Dan Goelzer

AUDIT COMMITTEE AND AUDITOR OVERSIGHT UPDATE

Update No. 77
September-October 2022

This Update summarizes recent developments relating to public company audit committees and their oversight of financial reporting and of the company's relationship with its auditor.

In This Update:

PCAOB Reports 2021 Target Team Observations

Since 2019, the Public Company Accounting Oversight Board's annual inspections program has included a "target team." The target team examines how auditors handled specific issues on a cross-firm basis. The team "executes in-depth reviews across audit firms using information-gathering inspection procedures that extend beyond traditional inspection procedures." The target team inspectors focus on emerging audit risks and topics that the PCAOB staff believes could have important implications for audits.

Dan Goelzer is a retired partner of Baker McKenzie, a major international law firm. He advises a Big Four accounting firm on audit quality issues. From 2017 to July 2022, Dan was a member the Sustainability Accounting Standards Board. The SEC appointed him to the Public Company Accounting Oversight Board as one of the founding members, and he served on the PCAOB from 2002 to 2012, including as Acting Chair from 2009 to 2011. From 1983 to 1990, he was General Counsel of the Securities and Exchange Commission.

In Spotlight: Observations From the Target Team's 2021 Inspections, the staff summarizes the target team's work in 2021, including deficiencies observed and good practices identified. The 2021 target team reviewed 40 public company audits in nine industry sectors. The team looked at four core areas – fraud risk, interim reviews of special purpose acquisition companies (SPACs), going concern, and cash and cash equivalents.

Fraud Risk

The potential for fraudulent financial reporting (e.g., as a result of aggressive assumptions and estimates, improper revenue recognition, and misleading disclosures) is elevated in the current economic environment. Under the PCAOB's standards, the auditor has a responsibility to consider the possibility of fraud and how it might be committed and to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether caused by error or fraud. (Regarding the auditor's responsibility for fraud, see SEC Chief Accountant Issues a Reminder on Fraud in this Update.)

The target team observed various types of deficiencies in auditors' responses to fraud risk, including:

- Failure to perform sufficient procedures to understand the company's whistleblower program.
- Failure to properly consider company-specific factors when identifying and selecting journal entries for testing and performing other fraud procedures.
- Failure to sufficiently document the assessment and evaluation factors used to select journal entries for testing, the performance of procedures to test such entries, and the understanding of individuals empowered to initiate general ledger entries.

The target team also identified certain procedures that may have enhanced audit quality with respect to fraud risk. These included querying a database of registered businesses to determine whether any were associated with company employees; asking open-ended questions to solicit employees' views on the company's financial reporting process; and involving the audit firm's forensic staff in the engagement team's fraud risk-assessment procedures in high-risk industries.

Interim Review of SPACs and De-SPAC Transactions

In light of the increased level of initial public offerings and merger and acquisition transactions involving SPACs, the target team focused on auditor interim reviews of financial statement accounts for SPACs and de-SPAC transactions. The objective of an interim review is to provide the auditor with a basis for communicating whether he or she is aware of any material modifications that should be made to the interim financial information. The target team observed three types of deficiencies:

- Failure to identify that the company's equity statement did not agree with its accounting records.
- Failure to consider whether presentation and disclosures of the interim financial statements conformed to GAAP.
- Failure to recognize that public warrants were incorrectly included in the Level 3 fair value roll-forward.

The target team also observed three types of good practices with respect to SPAC interim reviews:

- Use of auditor-employed specialists to review the work of the company specialists in determining valuations, such as of warrant liability and intangible assets.
- Required consultation when evaluating quantitative factors for establishing materiality for start-up entities.

- National office participation in discussion of whether engagement teams should involve financial instrument specialists in de-SPAC transaction reviews.

