Dan Goelzer

AUDIT COMMITTEE AND AUDITOR OVERSIGHT UPDATE

Update No. 84
August-September 2023

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:

SEC Adopts Cybersecurity Disclosure Rules

On July 26, the Securities and Exchange Commission, by a 3-2 vote, adopted final rules on cybersecurity disclosure. The rules are a modified version of proposals published for public comment in 2022. See SEC Proposes Cyber Risk Management and Attack Reporting Requirements, March 2022 Update. The SEC's objective in adopting these rules is to standardize the content and timing of disclosures regarding cybersecurity. In the SEC's press release announcing adoption of the rules, SEC Chair Gensler states, "Currently, many public companies provide cybersecurity disclosure to investors. I think companies and investors alike, however, would benefit if this disclosure were made in a more consistent, comparable,

---

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.

and decision-useful way. Through helping to ensure that companies disclose material cybersecurity information, today's rules will benefit investors, companies, and the markets connecting them."

Overview of Cybersecurity Disclosures

The SEC's release adopting the new rules contains this chart summarizing the new requirements.

Item	Summary Description of the Disclosure Requirement
Regulation S-K Item 106(b) – *Risk management and strategy*	Registrants must describe their processes, if any, for the assessment, identification, and management of material risks from cybersecurity threats, and describe whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect their business strategy, results of operations, or financial condition.
Regulation S-K Item 106(c) – *Governance*	Registrants must: - Describe the board's oversight of risks from cybersecurity threats. - Describe management's role in assessing and managing material risks from cybersecurity threats.
Form 8-K Item 1.05 – *Material Cybersecurity Incidents*	Registrants must disclose any cybersecurity incident they experience that is determined to be material, and describe the material aspects of its: - Nature, scope, and timing; and - Impact or reasonably likely impact. An Item 1.05 Form 8-K must be filed within four business days of determining an incident was material. A registrant may delay filing as described below, if the United States Attorney General ("Attorney General") determines immediate disclosure would pose a substantial risk to national security or public safety. Registrants must amend a prior Item 1.05 Form 8-K to disclose any information called for in Item 1.05(a) that was not determined or was unavailable at the time of the initial Form 8-K filing.
Form 20-F Form 6-K	FPIs must: - Describe the board's oversight of risks from cybersecurity threats. - Describe management's role in assessing and managing material risks from cybersecurity threats. FPIs must furnish on Form 6-K information on material cybersecurity incidents that they disclose or otherwise

Source: SEC Release No. 33-11216, pages 12-13 (footnote omitted). FPIs are foreign private issuers.

Cybersecurity Incident Disclosure

As reflected in the chart, new Item 1.05 of Form 8-K will require reporting companies to disclose any cybersecurity incident the company decides is material within four days of determining the materiality of

the incident. The company may delay disclosure for 30 days if the Attorney General determines that disclosure of the incident poses a substantial risk to national security or public safety and notifies the company and the SEC of this of this determination in writing. (The practicality of obtaining such a determination from the Attorney General within the four-day window seems remote at best.)

For U.S. companies, incident disclosure must "describe the material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations." Non-U.S. companies must furnish (not file) information on material cybersecurity incidents that any foreign jurisdiction requires them to disclose.

Only material events must be disclosed, and determining materiality will be one of the key compliance challenges. Disclosure is triggered, not by the discovery or occurrence of the incident, but by the company's determination that it is material. Companies must decide whether an incident is material "without unreasonable delay" after its discovery. The materiality of cybersecurity incidents should be evaluated based on the general standard for securities law materiality set out in Supreme Court case law -- information is material if there is a substantial likelihood that a reasonable shareholder would consider it important in making an investment decision or if the information would significantly alter the "total mix" of information made available. Materiality determinations are often not clearcut, and the SEC's release adopting the rules seems to encourage companies to take a broad view when applying the concept to cyber incidents:

> "[T]he material impact of an incident may encompass a range of harms, some quantitative and others qualitative. A lack of quantifiable harm does not necessarily mean an incident is not material. For example, * * * whereas a cybersecurity incident that results in the theft of information may not be deemed material based on quantitative financial measures alone, it may in fact be material given the impact to the registrant that results from the scope or nature of harm to individuals, customers, or others, and therefore may need to be disclosed."

Unlike the proposal, the final rules do not contain a requirement that companies update their Form 8-K disclosures concerning cybersecurity incidents in periodic reports. Instead, Item 1.05 provides that the initial Form 8-K must include a statement identifying any required information that is not determined or is unavailable at the time of the filing and that a Form 8-K amendment must be filed within four business days after such information becomes available.

