Dan Goelzer

AUDIT COMMITTEE AND AUDITOR OVERSIGHT UPDATE

Update No. 85
October 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 Chief Accountant: When Assessing Risk, Look at the Big Picture

No Surprises, Please. 2022 PCAOB Conversations with Audit Committee Chairs

California Outflanks the SEC on Climate Disclosure

E.U. ESG Disclosure Requirements Will Affect Many U.S. Companies

Ready or Not: KPMG Finds that Few Companies are Prepared for ESG Assurance

Ineffective ICFR Ticked Up for the Second Straight Year in 2022

On the Update Radar: Things in Brief

PCAOB Adopts a New Confirmation Standard

Top Technology Risks that Keep Internal Audit Up at Night

The Audit Blog

The PCAOB Takes Aim at Negligent Auditors

SEC Chief Accountant: When Assessing Risk, Look at the Big Picture

SEC Chief Accountant Paul Munter has issued a statement discussing risk assessment. In The Importance of a Comprehensive Risk Assessment by Auditors and Management, Mr. Munter warned that, in some instances, "management and auditors appear too narrowly focused on information and risks that directly impact financial reporting, while disregarding broader, entity-level issues that may also impact financial reporting and internal controls." He urged taking "a holistic approach" to risk assessment.

Mr. Munter expressed particular concern about the tendency to treat problems as isolated incidents, rather than considering their significance as indicators of financial reporting risk or of weaknesses in

---

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.

internal control over financial reporting (ICFR). As examples of the kinds of incidents that may be mistakenly viewed as one-off events, he cites "a data breach in a system not part of ICFR, a repeat non-financial reporting-related regulatory finding classified as lower risk, a misstatement to the financial statements determined to be a revision restatement (i.e., 'little r'), or a counterparty risk limit breach." Management and auditors should guard against evaluating these types of occurrences "individually or rationalizing away potentially disconfirming evidence" and thereby concluding that such "matters do not individually, or in the aggregate, rise to the level of management disclosure or auditor communication requirements."

Against this background, the statement discusses three topics:

- Risk Assessment. Management needs to be alert to new or changing business risks that could impact internal controls or disclosure in periodic filings. "Management's risk assessment processes must comprehensively and continually consider * * * objectives, strategies, and related business risks; evaluate contradictory information; and deploy appropriate management resources to respond to those risks." Similarly, in performing its risk assessment, the auditor should consider public statements regarding changes in the company's "strategy, board composition, or other governance matters—and whether such statements contradict management's assessment of its control environment." If there are material inconsistencies between company disclosures and information obtained in performing the audit, the auditor should determine whether the disclosures "indicate a potential new or evolving business risk that could materially affect the financial statements or the effectiveness of ICFR."

- Entity-Level Controls. Management should evaluate whether the company has implemented processes and controls that can timely prevent or detect a material misstatement in financial statements. But that evaluation should not focus only on controls directly related to financial reporting. When evaluating control deficiencies that are "outside of an issuer's financial reporting objective," management and auditors should consider the root cause of the deficiency and whether it impacts ICFR. "For example, the root causes behind a regulator's findings related to enterprise-wide governance and controls, while not directly related to financial reporting control activities, could have an impact on management's ICFR conclusions due to their impact on the risk assessment and monitoring components of ICFR."

  Also, when assessing the severity of a control deficiency that is identified because of a misstatement, management and the auditor should consider, not just the identified misstatement, but also the magnitude of potential misstatement that could have resulted from the control deficiency. Mr. Munter refers to this as the "could factor" – the possibility that a control deficiency could have affected a large population of accounts or transactions. "In particular, when the root cause is an inadequate entity-level risk assessment process, the 'could factor' can extend to a wider population of potential misstatements beyond the identified misstatement."

- Reporting Obligations. In addition to disclosures related to ICFR evaluations and control changes, SEC filings are required to discuss material factors that make an investment in the company speculative or risky. Management's risk assessment process, which should include contradictory information, may identify factors that should be included in this disclosure. Moreover, some business risks may also impact financial statement disclosures.

  Auditors also have a role in communicating with investors regarding risk. This takes two forms – disclosure in the auditor's report of critical audit matters (CAMs) and the possible inclusion in the report of an emphasis-of-matter paragraph. If the auditor determines that a business risk represents a risk of material misstatement to the financial statements and discusses the risk with the audit committee, the business risk may be a CAM that must be described in the auditor's report. Auditors may also use an emphasis-of-matter paragraph "to highlight any matter relating to the financial statements and disclosures, which could include matters related to an issuer's objectives, strategies, and related business risks * * * ."