Going Concern

Under the PCAOB's standards, the auditor has a responsibility to evaluate whether there is substantial doubt about the entity's ability to continue as a going concern for a reasonable period of time, not to exceed one year beyond the financial statements date. If the auditor concludes there is substantial doubt, he or she should consider the adequacy of disclosure about the entity's possible inability to continue as a going concern and include an explanatory paragraph in the audit report.

The target team observed multiple audits where engagement teams either did not perform procedures at all or the procedures performed were insufficient to evaluate aspects of going concern risk. For example, in some cases engagement teams did not perform sufficient procedures to evaluate the reasonableness of forecasted cash outflows, perform procedures to assess the reasonableness of forecasted available borrowings, or evaluate the relevance and reliability of information from external sources used in earnings projections.

Good practices in going concern assessments included requiring consultation in connection with managements' going concern evaluation and related assumptions, assigning experienced staff members to the going concern assessment, and collaboration among members of audit firm industry groups.

Cash and Cash Equivalents

In light of recent high profile frauds involving cash, the target team focused on arrangements for holding cash and cash equivalents that could result in elevated audit risk. The team observed deficiencies relating to the use of third-party cash confirmations, including failure to perform sufficient procedures to support the validity of confirmations received. The team also detected situations in which work papers did not adequately document confirmation procedures. Audit quality-enhancing practices in this area included updated firm guidance on bank account confirmations and use of service providers to facilitate direct electronic transmission of confirmations.

Comments: The target team report may be useful to the audit committee in performing the committee's own analysis of financial reporting risk and in understanding auditor risk assessment and resource allocation decisions. The report's descriptions of deficiencies and good practices observed by the target team may also provide the audit committee with insights that can facilitate discussion of audit planning with the engagement team. Finally, the target team report may be helpful to the audit committee in understanding what aspects of the company's future audits are likely to attract PCAOB inspection staff attention.

PCAOB Updates its Standard-Setting Agenda

In May, the Public Company Accounting Oversight Board released a new standard-setting and research project agenda. See PCAOB Announces an Ambitious Standard-Setting Agenda, April-May Update. On October 12, the Board issued an updated agenda, adding two new standard-setting initiatives and one new research project. The Board also revised the target action dates for three projects.

The new standard-setting projects are:

- Amendments Related to Certain Aspects of Designing and Performing Audit Procedures that Involve Technology-Assisted Data Analysis. This project will consider how PCAOB standards should be revised to address designing and performing audit procedures using technology-assisted data analysis. One of the projects on the Board's research agenda is examining the increased use of technology-based tools by auditors and preparers. The Board states that, while

results of that research indicate that PCAOB standards do not preclude auditors' use of technology, updates to some standards may be necessary.

- Interim Standards – AS 1000. The PCAOB will consider changes to auditing standards in the AS 1000 series (*General Principles and Responsibilities*) and to AS 2815, *The Meaning of "Present Fairly in Conformity with Generally Accepted Accounting Principles*. The AS 1000 series consists of four standards: AS 1001, *Responsibilities and Functions of the Independent Auditor*; AS1005, *Independence*; AS 1010, *Training and Proficiency of the Independent Auditor*; and AS 1015, *Due Professional Care in the Performance of Work*. These standards are substantially the same as the AICPA standards the PCAOB adopted on an interim basis in 2003. The staff believes that "the concepts in these standards remain sound, but the standards could be modernized and streamlined through updates that would clarify auditor responsibilities and enhance the usability of the standards by making them easier to read, understand, and apply."

The Board anticipates issuing proposals for comment in both of these new projects during 2023.

The project added to the Board's research agenda is entitled Firm and Engagement Performance Metrics. This project will assess the need for guidance, changes to standards, or other actions in light of the increased disclosure and demand for firm and engagement metrics. As part of the project, the staff will evaluate metrics that audit firms already disclose to audit committees and the public. Performance metrics, or audit quality indicators, have been under consideration for some time. In 2008, the Department of Treasury's Advisory Committee on the Auditing recommended that the PCAOB determine the feasibility of developing key indicators of audit quality and of requiring audit firms to publicly disclose these indicators. In 2015, the PCAOB issued a concept release on audit quality indicators and invited public comment on 28 potential indicators.