Cybersecurity Risk Management and Governance Disclosure

New Item 106 of Regulation S-K will require annual disclosure concerning management and board oversight of cybersecurity risk. As to management, companies must describe the processes, if any, by which management assesses, identifies, and manages material risks from cybersecurity threats and the management positions or committees responsible for assessing and managing cybersecurity risk, including their relevant expertise. Companies must also disclose the material effects, or reasonably likely material effects, of risks from cybersecurity threats and previous cybersecurity incidents on their business strategy, results of operations or financial condition.

As to the board, disclosure must include whether management reports information about cybersecurity risks to the board and the board's role in overseeing cybersecurity threat risks. Any board committee or subcommittee that oversees cybersecurity risks must be identified, along with the processes by which management informs the committee about such risks. (The Commission did not adopt the aspect of the proposal that would have required disclosure of cybersecurity expertise, if any, of the company's directors.)

Effective Date

The new rules become effective 30 days following publication in the Federal Register. (The effective date is therefore September 5, 2023.) The Form 10-K and Form 20-F disclosures will be due beginning with annual reports for fiscal years ending on or after December 15, 2023. The Form 8-K and Form 6-K

disclosures will be due beginning on December 18, 2023. Smaller reporting companies have an additional 180 days before they must begin providing the Form 8-K disclosure.

Comment: In many cases, determining whether a cybersecurity incident is material "without unreasonable delay" after its discovery and then, within four business days, making a filing with the SEC describing the material impact or "reasonably likely material impact" of the incident will be difficult and highly judgmental. Management and the board will need to evaluate the materiality of breaches in an environment in which information may be limited and the company's understanding of the event may still be evolving. The company's disclosure will attract the close attention of shareholders, the press, regulators, and the plaintiff's bar.

Audit committees should, to the extent possible, prepare in advance to fulfil their role in meeting these challenges. For example, the audit committees should ask management to evaluate whether the company's existing disclosure controls and procedures regarding cybersecurity incidents are consistent with the new Form 8-K requirements. It will be imperative that the IT staff immediately bring information about cybersecurity incidents to the attention of management with disclosure responsibility and of the audit committee and any other relevant board committees. Audit committees may also want to make sure that management and the board have identified and entered into arrangements with outside experts and advisors who specialize in evaluating cybersecurity incidents. Board training on cybersecurity, including incident response dry runs, could also be considered.

Audit committees may also want to review the impact of the new cybersecurity risk management disclosures. As noted in prior Updates, cybersecurity risk oversight is often assigned to the audit committee. See Slight Increases, Some Stagnation: CAQ and EY Report Cards on Audit Committee Transparency, November-December 2021 Update.) Accordingly, the requirement to describe board oversight of cybersecurity risk, including committees with cyber oversight responsibility, will frequently result in new disclosure about the work of the audit committee. Audit committees may therefore want to review their processes and consider whether any changes or enhancements are necessary.

The Average Audit Fee Reached an All-Time High in 2022

In 2022, the average audit fees for an SEC-registered public companies increased 11 percent over 2021 and hit an all-time high of $2.24 million. That is the headline finding of 20-Year Review of Audit Fee Trends 2003-2022, Ideagen Audit Analytics' (AA) annual analysis of fees paid to external auditors. Last year, AA reported that 2021 audits fees had increased over the prior year, but not to record levels. See AA's 20-Year Review Finds Audit Fees are Rising Again, September-October 2022 Update. For S&P 500 companies, the average audit fee was $10.78 million, a record high for the S&P 500 and a 3 percent increase from FY2021. See Audit Fee Trends of S&P 500 (an AA blog post which breaks out the findings of the annual study for the S&P 500).

Highlights of AA's report and blog post include:

- Total audit fees increased.

  Total audit fees paid by SEC registered public companies (domestic and foreign) were $16.8 billion in FY 2022, an increase of 0.6 percent over FY2021. Total audit fees paid by U.S. companies (i.e., excluding foreign registrants) in 2022 rose to $12.36 billion, up 0.7 percent from 2021. For the S&P 500, total audit fees reached an all-time high of $5.38 billion.

  Total audit fees increased despite a 9 percent decline in the number of reporting companies (from 7,963 in FY2021 to 7,279 in FY 2022. The drop in companies was largely the result of changes in the SPAC market. SPAC IPOs fell 86 percent between 2021 and 2022, and 35 percent of SPACs that reported fees in FY2021 did not file in FY2022.

- Total fees paid to auditors fell.