Comment: While Mr. Munter's statement is aimed primarily at management and auditors, audit committees should also review the concepts he discusses. The statement signals that the SEC expects companies and auditors to take a broad approach to risk assessment. Audit committees may want to discuss with both management and the auditor their reactions to the statement and how it relates to their respective risk assessment procedures.

No Surprises, Please. 2022 PCAOB Conversations with Audit Committee Chairs

Audit committee chairs are worried about the impact of the "great resignation" on their engagement team and on the financial reporting staff at their company. And they don't like inconsistent or last-minute auditor communications which could lead to surprises during the audit. Those are two of the conclusions that can be drawn from the Public Company Accounting Oversight Board (PCAOB) annual report on its inspection staff's discussions with audit committee chairs.

Each year, the PCAOB invites the audit committee chairs of the U.S. public companies it has selected for inspection to participate in "unstructured, substantive conversations in an informal setting" with the staff of the Division of Registration and Inspections. In 2022, 211 audit committee chairs accepted this invitation; 85 percent of these chairs had not previously participated in dialogue with the PCAOB inspections staff. Spotlight: 2022 Conversations with Audit Committee Chairs (2022 Conversations Report) summarizes these discussions. This is the fourth year the PCAOB has published the results of the inspection staff's interactions with audit committee chairs. For last year's report, see The PCAOB Reports on its 2021 Conversations with Audit Committee Chairs, March 2022 Update.

The 2022 Conversations Report discusses five recurring themes that emerged from these conversations:

- Staffing. Concern about the impact of turnover (the "great resignation") on both financial reporting and auditing was a frequent theme. Audit committee chairs noted that both the number of CPAs at the issuer responsible for financial reporting and the level engagement team staffing and experience may have impacted audit efficiency.

- Covid-19. Most audit committee chairs did not believe the pandemic had significantly impacted their audit. However, many thought that an audit performed in a remote or hybrid environment presents elevated risk, particularly regarding controls and cybersecurity, and requires heightened supervision and review. On the positive side, some noted that remote and hybrid auditing resulted in more frequent communications between the auditor and the audit committee.

- Communications. Audit committee chairs value early, ongoing, and proactive communication with their auditors. Many interviewees felt that their auditor was meeting these expectations. However, several complained of "inconsistent or last-minute communication" and would like to see improvement to "minimize the possibility of surprises throughout the audit."

- Critical Audit Matters. For the past several years, auditors have been required to discuss critical audit matters (CAMs) in the audit report. (CAMs are challenging or judgmental aspects of the audit that were discussed with the audit committee.) Audit committee chairs were generally pleased with their auditor's preparation for CAMs-related discussions and did not cite significant disagreements over what should be included as a CAM in the auditor's report. However, "a small percentage of audit committee chairs questioned whether CAMs reporting is becoming a generic compliance exercise, sometimes resulting in 'boilerplate' language provided by the auditor."

- Information Outside the Financial Statements. The PCAOB staff asked audit committee chairs whether they were discussing with their auditor information outside of the financial statements, such as non-GAAP financial measures. While the use of non-GAAP measures varies from

industry to industry, ensuring the accuracy of any non-GAAP information disclosed was of "almost universal importance" to audit committee chairs. In addition, many chairs indicated that they are discussing with their auditor financial statement, internal control, and assurance implications of potential climate-related disclosure requirements. (As discussed in prior Updates, the SEC's climate disclosure proposals would both impact the content of the financial statements and require independent attestation of greenhouse gas disclosures outside the financial statements.)

Comment: The 2022 Conversations Report provides insight as to the current views and concerns of audit committee chairs. In addition, an audit committee chair who is contacted by the PCAOB inspection staff as part of an inspection of the company's auditor may want to review the 2022 Conversations Report and prior reports on these dialogues as a way of preparing for the interview.