In addition to these new matters, the Board updated the timeline for three previously-announced projects:

- The anticipated timing for publication of a re-proposal of the updated standard on the confirmation process has moved up to 2022 from 2023. The Board plans to issue the re-proposal before the end of this year.

- The standard-setting project on the auditor's consideration of possible noncompliance with laws and regulations and the project on updating the Board's attestation standards have both been pushed back. The Board now anticipates issuing proposals in these two projects in 2023, rather than 2022, as previously announced.

The Board removed from its agenda the project on standards governing the principal auditor's use of other auditors. That project was completed by the adoption of a final standard in June. See PCAOB Strengthens the Standards for Audits Involving Multiple Auditors, June-July 2022 Update. The content and timing of other standard-setting and research projects on the agenda published in May are unchanged.

Comment: Audit committees should follow developments in the new research project on performance metrics. Depending on the outcome, this project could provide committees with a useful new set of tools for evaluating engagement team and audit firm performance. Moreover, if the Board promulgates a set of performance metrics, audit firms will likely seek to maximize their scores on these indicators. This could, in turn, impact engagement staffing and performance. Hopefully, the metrics would also have the effect of increasing audit quality. In any event, the development of widely accepted audit quality indicators could have direct and indirect implications for the work of audit committees.

EY's Annual Cybersecurity Disclosure Analysis: Most Breaches Go Unreported

The EY Center for Board Matters (EY Center) has released How cyber governance and disclosures are closing the gaps in 2022, its annual analysis of cybersecurity-related disclosures in the proxy statements and Form 10-K filings of Fortune 100 companies. The EY Center reports that "over the past five years, we have seen steady and significant increases in the percentage of disclosures in certain categories of cyber management and oversight." However, the Center believes that, in one area, reporting is lagging: "There appears to be a gap between disclosures around material cybersecurity incidents, including the depth of the disclosures, as compared with the number and scale of cyber incidents reported in the news media and third-party reports."

The EY Center reviewed reports of the 74 Fortune 100 companies that filed with the SEC from 2018 through May 31, 2022. In general, cybersecurity disclosure trends identified in last year's EY report continued in 2022. (For discussion of the 2021 EY Center report, see EY Reports on the State of Cybersecurity Risk Disclosure, September-October 2021 Update.) Key 2022 findings include:

- Ninety-five percent of the surveyed companies disclosed a focus on cybersecurity in the risk oversight section of the proxy statement, up from 76 percent in 2018.

- Seventy-four percent of the companies provided insights into management reporting to the board or to committees overseeing cybersecurity matters, up from 54 percent in 2018. Sixty-eight percent discussed the frequency of such reporting, compared to 36 percent in 2018. In addition, 39 percent disclosed that management reports to the board on cybersecurity at least annually or quarterly; only 11 percent did so in 2018.

- More than half of the companies cited cybersecurity experience in at least one director biography, up from 28 percent in in 2018. Further, 46 percent disclosed cybersecurity as an area of expertise sought on the board.

- Forty-nine percent identified at least one cybersecurity point person (e.g., the chief information security officer or the chief information officer) who reports to the board. Twenty-three percent identified such a person in 2018.

- Fifty-one percent reported maintaining cybersecurity insurance, compared to 31 percent in 2018.

- Only 9 percent of the Fortune 100 companies reviewed disclosed performing cyber tabletop exercises and response readiness simulations. Three percent reported such exercises and tests in 2018. (In a 2021 EY survey of board members, 86 percent said their board had not participated in a breach or ransomware simulation exercise in the last 12 months.) The EY Center strongly recommends that companies engage in such simulations. "If cybersecurity breach simulation plans are not practiced and a breach occurs, the reaction by the board and management is largely improvised. Well-designed incident simulations and tabletop exercises can stress-test the organization and improve readiness by providing clarity of roles, protocols and escalation processes * * * ."