  Although total audit fees rose, the total fees of all types that SEC registrants paid to their auditor decreased slightly. (Total fees include audit fees, audit-related fees, fees for tax services and fees for other services.) Total FY 2022 fees were $20.2 billion, a decrease of less than 1 percent from FY2021. AA states that the decrease in total fees aligns with the decrease in the reporting company population in FY2022. Each category of non-audit fee saw a decrease from FY2021. Audit related fees decreased 8 percent, tax fees decreased 4 percent, and other fees decreased 15 percent.

- The average audit fee and the average total payment to the auditor both increased.

  As noted above, the average audit fee increased 11 percent from FY2022, reaching an all-time high of $2.24 million per SEC registrant. Average audit-related fees and average tax fees increased by 2 percent and 7 percent, respectively, while the average of other fees decreased by 6 percent in FY2022. Overall, average total fees paid grew 10 percent to $2,702,922, a 20-year record.

- Audit fees per $1 million of company revenue fell.

  Audit fees as a percentage of client revenue were $576 per $1 million of revenue in FY2022, a 6 percent decrease from FY2021 and a nine-year low. Although both audit fees and audit client revenue increased in FY2022, client revenue grew faster – revenue rose 8 percent from FY2021, compared to audit fee growth of only 0.6 percent. For the S&P 500, revenue increased 12 percent in FY2022, while audit fees paid rose by only 4 percent, resulting in audit fees per $1 million dollars of revenue dropping to $343.

  For U.S.-based companies, the average was $583 in audit fees per $1 million of revenue, down 8 percent from FY2021, while foreign SEC filers experienced a 2 percent decrease to $558 per $1 million of revenue. AA points out that SEC-registered foreign companies are, on average, larger than U.S.-based public companies and that the PCAOB's focus on audits performed by non-U.S. accounting firms may be affecting foreign company audit fees.

  EisnerAmper had the highest audit fees per million dollars of client revenue, at $16,595; by comparison, PwC's audit fees averaged $616 per million of client revenue. (The difference in fee per million in client revenue is presumably a function of difference in average client size.)

- The average audit fee rose for larger companies but fell for smaller.

  In FY 2022, average audit fees increased 7 percent (to $5.27 million) for large accelerated filers, the biggest public companies. For the next size tier, accelerated filers, average audit fees paid increased by a stunning 33 percent in FY 2022 to $1,453,905. However, the smallest public companies, non-accelerated filers, experienced a modest decrease in average audit fees paid. In FY2022, the average non-accelerated audit fee was $616,706, down 1 percent from FY2021.

- The large firms dominate SEC filer auditing.

  The four largest accounting firms earned 92 percent of audit fees paid by SEC registrants in FY2022. PwC led with 28 percent of total audit fees ($4.66 billion). EY had a 25 percent share of total audit fees ($4,27 million), followed by DT at 23 percent ($3.81 billion), and KPMG at 16 percent ($2.74 billion).

  Six firms audited the S&P 500 -- the four firms listed above, plus Grant Thornton and BDO. PwC had a 35.7 percent share of total S&P 500 audit fees.

- There was little change in the industries with the highest and lowest average fees and fees per $1 million of revenue.

  The 2022 highest average audit fees were in Transportation ($3.016 million) and Finance ($2.676 million). The industries with the lowest average audit fees were Agriculture ($1.322 million) and Mining ($1.513 million). These same industries were at the top and bottom of the 2021 average fee list.

  The industries with the highest audit fees per $1 million dollars of revenue in 2022 were Agriculture ($1,290 per million) and Finance ($1,016 per million). The industries with the lowest fees per $1 million dollars of revenue were Retail Trade ($168) and Wholesale Trade ($225).

Comment: Audit committees may find it useful to compare changes in their company's fees with the information in the AA report. AA points out in the Introduction to its 2022 report that "[a]udit fees paid to external auditors can be an indicator of audit complexity. Analyzing fees provides further insights into audit risk and auditor independence."

Committees might also want to focus on how their non-audit fees compare to the broad metrics. As noted above, AA found that non-audit fees declined in 2022. AA observes that "much discussion has centered around the effect that significant non-audit services have on external auditors' level of independence" and that many countries (including the U.S.) restrict the type of non-audit services allowed or the amount auditors can be paid for non-audit services. Beyond regulatory restrictions, many audit committees limited their company's use of the financial statement auditor for non-audit services to avoid questions about the possible impact of such services on auditor objectivity.

Audit Committee Members Weigh in on NOCLAR Proposal

The PCAOB's proposal to broaden the scope of the auditor's responsibilities for audit client noncompliance with laws and regulations (NOCLAR) is attracting an unusually high level of comment from audit committee members. Overwhelmingly, but not unanimously, audit committee members that have submitted views to the PCAOB oppose the NOCLAR proposal.