California Outflanks the SEC on Climate Disclosure

California Governor Newsom has signed legislation that will require many U.S. companies to disclose their scope 1, 2, and 3 greenhouse gas (GHG) emissions and to prepare an annual climate-related financial risk report. The Climate Corporate Data Accountability Act (CCDAA) and the Climate-Related Financial Risk Act (CRFRA) are estimated to apply to as many as 10,000 companies that do business in California, including a significant share of SEC reporting companies. The SEC has also proposed extensive climate disclosure requirements, although it is uncertain when the Commission will take final action on its proposals. See SEC Unveils its Climate Disclosure Proposals, March 2022 Update. In recent Congressional testimony, SEC Chair Gensler suggested that the California law may make it easier for the SEC to act on its proposal: "That may change the baseline. If those companies were reporting to California, then it would be in essence less costly [to comply with an SEC GHG reporting requirement] because they'd already be producing that information." SEC chief says new California law could 'change baseline' for coming SEC climate rule, Reuters, September 27, 2023

The California legislation is a major milestone in mandatory in U.S. public company climate disclosure and may have national ramifications. However, it is difficult to fully assess the likely effects at this early stage. In his statement on the signing of the CCDAA, Governor Newsom noted that the implementation deadlines "are likely infeasible" and that the GHG reporting protocol specified in the new law could result in inconsistent reporting. He directed his staff to work with the California Legislature to address these issues next year. He also expressed concern about "the overall financial impact of this bill on businesses" and instructed the administrative agency that will oversee the law "to make recommendations to streamline the program." Governor Newsom issued a similar statement with respect to CRFRA. Accordingly, although the bills have been signed into law, their final scope and timing appears to still be in flux.

The Climate Corporate Data Accountability Act

CCDAA requires the California State Air Resources Board (CARB) to adopt regulations by January 1, 2025, requiring "reporting entities" to annually report their scope 1, scope 2, and scope 3 GHG emissions. A reporting entity for CCDAA purposes is any U.S. public or private entity with annual global revenue exceeding $1 billion that does business in California. The concept of doing business in California is not defined in either CCDAA or CRFRA.

CARB is directed to structure the GHG reporting regulations "in a way that minimizes duplication of effort" and to permit reporting entities to submit reports prepared to meet other national and international reporting requirements, "as long as those reports satisfy all of the requirements" of CCDAA. Reporting will be made publicly to a nonprofit emissions reporting organization under contract with CARB.

The legislation defines scope 1, 2, and 3 emissions as follows:

- "Scope 1 emissions" means all direct greenhouse gas emissions that stem from sources that a reporting entity owns or directly controls, regardless of location, including, but not limited to, fuel combustion activities.

- "Scope 2 emissions" means indirect greenhouse gas emissions from consumed electricity, steam, heating, or cooling purchased or acquired by a reporting entity, regardless of location.

- "Scope 3 emissions" means indirect upstream and downstream greenhouse gas emissions, other than scope 2 emissions, from sources that the reporting entity does not own or directly control and may include, but are not limited to, purchased goods and services, business travel, employee commutes, and processing and use of sold products.

Scope 3 disclosure requirements are controversial because they require estimation and reliance on information from third parties. Significantly, the California law is broader than the SEC's proposed GHG reporting regime in that the SEC proposal would only require Scope 3 emissions disclosure if material or if the company has disclosed a Scope 3 emissions target.

CCDAA disclosure will begin in 2026 with respect to FY 2025 scope 1 and scope 2 emissions and in 2027 with respect to FY 2026 scope 3 emissions. As noted above, however, Governor Newsom apparently intends to ask the Legislature to extend these deadlines.

The CCDAA also requires an independent audit of GHG disclosures. It provides that reporting entities must "obtain an assurance engagement performed by an independent third-party assurance provider on all of the reporting entity's scope 1 emissions, scope 2 emissions, and scope 3 emissions." These assurance engagements "shall be performed at a limited assurance level beginning in 2026 and at a reasonable assurance level beginning in 2030."

The Climate-Related Financial Risk Act (CRFRA)

CRFRA requires covered entities to prepare a biennial climate-related financial risk report. The CRFRA is broader in scope than the CCDAA: A covered entity for CRFRA purposes would be any U.S. public or private entity with annual global revenue exceeding $500 million that does business in California.

CRFRA reports must disclose (1) the company's climate-related financial risks, in accordance with the 2017 recommendations of the Task Force on Climate-Related Financial Disclosures, and (2) measures the company has adopted to reduce and adapt to such climate-related financial risks. The reporting requirement may be satisfied by preparing a publicly accessible report that includes climate-related financial risk disclosure information in compliance with an exchange listing standard, a requirement of federal law, or the standards of the International Sustainability Standards Board.