Cybersecurity risk is typically an audit committee responsibility. The EY Center found that 70 percent of the Fortune 100 companies reviewed assign cybersecurity oversight to the audit committee – a slight increase over 2021 and up from 57 percent in 2018. Sixty-nine percent of those companies formalized the audit committee's cyber responsibility in the committee charter.

As noted above, the EY Center believes that many cybersecurity breaches are not disclosed. The report states that only 40 of the 74,098 Form 8-K filings in 2020 reported material cybersecurity incidents. In contrast, the 2020 Verizon Data Breach Incident Report stated there were 3,950 confirmed data breaches

in 2020 (Verizon did not address the materiality of these breaches). The EY Center report also quotes a government official as opining that only about a quarter of ransomware intrusions are reported.

Based on EY's work in this field, the report lists ten "leading practices" in board cyber risk oversight. These practices, which are similar to the nine leading board practices in last year's report, are:

1. Elevate the tone. Establish cybersecurity as a key consideration in all board matters.

2. Stay diligent. Address new issues and threats stemming from remote work and the expansion of digital transformation. And remember that every employee needs to be diligent, too — 82% of breaches involve a human element, according to Verizon's 2022 Data Breach Incident Report, issued in late May.

3. Determine value at risk. Reconcile value at risk in dollar terms against the board's risk tolerance, including the efficacy of cyber insurance coverage.

4. Leverage new analytical tools. Such tools inform the board of cyber risks ranging from high-likelihood, low-impact events to low-likelihood, high-impact events (i.e., a black swan event).

5. Embed security from the start. Embrace a "trust by design" philosophy when designing new technology, products, and business arrangements.

6. Independently assess your program. Obtain a rigorous third-party assessment of your cyber risk management program (CRMP).

7. Evaluate third-party risk. Understand management's processes to identify, assess and oversee the risk associated with service providers and third parties involved in your supply chain. Supply chains were responsible for 62% of system intrusion incidents in 2021, according to Verizon's 2022 Data Breach Incident Report.

8. Test response and recovery. Enhance enterprise resilience by conducting rigorous simulations and arranging protocols with third-party specialists before a crisis.

9. Understand escalation protocols. Have a defined communication plan for when the board should be notified, including incidents involving ransomware.

10. Monitor evolving practices and the regulatory and public policy landscape. Stay attuned to evolving oversight practices, disclosures, reporting structures and metrics.

The report also discusses public policy developments affecting cyber defenses, risk, and breach disclosure. One of the themes of the report is that the SEC's proposed cybersecurity rules will have a significant impact on future disclosure. Among other things, the SEC proposals would require reporting within four business days of a material cybersecurity incident and periodic reporting of a company's cybersecurity risk management, strategy, and governance. The SEC has indicated that it plans to finalize these proposals in early 2023. See SEC Proposes Cyber Risk Management and Attack Reporting Requirements, March 2022 Update. The EY Center reviews various other government actions related to cybersecurity, including passage of the Cyber Incident Reporting for Critical Infrastructure Act of 2022. See New Legislation Requires Cyber Incident Reporting, March 2022 Update.

Comment: Cybersecurity risk and related disclosures should be on the agenda of all audit committees. Even in those cases where the audit committee is not charged with substantive responsibility for cyber risk, disclosure related to strategy and any breaches would fall within the scope of the committee's oversight. The Appendix to the report contains a compilation of sample cybersecurity disclosures from public filings. These examples are worth reviewing to understand how other companies are approaching disclosure in this area.

In the next six months the SEC is likely to adopt both its proposed climate change disclosure rules and its cybersecurity reporting proposals. The EY Center observes that it will be challenging for audit committees to "absorb both incremental cyber and ESG reporting obligations and governance responsibilities." As to cyber, the Center's advice is to begin now: "Although the proposed SEC rules would formalize the timing and specify the content and location of cybersecurity disclosures by companies, the opportunity remains for registrants to not wait for the rules to become final or to limit themselves to doing only what is required. In other words, an opportunity is at hand to strengthen disclosures to demonstrate accountability and engagement, and to build stakeholder trust around how cybersecurity is prioritized, managed and overseen as a critical enterprise risk and strategic function."