Background

In June, the PCAOB issued for public comment a proposal to amend the auditing standards related to the auditor's responsibility for considering a company's noncompliance with laws and regulations. See PCAOB Proposes to Expand Auditor Responsibility for Financial Statement Fairness and for Legal Compliance, May-June 2023 Update. Current PCAOB standards require the auditor to perform procedures designed to provide reasonable assurance of detecting illegal acts that would have "a direct and material effect" on the determination of financial statement amounts. The proposal would discard the distinction between direct and indirect effects of illegal acts on the financial statements and instead broadly require auditors to identify and evaluate information indicating that noncompliance with laws and regulations, including fraud, has or may have occurred and to communicate such information to management and the audit committee.

Under the new standard, if adopted, the auditor would be required to plan and perform audit procedures to (1) identify laws and regulations with which noncompliance could reasonably have a material effect on the financial statements; (2) assess and respond to risks of material misstatement of the financial statements due to noncompliance with those laws and regulations; and (3) identify whether there is information indicating such noncompliance with those laws and regulations has or may have occurred. The Board approved the NOCLAR proposal by a 3-2 vote, with the two CPA members dissenting. Board Member Christina Ho characterized the proposal as "a breathtaking expansion of the auditors' responsibilities, which I believe will hurt investors."

Audit Committee Member Comments

As of August 31, the Board had posted 137 NOCLAR public comments on its website. Fourteen of the comments express the views of audit committee members. Three are letters from groups of audit committee members or organizations summarizing the views of their audit committee members; six are from individual audit committee members; two were submitted on behalf of public company audit committees; and three are company comments in which the audit committee or its chair joined. Below is a sample of the views expressed in these comments.

1. Group Comments

   A. Audit Committee Chairs, Members, and Board Members. This letter, which is signed by 170 individuals, states that it "represents the views of audit committee chairs and members, as well as other corporate board members." The Center for Audit Quality (CAQ) organized the letter, facilitated audit committee chairs and members across various industries in joining in the letter, and submitted it to the PCAOB on behalf of the participants. The signatories are concerned that:

      - The proposed scope is too broad. ("The proposed requirement that auditors identify 'laws and regulations with which noncompliance could reasonably have a material effect on financial statements' is duplicative and unnecessary.")

      - The proposal does not sufficiently take into account a company's existing compliance function and the shared responsibility of the board of directors, the audit committee, the chief compliance officer, and the general counsel.

      - Auditors are not lawyers and as a result the proposed amendments would expand the auditor's role to include knowledge and expertise outside their core competencies.

      - The proposal will substantially increase the cost of the audit without a commensurate benefit.

      The letter also states that this group believes that:

      - Any change should keep the auditor focused on NOCLAR that could materially impact the financial statements, such as material penalties or loss contingencies.

      - Any requirement of the auditor should be risk-based and consider the role the company's compliance program plays in detecting NOCLAR that could be material to the audited financial statements.

   B. The Audit Committee Council (ACC). The ACC letter expresses the views of a CAQ advisory committee comprised of audit committee chairs and members. The ACC makes five points:

      - *Proposed scope is too broad*. "The proposed amendments would require auditors to identify 'laws and regulations with which noncompliance could reasonably have a material effect on financial statements.' To do this an auditor would first be required to identify all the laws and regulations applicable to the company. The largest of public companies are subject to a vast number of laws, regulations, etc."

      - *Auditors are not lawyers*. The proposal would require skills, knowledge, and expertise that lie outside the auditor's core competencies. "Broadening the scope of the laws and regulations for which the auditor considers whether non-compliance could reasonably have a material impact on the financial statements beyond the finite laws and regulations for which auditors have an understanding (e.g., financial, tax, etc.) does not seem to be consistent with the objectives of a financial statement audit."

- *Existing three lines of defense within companies.* "By design a significant control element of compliance with laws and regulations appropriately rests with the three lines of defense within corporations. * * * External auditors do not represent a large percentage of identified frauds because compliance programs are operating at a sophisticated level such that wrongdoings and/or potential wrongdoings are detected independent of the external auditor's procedures."

- *Increase risk to legal privilege*. Sharing of information related to legal compliance with the auditor "would increase risk to the legal privilege issuers have with their internal and external counsels."

- *Proposal will substantially increase the cost of the audit*. The NOCLAR proposal has the potential to significantly increase audit effort and audit fees, similar to the impact of the auditing standard that implemented the requirement in the Sarbanes-Oxley Act that auditors report on internal control over financial reporting.