Companies subject to CRFRA are required to submit their climate-related financial risk report to the state and to make the report available to the public on a website. The first biennial report is due on or before January 1, 2026, although, as noted above, this date may be extended.

Comment: These new California laws are likely to be subject to legal challenges and possibly to legislative revisions before they take effect. However, whatever their ultimate fate, the legislation serves as a warning that mandatory climate reporting is likely to become a reality for most, if not all, public companies (and many private companies as well) in the near future. Audit committees should be discussing with management its plans to generate the information to comply with likely disclosure requirements. For example, GHG emissions disclosure is a feature of virtually all climate change reporting frameworks, including both the CCDAA and the SEC proposal. Companies that are not currently collecting this information should consider how they will do so and what new controls and procedures will be needed to assure reliability, particularly as to scope 3 emissions. Climate disclosures, voluntary or mandatory, will almost certainly be a fertile source for litigation and regulatory challenge, and audit committees should be making sure that management is preparing to meet these new responsibilities.

E.U. ESG Disclosure Requirements Will Affect Many U.S. Companies

The SEC's climate-change proposal and the new California climate disclosure laws are not the only ESG disclosure requirements to which U.S. public companies may be subject. The European Union's ESG reporting regime will also affect many U.S. companies. To provide basic guidance on the application of the E.U.'s Corporate Sustainability Reporting Directive (CSRD) to companies based in the United States, Deloitte has released #DeloitteESGNow - Frequently Asked Questions About the E.U. Corporate Sustainability Reporting Directive.

Background

Adopted in 2022, the CSRD replaces the E.U.'s Non-Financial Reporting Directive. The CSRD aims to improve the quality and consistency of sustainability reporting by companies subject to E.U. disclosure requirements. The CSRD is part of the EU's efforts to achieve its climate and environmental goals and to foster corporate transparency and accountability. The CSRD is broad in scope, and many U.S. companies that have affiliates, or do business, in the European Union will be subject to its requirements. In addition, U.S. companies that are not directly subject to CSRD disclosure have customer or supplier relationships with reporting entities and may be asked to provide information so that the reporting entity can comply.

On July 31, the European Commission adopted the European Sustainability Reporting Standards (ESRS). These standards provide guidance for companies that are required to make ESG disclosures under the CSRD. The ESRS specifies the content and format of CSRD sustainability reports, which must include both qualitative and quantitative information, as well as forward-looking and historical data. The standards also introduce a materiality assessment process for companies to identify the most significant sustainability issues for their business and stakeholders. The ESRS covers 12 topics that are relevant for sustainability reporting, including climate change, biodiversity, human rights, workers in value chain, and business conduct. The reporting requirements will be phased in over time for different companies, depending on their size and previous reporting obligations.

Deloitte Q&As

Deloitte's paper addresses thirteen questions related to the application of the CSRD to U.S. companies. Six examples of these questions, along with a brief overview of Deloitte's responses, include –

- Question 1: How does the CSRD affect U.S. companies? Deloitte describes the criteria for determining whether a U.S. companies will be subject to CSRD. These criteria are complex and will require careful analysis in many cases. In very broad terms, the CSRD will apply to "large" (as defined) non-E.U. companies (including subsidiaries of non-E.U. parents) with securities listed on an E.U.-regulated market and to certain companies based outside of the E.U. that generate "net turnover" in the EU exceeding specified thresholds.

- Question 2: When will U.S. companies be affected by the CSRD, and what if a company is on an off-calendar reporting timeline? The CSRD will apply to in-scope U.S. companies in stages. In 2024, only large U.S. companies that are listed on an E.U.-regulated market and that have more than 500 employees will be subject to the CSRD. Starting in 2025, all large U.S. companies that are listed on an E.U.-regulated market will be subject to the CSRD. In 2026 and 2028, additional U.S. companies will come into the CSRD, including those captured by the net turnover test.

- Question 5: How does the CSRD compare with the SEC's proposed climate disclosure requirements? "The CSRD will require disclosure and assurance on a much broader suite of ESG topics than would the SEC's proposed rule on climate-related disclosures. The CSRD will include requirements for non-climate-related environmental topics and various social topics, while

the SEC's proposed rule on climate-related disclosures would only mandate disclosures specific to climate impacts and risk."