AA's 20-Year Review Finds Audit Fees are Rising Again

Audit Analytics (AA) has released Twenty-Year Review of Audit Fee and Non-Audit Fee Trends, its annual analysis of fees paid to external auditors. After a decline in 2020, average audit fees increased in FY 2021, although the average fee remained below 2019 levels. But, from one perspective, audits seem to be getting cheaper. Despite the increase in the average fee, the ratio of audit fees to company revenue fell in 2021 as revenues rebounded from a decrease during the COVID-19 pandemic. AA also found that the trend away from providing non-audit services to audit clients continued in 2021. Non-audit fees (exclusive of audit related fees) as a percentage of total fees hit an all-time low in FY 2021 of 8.9 percent. (AA's prior audit fee report is discussed in Audit Fees Declined in 2020, But Don't Get Used to It, January-February 2022 Update.)

Findings of the Twenty-Year Review that may be of particular interest include:

- In 2021, aggregate total fees (including for audit, tax, and other services) paid to the external auditor by SEC reporting companies grew 3.3 percent from 2020, to $18.9 billion. AA states that the aggregate fee increase was primarily a result of an increase in the number of SEC registrants from 7,041 to 7,133. Aggregate audit fees increased 2.9 percent, while audit-related fees increased 10.2 percent. Total tax fees decreased by 0.8 percent, continuing the downward trend that began in 2018. The total amount of other/miscellaneous fees increased by 3.0 percent.

- The average SEC registrant audit fee increased about 1.6 percent to $2,176,000 in 2021. Average audit-related fees increased to $239,000, and average tax fees decreased to $203,000, the lowest since 2014. The average amount of fees classified as "other" remained stable.

- When analyzed by company size, the changes in the average audit fee present a more varied picture. The average audit fee rose slightly for smaller companies in 2021 but fell for larger companies. Average audit fees for non-accelerated filers increased by 1.3 percent, while the accelerated filer average audit fee decreased by 12.7 percent and the average large accelerated filer audit fee fell by 8.8 percent.

- Audit fees per million dollars of revenue declined to $594 in 2021. AA states that "this was expected, as revenues returned to pre-pandemic levels."

- As a percentage of total fees, non-audit fees (exclusive of audit-related fees) declined to 9 percent in 2021. By comparison, in 2002 such fees were approximately 36 percent of total fees paid to the external auditor.

In the introduction to its report, AA points out that audit fees are an indicator of audit complexity and risk because "[h]igher risk audits require more auditor resources (hours, personnel, specialists, etc.) to reduce audit risk to an acceptable level." Accordingly, "[a]nalyzing fees by industry, company size, and location can provide insight into the level of risk and auditor effort various sectors of publicly listed companies entail." From an industry perspective –

- The 2021 highest average audit fees were in Transportation ($3.015 million) and Finance ($2.375 million). The industries with the lowest average audit fees were Agriculture ($1.312 million) and Mining ($1.472 million).

- The 2021 highest audit fees per million dollars of revenue were in Agriculture (approximately $1,500) and Services (approximately $1,000). The lowest fees per million dollars of revenue were in Retail Trade (approximately $175) and Wholesale Trade (approximately $250).

Comment: Audit committees may find it useful to compare changes in their company's fees with the information in the AA report. Committees might also want to focus on how their non-audit fees compare to the broad metrics. As noted, AA found that in 2021 non-audit fees, as a percentage of total fees paid, reached the lowest level since AA began complying this data. AA observes that there has been "a global focus on restricting certain non-audit services to safeguard auditor independence." Beyond regulatory restrictions, many audit committees have limited their company's use of the financial statement auditor for non-audit services in order to avoid questions about the possible impact of such services on auditor objectivity.