The ACC recommendations that the PCAOB broaden its procedures for stakeholder input beyond the comment letter process to include "audit committee roundtables, individual outreach, and surveys" to make the standard setting process more accessible to audit committee members and to obtain input "prior to publishing a significant proposal such as NOCLAR."

C. Tapestry Networks (Tapestry). Tapestry's letter states that Tapestry convened a selection of audit committee chairs who participate in its U.S. Audit Committee Networks and Audit Committee Leadership Network to discuss the NOCLAR proposal. (EY sponsors Tapestry's U.S. audit committee networks but did not participate in the discussion.) Tapestry's letter reflects the dialogue with these audit committee chairs. Tapestry discusses six "overarching themes" and five "specific concerns." The overarching themes are:

- *Clarity of intent*. Most audit committee chairs would like to see greater clarity from the PCAOB about the intent and focus of the proposed changes.

- *Open discussions with the external auditor*. An audit chair is quoted as commenting that "these proposals could have a chilling effect on audit quality gains made in the last five to ten years and the stronger relationship between audit committees and the external auditor."

- *Expectations gap*. Audit committee chairs felt that the proposed changes could further widen the gap between what auditors are required to do in a financial statement audit and what stakeholders expect auditors to do.

- *Role of the SEC*. Audit committee chairs asked whether the SEC was better positioned than the PCAOB to address NOCLAR issues.

- *Impact on the audit profession*. An audit chair expressed concern about "the effect of the proposed changes and the increase in the auditor's responsibilities on the profession more broadly, which is already challenged for talent and skills."

The specific concerns are:

- The proposals do not take other regulators or existing compliance functions into account.

- The proposals would require inordinate efforts to build new systems and procedures.

- Legal matters are complex and constantly evolving, and there may be issues around privilege.

- The proposals fail to take account of the [audit and risk] committees' existing scope and activities.

- Auditors may not have the expertise to comply with the new requirements.

2. Individual Audit Committee Member Comments

   Six individuals who described themselves as audit committee chairs or members submitted comments. Five of the six were critical of the proposal. For example:

   - Vanessa C.L. Chang. "The Proposal to expand auditing standards also expands the liability and responsibility of the Audit Committee in their oversight of the auditors who are not qualified to conclude on noncompliance of the laws and regulations applicable to the company."

   - Donna Harman. "This proposed rulemaking is a gross over-reach of the PCAOB's legitimate role of ensuring proper auditing to protect the public's interest. It is duplicative and conflicting with other local, state and federal government agencies' oversight and enforcement responsibility. Accountants are not equipped to judge compliance with all rules and laws * * *."

   Lawrence M. Alleva, Tom Maurer, and Kent Kresa also filed comments opposing the proposal.

   However, one audit committee chair expressed strong support: "Where we are today is not adequate. It's not even in the neighborhood of adequate. I strongly support the expansion of auditor responsibility to consider instances of noncompliance and their potential impact on the financial statements whether those impacts are direct or indirect." Jon Lukomnik.

3. Audit Committees and Public Company Comment with Audit Committee Concurrence

   Two comments were submitted on behalf of the entire membership of the audit committee of specific companies. (Audit Committee of Microchip Technology Incorporated, Audit Committee of Primerica, Inc.) In addition, in three cases, the audit committee chair or full committee submitted or joined in comments on behalf of the public company. (The Williams Companies, World Kinect Corporation, Stewart Information Services Corporation). All five of these comments opposed the NOCLAR proposal.

Comment: The PCAOB's comment file indicates that the great majority of audit committee members who commented do not support the NOCLAR proposal, at least in its current form. Regardless of one's views on the benefits of greater auditor responsibility to identify legal violations, it seems clear that the proposal would significantly increase the scope of the auditor's responsibilities, the cost of the audit, and the volume of information concerning possible violations that the auditor would be required to bring to the audit committee's attention. Sifting through this information would place new demands on audit committee time and resources.

In light of the comments received, it seems likely that the PCAOB will modify its NOCLAR proposal before moving to final adoption. Because of the potential impact on the audit committee's work, committees should ask their auditor or legal counsel to keep them informed of the progress of this initiative.

Material Weaknesses are Increasing and the Accountant Shortage May Be to Blame

PwC reports a "resurgence" of public company material weakness disclosures. In The resurgence of the material weakness, PwC warns that, when material weaknesses are reported, "shareholders' confidence in the integrity of the financials and the control environment can be shaken, and reputations of company

executives and governing boards (e.g. the Audit Committee) can be harmed by a loss of trust. For these reasons, prompt resolution and remediation of an identified material weakness is typically expected."

