for comprehensive analysis.) The PCOAB **revealed** that fraud considerations were among the common deficiencies in their most recent inspections and further emphasized this point by **announcing** that the Board plans to continue its focus on audit risk factors including fraud, during the current inspection cycle.

AC members should familiarize themselves with recent SEC enforcement actions, which resulted in a 9% increase in 2022 with 760 actions in total resulting in $6.4 billion in penalties. Themes in enforcement centered around ethical or fraudulent behavior by companies and individuals. Examples include making materially misleading or false public statements and overvaluing assets. The Department of Justice (DOJ) is further taking immediate steps to tackle corporate crime. Deputy Attorney General Lisa O. Monaco updated the **DOJ's four-step enforcement plan** in September 2022. Recent **remarks** highlight a focus on individual accountability together with consideration of voluntary disclosure as an indication of an effective compliance program.

ACs are reminded of the importance of an effective internal control environment and culture in the oversight of financial reporting and risk. The PCAOB has included fraud within their recent **Spotlight: Audit Committee Resource**, the **Anti-Fraud Collaboration** offers resources, and The Committee of Sponsoring Organizations of the Treadway Commission (COSO) has a specific **Fraud Risk Management Guide** to assist companies in going beyond assessment to include guidance on establishing an overall fraud risk management program. Fraud risk is rife in today's environment and directors should employ the same professional due care and skepticism expected of auditors when overseeing this risk.

EMERGING RISKS

Call them what you will: "black swans," "gray rhinos," "white elephants," Boards should be aware and evaluate a variety of emerging risks ranging in likelihood, predictability and impact. Recent experiences have demonstrated the value of **resilience** in addressing many of these concerns. **Boards** who have invested in crisis preparedness and planning, including communication plans and table-top mock scenarios, are able to respond to these events faster and more efficiently.

Next Steps

We encourage ACs to remain up to date on evolving trends and work with advisors on continuing education plans. Subscribe to future publication and events offered by **BDO's Center for Corporate Governance**. We further invite you to review our 2023 priorities for the **full Board**, the compensation committee and the nominating and governance committee.

Contact Us

AMY ROJIK
National Managing Partner, Corporate Governace,
Communications and Emerging Issues
617-239-7005 / arojik@bdo.com

LEE SENTOR
Director, Professional Practice
617-239-4142 / lsentor@bdo.com