On the Update Radar: Things in Brief

PCAOB Chair Has Advice for Audit Committees. On October 7, PCAOB Chair Erica Williams delivered remarks on audit committee responsibilities at the University of California-Irvine's Audit Committee Summit. Her comments included the following points:

- The PCAOB recently issued a publication focused on questions for audit committee members to consider in their interactions with their auditors. (See We Have Some Questions for You. The PCAOB Releases a New Audit Committee Resource, August 2022 Update.)

- PCAOB inspection reports can be useful in connection with an audit committee's evaluation of its auditor. "If you see a particular firm has had deficiencies in the past, ask them what they are doing to avoid repeating those deficiencies in your audits." Audit committees should also ask for information beyond what appears in PCAOB public reports. "Find out what your firms are doing to ensure the highest quality in your audit. How does their system of quality control work, and how do they determine that it is working effectively both at the engagement and the firm levels?"

- Independence is a responsibility of both the auditor and the company. Audit committees should assess the auditor's independence "carefully and regularly."

- Audit committees should make sure the auditor's skills, expertise, and experience are the right fit for the specific needs of the company.

- The audit committee should understand the company's "control environment, communication, monitoring, risk assessment, and policies and procedures. The better you understand your company's control and compliance environment, the better you can protect the integrity of its financial disclosures."

- The PCAOB plans to release rule proposals regarding the auditor's responsibility when he or she detects possible noncompliance with laws and regulations (NOCLAR). Auditors are required to assess illegal acts and notify the audit committee, and committees should consider commenting on the Board's NOCLAR proposals.

SEC Chief Accountant Issues a Reminder on Fraud. Acting SEC Chief Accountant Paul Munter has released a statement emphasizing the auditor's responsibilities for financial statement fraud. In The Auditor's Responsibility for Fraud Detection, Mr. Munter notes that auditors are gatekeepers and that their responsibilities with respect to the identification of fraud risks and the detection of material misstatements due to fraud "should not be underestimated." Auditor fraud responsibility is particularly important when "the macroeconomic and geopolitical environment in which companies operate may result in new pressures, opportunities, or rationalizations for fraud."

Mr. Munter points out that, under PCAOB auditing standards, auditors have a responsibility to consider the possibility of fraud and to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether caused by fraud or error. Regarding materiality, he notes that the SEC staff has long taken the position that qualitative factors may cause misstatements of quantitatively small amounts to be material and that "auditors should not assume that even small intentional misstatements in the financial statements are immaterial."

Mr. Munter sees evidence of "shortcomings" in auditors' discharge of their responsibility to detect material misstatements due to fraud. This evidence includes PCAOB inspections that identify concerns as to auditors' professional care and skepticism when considering fraud; SEC enforcement actions that highlight improper auditor professional conduct with respect to fraud risk; and "troubling feedback that auditors many times frame the discussion of their responsibilities related to fraud by describing what is beyond the auditor's responsibilities and what auditors are not required to do."

The statement offers suggestions for auditors in discharging their fraud responsibilities, including –

- Be skeptical of evidence provided by management when the timing or manner in which such evidence is produced is questionable (e.g., invoices for large amounts with vague descriptions, invoices with related parties with descriptions that are outside of the normal course of business, or new evidence provided by management in the late stages of the audit to address a potentially difficult audit matter).

- Devote sufficient time and resources to assessment of the issuer's entity-level controls. "An auditor is required to obtain an understanding of the issuer's control environment. This would include assessing whether the organization demonstrates a commitment to integrity and ethical values."

- Consider whether the involvement of a forensic specialist is necessary to assist in identifying and responding to fraud risks or to challenge and evaluate the reasonableness of management's assumptions underlying particular estimates.

- Avoid using examples of fraud risk considerations and related responses in the auditing standards as a checklist. "Audit responses should be tailored to the identified fraud risk and dynamic to changing business environments."