In a July 11 article, the Wall Street Journal also discussed material weakness disclosures, but from a different angle. In Maurer, The Accountant Shortage is Showing Up in Financial Statements, the Journal noted that an increasing number of companies are reporting material weaknesses resulting from an inability to attract and retain enough qualified personnel to perform internal control responsibilities. The Journal states: "The disclosures come as fewer people are pursuing degrees in accounting and entering the field, resulting in more positions open and for longer periods of time. What's more, academics say, the shortage will likely be compounded as more accountants retire without a robust pipeline of replacements."

Using information from data provider Ideagen Audit Analytics (AA), PwC reports that material weaknesses disclosed in public company annual reports on Form 10-K rose 73 percent from 2021 to 2022. Further, in the first quarter of 2023, material weaknesses increased 25 percent compared to the same period in 2022. Under the Sarbanes-Oxley Act of 2002 (SOX), public companies must assess the effectiveness of their internal control over financial reporting (ICFR) and disclose any material weaknesses; in addition, SOX requires larger public companies to obtain an opinion from their auditor on ICFR effectiveness. A material weakness, which indicates that ICFR is not effective, is "a deficiency, or a combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the company's annual or interim financial statements will not be prevented or detected on a timely basis."

PwC attributes the increase in material weaknesses to three factors:

- Increase in IPOs and SPACs. PwC states that 41 percent of U.S. initial public offerings since 2017 disclosed at least one material weakness before going public. "These companies typically have fewer resources and a leaner operating model, which can result in weaknesses related to inadequate personnel, oversight and level of reviews."

- Increase in digitization and technology investments. "Companies often overlook risk mitigation measures and controls intended to address digital transformation initiatives such as cloud migration, greater automation, and increasing reliance on machine learning."

- Increase in turnover of resources. "Whether related to restructuring efforts or resignations, there is often insufficient change management, transition, and transfer of knowledge to new control owners as turnover occurs."

Based on AA data, PwC also finds that three areas were the basis for more than half of all reported material weaknesses: Consistent with the Wall Street Journal article noted above, personnel inadequacies (such as number, training, qualifications of personnel, and inadequate segregation of duties) topped the list, accounting for 20.3 percent of material weaknesses. Financial close process (19.8 percent) and IT general controls (e.g., access to programs and data, computer operations, system change management, and system implementation – 15.1 percent) were the second and third most frequent explanations. In terms of company size, companies with revenue between $100 million and $500 million reported 62 percent of 2022 material weaknesses.

PwC's paper concludes with six suggestions for remediating and avoiding material weaknesses:

- Compile your remediation plan - what gets measured gets done.

- Plan your resourcing strategy - give precedence above other competing priorities.

- Start early - remediation doesn't happen overnight.

- Communicate often - all parties need to be involved.
- Think about the long-haul - build a sustainable solution.
- Consider the warning signs - get ahead of potential issues.

Comment: PwC's report, and the Wall Street Journal's article, seem to mirror the conclusions in AA's most recent report on material weakness disclosure. See Ineffective ICFR is More Common; Staff Shortages May be the Cause, August 2022 Update. That report found that, in fiscal 2021, the percentage of companies that reported ineffective ICFR increased across all company sizes and was at the highest level since SOX ICFR reporting began in 2004. Further, lack of qualified accounting personnel was the most frequently cited control issue in adverse ICFR assessments. These trends appear to be continuing, if not accelerating.

The federal securities laws require all public companies to establish and maintain a system of internal accounting control to provide reasonable assurance that (among other things) transactions are recorded as necessary to permit preparation of GAAP financial statements. Audit committees may want to reflect on whether personnel vacancies or turnover could be affecting their company's controls and what steps management could take to address these issues.

On the Update Radar: Things in Brief

PCAOB Charges Five Firms with Audit Committee Communications Failures. On July 28, the Public Company Accounting Oversight Board announced settled disciplinary orders sanctioning five audit firms for violating the Board's rules related to communications with audit committees. Three of the firms failed to obtain audit committee pre-approval in connection with providing audit or non-audit services to public company audit clients, in violation of the PCAOB's auditor independence rule. These firms, the sanctions to which they consented, and the nature of the violations are:

- BPM LLP – $50,000 civil money penalty and censure. The PCAOB's order alleges that BPM failed to obtain pre-approval from the audit committee to provide tax compliance services to an audit client.
- Plante & Moran, PLLC – $40,000 civil money penalty and censure. The PCAOB's order alleges that Plante & Moran failed to obtain pre-approval from the audit committee of one audit client to provide services in connection with the filing of comfort letters related to SEC registration statements. The order also alleges that Plante & Moran failed to obtain pre-approval from the audit committee of another audit client to provide tax return preparation services for two employees of the audit client.
- S. R. Snodgrass, P.C. – $35,000 civil money penalty and censure. The PCAOB's order alleges that Snodgress failed to obtain pre-approval from the audit committee to provide information technology consulting services to an audit client.