- Question 6: Will non-E.U. companies be permitted to use other standards instead of the ESRS? Which sustainability reporting standards are most likely to be deemed "equivalent" to ESRS for use by non-E.U. companies? Is the proposed SEC climate disclosure rule expected to be eligible for equivalence? The Europe Commission has indicated that it will allow in-scope non-E.U. companies to use sustainability standards equivalent to the ESRS. However, no decisions have yet been announced as to which standards will be deemed equivalent.

- Question 10: Which disclosures will be subject to assurance, and what level of assurance is required? Companies within the scope of the CSRD will be required to seek limited assurance over their compliance with the sustainability reporting standards from an independent third-party assurance provider. Reasonable assurance may be required in the future.

- Question 13: What are some initial steps that companies can take to start preparing for CSRD compliance? U.S. companies should assess whether they are within the scope of the CSRD and, if so, their reporting timeline. These determinations may require the assistance of legal counsel. Companies that will be subject to CSRD disclosure "should evaluate and strengthen their processes and controls over sustainability information so they can be 'assurance ready.'"

Comment: Audit committees of companies with any level of contact with the E.U. should make sure that management is considering how the CSDR may affect the company. Even if the company is not within the scope of the directive, thought should be given to whether customers that are subject to the directive are likely to request information to aid in their compliance. Companies that will be subject to CSRD reporting should begin considering how their controls and disclosure procedures will need to be modified to generate the necessary information and to permit their financial statement auditor, or some other independent third party, to provide the required assurance. Deloitte's Q&A paper provides a good introduction to the complex issue of the CSRD's impact on U.S. companies.

Ready or Not: KPMG Finds that Few Companies are Prepared for ESG Assurance

KPMG has released Road to Readiness, the inaugural report on the KPMG ESG Assurance Maturity Index. The Maturity Index, measured on a scale of 0−100, gauges "the relative maturity of a company's ESG reporting program in order to assess its assurance readiness" – that is, readiness to obtain third-party assurance on its ESG reporting. For 2023, KPMG finds that the average ESG assurance readiness score for U.S. companies is 49.4. The averages for companies headquartered in other high-scoring countries are France (50.4), Japan (50.0), Brazil (43.1), and China (43.0).

The Maturity Index is based on survey responses concerning five areas, or pillars, of readiness for third-party assurance. The pillars are (1) governance, (2) skills, (3) data management, (4) digital technology, and (5) value chain. To measure progress on these pillars, KPMG surveyed senior executives and board members at 750 companies. The mean annual revenue of companies represented in the survey was US$15.6B.

In addition to the overall readiness scores, other findings of the 2023 report include:

- Only 25 percent of companies believe they have the ESG policies, skills, and systems in place to be ready for independent ESG data assurance.

- Companies with US$10 billion or more in revenue tend to be more ESG assurance ready, with an average score of 56.3, compared to companies with revenue of between US$5 and 10 billion (45.3 average score) and those with revenue under US$5 billion (41.7 average score).

- Fifty-two percent of respondents are already obtaining some level of external assurance over their current ESG disclosures. Of those, 14 percent are obtaining reasonable assurance and 16 percent are obtaining limited assurance over ESG disclosures that will be required under "incoming regulations."

- At firms that are less ready for ESG assurance, 58 percent of CEOs and board members say it is challenging to balance ESG assurance goals with the shareholder profit expectations. Specific challenges to preparing for ESG assurance cited by respondents included high initial costs/ inefficient budget (44 percent); lack of internal skills and experience (44 percent); lack of clarity/ evolving regulations (42 percent); inadequate supplier ESG performance (42 percent); insufficient IT/digital solutions (36 percent); and lack of clear metrics/measurement tools (36 percent).

- About half of all respondents said that ESG assurance has the potential to increase market share because assured ESG data "helps to give companies greater credibility with investors and all stakeholders potentially increasing brand loyalty." Other potential benefits cited by respondents included increased customer satisfaction (46 percent), greater innovation (49 percent), and decreased operational costs (44 percent).

The report discusses five "critical steps" that companies are taking to become ESG assurance ready: (1) Determine applicable ESG reporting standards; (2) Build robust ESG governance and develop the right skills; (3) Identify the applicable ESG disclosures and data requirements across functions; (4) Digitize ESG data processes and ensure high quality data; and (5) Work with the value chain to collect ESG information.