- Review the whistleblower hotline. Examine whether the issuer has "a culture that encourages whistleblowers who see something to actually say something." The auditor may want to discuss with the audit committee the nature of the whistleblower hotline's operation.

The Munter statement is a forceful reminder to auditors of their fraud risk responsibilities and a warning that the SEC will be aggressive when it believes there have been lapses in this key area. Audit committees can expect that their auditor will respond accordingly. Mr. Munter's emphasis on the need for auditors to consider the possibility of frauds that are qualitatively (but not quantitatively) material and to assess the audit client's commitment to integrity and ethical values do not break new ground. The fact that he highlights these points in a public statement may however lead auditors to devote a higher level of attention to such issues in their future work.

DOJ Announces Tougher Corporate Enforcement and Self-Policing Policies. On September 15, Criminal Division Assistant Attorney General Lisa Monaco issued a memorandum outlining new Department of Justice corporate criminal enforcement policies. The memorandum emphasizes that the Department intends to hold individuals criminally responsible for corporate violations and that it expects companies to disclose misconduct voluntarily and promptly. In a speech delivered the same day as release of the memorandum, Assistant AG Monaco elaborated on these points, stating that "the Department's number one priority is individual accountability * * *. Whether wrongdoers are on the trading floor or in the C-suite, we will hold those who break the law accountable, regardless of their position, status, or seniority." As to self-reporting, she added: "We expect good companies to step up and own up to misconduct. Voluntary self-disclosure is an indicator of a working compliance program and a healthy corporate culture. Those companies who own up will be appropriately rewarded in the Department's approach to corporate crime."

Other key points in the DOJ memorandum include:

- In order to obtain credit for cooperation, a company's voluntary disclosure must include information relevant to individual culpability. "To be eligible for any cooperation credit, corporations must disclose to the Department all relevant, non-privileged facts about individual misconduct. * * * [P]roduction of evidence to the government that is most relevant for assessing individual culpability should be prioritized."

- Past misconduct will be a factor in the Department's consideration of how to resolve a corporate criminal investigation. Prosecutors will weigh whether the conduct in prior and current matters reflects broader weaknesses in company compliance culture or practices. "One consideration is whether the conduct occurred under the same management team and executive leadership. Overlap in involved personnel -- at any level -- could indicate a lack of commitment to compliance or insufficient oversight of compliance risk at the management or board level." This comment suggests that, if the company is involved in a criminal matter, the board should consider the need for executive level management changes.

- In evaluating a company's compliance program, compensation policy will be an important factor. Ms. Monaco also makes clear in her speech that companies should employ compensation claw backs to hold individuals who contribute to criminal misconduct accountable. As the memorandum states, "Compensation systems that clearly and effectively impose financial penalties for misconduct can incentivize compliant conduct, deter risky behavior, and instill a corporate culture in which employees follow the law and avoid legal 'gray areas.'"

Audit committees often have responsibility for the corporate compliance program. The Monaco memo could serve as an opportunity to revisit whether the company's program is appropriately designed and functioning effectively and whether conduct that could trigger a criminal investigation is brought promptly to the board's attention. The decision whether to make a voluntary disclosure to the Department of Justice is difficult and complex and should only be made with the guidance of experienced counsel. But, if the Board does not receive prompt notice of potential criminal exposure, it will not be in a position to make a well-considered decision.

PCAOB Gives EY a Partial Fail on 2018 Remediation. On October 17, the PCAOB made public a portion of the previously nonpublic section of Ernst & Young's 2018 inspection report. This action indicates that, in the Board's view, the firm did not satisfactorily address the quality control issue discussed in that portion of the inspection report within 12 months of the report date. Criticisms of a firm's quality control system are discussed in Part II of the firm's inspection report. Under the Sarbanes-Oxley Act, Part II is nonpublic when the report is issued. If the firm does not satisfactorily address the quality control criticism within 12 months, the Board makes the criticism public.