The other two firms failed to make and/or to document required audit committee communications, including communications concerning other accounting firms, in addition to the principal auditor, which participated in the audit. (SEC Chief Accountant Munter recently emphasized the importance of audit committee oversight of the participation of other firms. See SEC Chief Accountant Discusses Audit Committee Oversight of Other Auditors, April 2023 Update.) These firms, the sanctions to which they consented, and the nature of the violations are:

- Mancera, S.C. – $40,000 civil money penalty and censure. The PCAOB's order alleges that Mancera failed to inform an audit committee of the name, location, and planned responsibilities of nine other firms that would be participating in the audit.

- MSPC, Certified Public Accountants and Advisors, A Professional Corporation – $30,000 civil money penalty and censure. The PCAOB's order alleges that MSPC failed to communicate significant risks the firm had identified associated with revenue recognition and override of controls. The Board also alleges that the firm failed to document in its workpapers communications to the audit committee regarding the participation in the audit of another firm.

The press release announcing these cases includes this statement from PCAOB Chair Erica Williams:

> "Audit Committees play a critical role in helping protect investors, and the PCAOB will hold firms accountable for their part in making sure audit committees are appropriately informed. * * * Firms must be vigilant in preserving their independence, and part of that means making sure that services performed for issuer audit clients are pre-approved by their audit committees. At the same time, required disclosures are critical to ensure audit committees have the information they need to effectively oversee the auditor's work."

Advice for Audit Committee Chairs on Conducting Special Investigations. Audit committee chairs are often asked to conduct investigations of suspected financial frauds, corrupt payments, or other sensitive and complex matters, particularly those with financial reporting, accounting, internal control, or disclosure aspects. During the second quarter of 2023, Tapestry Networks, an independent firm supported by EY, convened the audit committee chairs of 100 large U.S. public companies to discuss oversight of special investigations. Oversight of Special Investigations, a publication in Tapestry's Viewpoints series, summarizes considerations regarding such investigations that audit committee chairs should be aware of, based on these sessions.

Tapestry's paper has three sections, mirroring the stages of an investigation:

- The preliminary inquiry. During the preliminary inquiry stage, key issues that must be addressed are deciding whether and when to launch a board-led investigation; determining who from the board should lead the investigation (e.g., the audit committee, a special committee, or the full board); and selecting legal counsel.

- Overseeing the investigation. Tapestry states that "[e]ffective oversight of investigations involves managing the investigation's scope and establishing a collaborative relationship with stakeholders connected to the investigation." The paper discusses the importance of properly scoping the investigation (e.g., creating a written work plan), ensuring timely and appropriate communications (e.g., with management, the board, the external auditor, and shareholders), and preparing for interactions with regulators.

- Concluding the investigation. Ending a special investigation "requires strategic planning, comprehensive assessment, and applying effort to improvement." Concluding a board-led investigation involves ensuring that the inquiry has met its original objectives and that the results can withstand scrutiny. In addition, the investigation should result in "forward-looking remediation [that] improves future resilience and governance" and in identifying and addressing the root cause of the matter.

The paper includes an appendix listing questions for audit committee chairs to consider in connection with special investigations.

IAASB Issues Proposed Sustainability Auditing Standard. On August 2, the International Auditing and Assurance Standards Board (IAASB) issued Proposed International Standard on Sustainability Assurance 5000, General Requirements for Sustainability Assurance Engagements (Proposed ISSA 5000). Proposed ISSA 5000 would provide a framework for third-party assurance on sustainability reporting and would serve as a comprehensive, stand-alone standard suitable for any sustainability assurance engagements. The comment period on the proposal is open until December 1, and the IAASB plans to issue a final standard before the end of 2024.

- Scope. The IAASB's web page for this project states that ISSA 5000 "will apply to sustainability information reported across any sustainability topic and prepared under multiple frameworks, including the recently released IFRS Sustainability Disclosure Standards S1 and S2." (Regarding these new standards, see ISSB Issues its Inaugural Disclosure Standards, July 2023 Update.) The information as to which assurance is provided must be prepared in accordance with a sustainability reporting framework, standard or other suitable criteria. The proposal defines "sustainability matters" as "Environmental, social, economic and cultural matters, including: (i) The impacts of an entity's activities, products and services on the environment, society, economy or culture, or the impacts on the entity, and (ii) The entity's policies, performance, plans, goals and governance relating to such matters."