Comment: ESG assurance readiness is becoming an important issue for many audit committees. As noted in this and other studies, many companies already obtain external assurance over at least some portion of their ESG disclosures. As more companies obtain assurance, investor and customer pressure on their peers to follow suit increases. Moreover, virtually all public companies will become subject to mandatory ESG assurance requirements within the next few years. Both the proposed SEC climate disclosure requirements (see SEC Unveils its Climate Disclosure Proposals, March 2022 Update) and the legislation enacted in California (see California Outflanks the SEC on Climate Disclosure in this Update) require some level of assurance over greenhouse gas emissions disclosures. In addition, companies subject to the E.U.'s new ESG rules (see E.U. ESG Disclosure Requirements Will Affect Many U.S. Companies, in this Update) will be required to obtain assurance over certain disclosures. Audit committees should be discussing with management the steps necessary for the company to become ESG assurance ready.

Ineffective ICFR Ticked Up for the Second Straight Year in 2022

Ideagen Audit Analytics has released SOX 404 Disclosures: A 19-Year Review, its annual analysis of disclosures under Section 404 of the Sarbanes-Oxley Act. AA found that, in FY 2022 the number of companies filing a management assessment that reported ineffective internal control over financial reporting (ICFR) increased for the second straight year – rising from 1,678 in 2021 to 1,740 in 2022, a 4 percent increase. Nearly one quarter (24.4 percent) of public companies reported that their controls were not effective. Since the reporting universe grew, the percentage of companies that filed an adverse ICFR disclosure during FY2022 was however slightly lower than in the prior year. The number of ICFR disclosures filed by special purpose acquisition companies (SPACs) seems to be a large factor in the increasing number of adverse ICFR disclosures. AA notes that SPACs comprised nearly 40 percent of all first-time adverse ICFR disclosures in FY2022.

AA also found that the total number of adverse ICFR auditor attestations rose to 257 in FY2022, a 21 percent increase over 2021. (Auditor ICFR reporting is only required for larger companies -- accelerated filers -- while all public companies must file a management report on ICFR effectiveness.) The

percentage of companies subject to the audit requirement that received an adverse ICFR auditor attestation during FY2022 rose from 6.2 percent in 2021 to 7.6 percent, the highest rate since 2007. Despite the increase in 2022, both the number and percentage of adverse auditor reports remained far below their all-time peaks of 489 adverse auditor reports in 2005 and 15.8 percent of all auditor reports issued in 2004.

For a discussion of last year's AA report on Section 404 reporting, see Ineffective ICFR is More Common; Staff Shortages May be the Cause, August 2022 Update. That item also contains a background description of the Section 404 reporting requirement. In comparing the 2022 report to prior AA reports, it should be noted that AA appears to have adjusted the statistics for 2021 and earlier years in the current report from those that originally appeared in those reports.

2022 SOX 404 ICFR Effectiveness Disclosures

In 2022, 7,139 management ICFR assessments were filed, up from 6,826 in 2021. There were 3,375 auditor's reports on ICFR, a decrease from 3,409 the prior year. In 2022, 3,701 companies filed only a management assessment of ICFR, up from 3,419 management assessment-only filers in 2021. With respect to the reporting of ineffective controls in these filings, AA found:

- Management reports. The number of adverse ICFR management reports increased to 1,740 in 2022, up from 1,678 in 2021. As noted above, 24.4 percent of all 2022 management reports were adverse, down slightly from 24.6 percent in 2021.

- Auditor attestations. The number of adverse ICFR auditor attestations increased to 257 in 2022, up from 213 in 2021. 7.6 percent of all attestations were adverse, compared to 6.2 percent in 2021. Since the SOX ICFR reporting requirements took effect, 2010 had the lowest percentage of adverse auditor attestations (3.5 percent) and 2004 had the highest (15.8 percent).

- Management only reports (i.e., reports filed by companies not required to obtain an auditor's opinion on ICFR effectiveness). In 2022, the number of adverse ICFR management-only reports increased to 1,477. This represents 39.9 percent of all management-only reports filed for the year, down from 42.7 percent in 2021. The number of companies that filed a management-only in 2022 was 3,701 and increase from 3,419 in 2021.

- First-time filers. For companies filing their first management ICFR assessment in 2022, 41.8 percent reported that their controls were ineffective, a decrease from 61.9 percent in 2020. AA observes that on average, "an ICFR disclosure is three times more likely to be classified as an adverse disclosure during a first-time assessment." Similarly, 28 percent of first-time auditor ICFR attestations (i.e., opinions filed by companies that had newly become accelerated filers) reported ineffective controls. This was a decrease from the all-time high of 29.6 percent of adverse first-time auditor reports in 2021.