The now-public PCAOB criticism in EY's 2018 report relates to EY's policies and procedures with respect to independence. In 2018, EY conducted a sampling review of compliance with its internal requirement that firm personnel report certain financial relationships to the firm. The review found that 33 percent of partners and 46 percent of managers in the sample had not reported financial relationships that they were required to report. The PCAOB's inspection report states: "These high rates of non-compliance with the firm's policies, which are designed to provide compliance with applicable independence regulatory requirements, provide cause for concern, especially considering that these individuals are required to certify on a quarterly basis that they have complied with the firm's independence policies and procedures." The 2018 EY inspection report is dated April 28, 2020. Therefore, release of this portion of the inspection report indicates that EY failed to persuade the PCAOB that, as of April 28, 2021, it had satisfactorily remediated this quality control deficiency.

Disclosure of a portion of Part II of a major firm's inspection report is unusual, but not unprecedented. The Board has taken such action at least once with respect to each of the Big Four firms.

Deloitte Updates its Audit Committee Guide. Deloitte's Center for Board Effectiveness has released an updated version of its Audit Committee Guide (Guide). In the press release announcing the updated Guide, the Center describes it as "providing a first-hand look at the latest requirements and an explanation of the shifting roles and responsibilities of audit committee members, especially in emerging areas such as environmental, social, and governance issues, including cybersecurity." The announcement also states that the enhanced Guide can serve as a resource for audit committee members on such topics as:

- How audit committees can fulfill their responsibilities to oversee financial reporting, risk, internal auditors, independent auditors, and ethics and compliance.
- To what extent committee composition meets the requirements of the SEC, NYSE, and Nasdaq with respect to independence and financial literacy.
- How an audit committee's charter aligns with current listing requirements, especially as the committee's responsibilities may have shifted in recent years.
- Common practices and considerations with respect to performing committee evaluations and self-assessments.
- How committees can improve their overall effectiveness.

The Guide is divided into three sections –

- Audit committee requirements discusses the required structure and composition of the audit committee as well as requirements for charters, independence, financial expertise, and literacy, and evaluating performance.
- Audit committee oversight responsibilities covers the audit committee's responsibility to oversee financial reporting and related internal controls, risk, ethics and compliance, and auditors.
- Audit committee effectiveness addresses leading practices audit committees can consider in preparing for and conducting meetings and in executing their oversight responsibilities.

Each section of the Guide includes questions that committees may wish to ask to promote dialogue on the topics covered in the publication. In appendices, the Guide presents a sample audit committee charter, an audit committee calendar of activities, and an audit committee performance evaluation questionnaire.

The Audit Blog

I am a co-founder of The Audit Blog and blog on developments in auditing and financial reporting, on auditor oversight and regulation, and on sustainability disclosure. Occasionally, items that appear in the Audit Committee and Auditor Oversight Update also appear on the blog. Recent posts include –

- In Search of a Purpose – The PCAOB's Attestation Standards Review (Dan Goelzer, October 20, 2022)
- Supercharging PCAOB Enforcement May Encounter Some Speedbumps (Dan Goelzer, October 6, 2022)

The blog is available here. You can follow it @BlogAuditor on twitter or @the-audit-blog on medium.com.

For further information, please contact:

Daniel L. Goelzer
301.288.3788
dangoelzer@gmail.com

The Update's website is www.auditupdate.com.

Email distribution of the Update is free of charge. If you would like to be added to the distribution, please email me at the address above. Readers are also free to recirculate the Update.

The Update seeks to provide general information of interest to audit committees, auditors, and their professional advisors, but it is not a comprehensive analysis of the matters discussed. The Update is not intended as, and should not be relied on as, legal or accounting advice.

Updates issued after June 1, 2020, are available here. Updates issued between January 1, 2019, and May 31, 2020, are available here. An index to titles and topics in the Update beginning with No. 39 (July 2017) is available here.