- Profession agnostic. The IAASB notes that the proposed standard is "profession agnostic, supporting its use by both professional accountant and non-accountant assurance practitioners." While any type of assurance provider could issue an ISSA 5000 report, the standard would require practitioners to comply with relevant ethical requirements and apply a system of quality management at least as rigorous as required by the International Code of Ethics for Professional Accountants and by the IAASB's quality management standards.

- Principles-based. Proposed ISSA 5000 focuses on principles or outcomes rather than procedures or steps. The IAASB states that this "allows the assurance practitioner to apply their professional judgment in planning and performing the assurance engagement." The principles-based approach also "supports the scalability and comprehensiveness of the standard by limiting possible exceptions from the principles that apply and demonstrating how a requirement applies to all entities regardless of, for example, the type of entity, industry, or sector, and whether their nature and circumstances are less complex or more complex."

- Reporting. Proposed ISSA 5000 would be available regardless of how or where the sustainability information is reported and for either limited or reasonable assurance engagements.

While assurance over sustainability reporting is not currently required in the United States, the standards under which such assurance is available are likely to be on the agenda for an increasing number of audit committees. A recent study found that 64 percent of companies that report sustainability information also provide some level of third-party assurance over at least part of the information. See IFAC Issues Third Report on ESG Disclosure and Assurance, February-March 2023 Update. Further, if the SEC adopts its climate disclosure proposals, it will require auditors to provide assurance on GHG emissions disclosures for certain large companies, and the audited financial statements of all public companies will be required to include footnote disclosure on certain climate-related matters. See SEC Unveils its Climate Disclosure Proposals, March 2022 Update. Audit committees may therefore want to monitor standard setting in this area.

A New Auditor is Likely to Charge Less, But Miss More Financial Statement Errors. A study conducted by three researchers at the University of Texas at Austin finds that, when companies change auditors, the new auditor is likely to charge a lower audit fee, compared to the prior auditor. But the lower fee comes at a price. Fee discounting results from the incoming auditor

underestimating client risk, and audit quality suffers in the first year of the new engagement. "[W]e document that fee discounting by successor auditors can be associated with impaired audit quality. Consistent with discounting successor auditors initially under-assessing client risk, we find that larger fee discounts are associated with a greater likelihood that successor auditors allow misstatements [to] go undetected in the first year of the audit engagement * * * ." Nicholas J. Hallman, Minjae Kim, and Jaime J. Schmidt, Audit fee discounts following auditor changes: Do they occur and impair audit quality?

Other findings of this study include:

- Firm size matters. Audit fee discounts are about 14 percent larger when clients switch from a Big 4 to a non-Big 4 auditor. Switches between two non-Big 4 auditors only result in a discount of approximately six percent. However, "audit quality impairment associated with discounting is concentrated in changes between non-Big 4 auditors. * * * [L]arge fee discounts are relatively rare in the non-Big 4 audit market, but problematic when they do occur."

- Discounting affects both the financial statement audit and ICFR. In first-year audit engagements, "larger audit fee discounts are associated with an increased likelihood that misstatements go undetected, but are not associated with the likelihood that material weaknesses in internal controls over financial reporting (ICFR) are disclosed." The authors state that this suggests that "discounting auditors are either unaware of, or unwilling to report on, the elevated level of misstatement risk."

- Timing matters. Audit quality impairment due to discounting is more likely in auditor changes that occur after the first 100 days of the client's fiscal year. This is "consistent with auditors not having enough time to update their beliefs about client risk before issuing their first opinion."

- Discounting only affects quality in the first year. The study finds that, in a new auditor's second year, fee discounting is not associated with the failure to detect misstatements. Moreover, in the second year, there is an increased likelihood of disclosure of material ICFR weaknesses. This suggests that, while discounting auditors initially underestimate client risk when pricing new engagements, they "update their beliefs about (and adjust their procedures to address) the risk after gaining sufficient experience with the client."

The authors conclude with the observation that, while "concerns about the audit quality implications of audit fee discounting appear to be warranted, the risks are short-lived, concentrated among smaller audit firms, and appear to be related to underestimating client risk rather than compromised auditor independence." Audit committees might want to keep this study in mind when considering the possibility of changing auditors to capture a significant fee reduction.

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 blog posts include –

- NOCLAR: The PCAOB Proposes to Broaden the Auditor's Role (Dan Goelzer, July 12, 2023)

The blog is available here. You can follow @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.