Nature of Control Weaknesses and Related Accounting Issues

Adverse auditor's reports and management assessments are required to describe the reasons controls were ineffective. In FY2022, the most common internal control issue cited as contributing to ineffective ICFR in management reports was the need for more highly trained accounting personnel. The most common issue cited in adverse auditor reports was information technology, software, and/or security issues. Other findings of interest include:

- Management reports. In management reports, the top five contributors to ineffective controls in 2022 were inadequate accounting personnel resources (cited in 67.6 percent of adverse reports); insufficient segregation of duties/personnel (cited in 57.8 percent of adverse reports); inadequate disclosure controls (cited in 35.8 percent of reports); information technology (cited in 22.4 percent of reports), and non-routine transaction controls (cited in 16.7 percent of reports). For companies

filing only a management assessment, the top three issues were the same, but an inadequate audit committee replaced information technology as the fourth most referenced weakness.

The top five accounting issues in adverse management reports were deficiencies in approach, understanding, or calculation associated with revenue recognition (cited in 9 percent of adverse disclosures); debt and equity (cited in 8.3 percent of disclosures); accounts receivable, investments and cash (cited in 6.8 percent of disclosures); subsidiary/affiliate issues (cited in 5.5 percent of disclosures); and liabilities (cited in 5.4 percent of disclosures). For companies filing only a management assessment, the top five accounting issues were the same, although debt and equity issues came in first while revenue recognition was second. The frequency of ICFR challenges related to debt v. equity accounting presumably stems from the substantial number of SPACs that restated their financials to correct the accounting for debt and warrants.

- Auditor attestations. In 2022 adverse auditor's reports, the five most frequently referenced sources of control weaknesses were information technology (cited in 54.5 percent of disclosures); accounting personnel resources (cited in 53.7 percent of disclosures); inadequate disclosure controls (cited in 39.7 percent of disclosures); segregation of duties) (cited in 39.3 percent of disclosures); and non-routine transactions (cited in 14.4 percent of disclosures). The top five accounting issues cited in adverse auditor ICFR assessments were revenue recognition (23.3 percent); accounts receivable, investments and cash (12.1 percent); inventory, vendor, cost of sales (11.7 percent); long-term assets (11.7 percent); and liabilities (10.1 percent).

Comment: The increases in the number of adverse management and auditor ICFR reports seem to have two primary causes. First, difficulty in hiring qualified accounting personnel and the related challenge of maintaining segregation of duties in the face of staffing shortages had a negative impact on control effectiveness. See, e.g., Material Weaknesses are Increasing and an Accountant Shortage May Be to Blame, August-September 2023 Update. Second, there has been an increase in the number of new reporting companies, driven by the popularity of SPACs. These companies typically have fewer resources to devote to controls.

Oversight of the adequacy of internal control is one of the most fundamental responsibilities of a public company audit committee. Audit committees may want to probe whether frequently cited control weaknesses described in the AA report are affecting their company's controls. Separate from the disclosure and audit requirements of SOX Section 404, 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. The SEC typically charges violations of this requirement in cases involving financial reporting matters. See SEC Accounting Enforcement Continues Apace, July 2023 Update.

On the Update Radar: Things in Brief

PCAOB Adopts a New Confirmation Standard. On September 28, the Public Company Accounting Oversight Board (PCAOB) adopted a new standard on the auditor's use of confirmations. See The Auditor's Use of Confirmation, and Other Amendments to PCAOB Standards. The new standard, which the Board describes as modernizing and strengthening the existing confirmation requirements, was originally proposed for comment in 2010 and reproposed with changes in 2022. See PCAOB Proposes to Modernize Confirmations, January 2023 Update. Assuming SEC approval, the new standard and related amendments to existing standards will take effect for audits of financial statements for fiscal years ending on or after June 15, 2025.

Confirmation is the process of verifying information about one or more financial statement assertions with a third party. Key features of the new confirmation standard include:

- Cash and cash equivalents. For cash and cash equivalents held by a third party, the auditor should perform confirmation procedures or otherwise obtain relevant and reliable audit evidence by directly accessing information maintained by a knowledgeable external source. The current standards do not address cash confirmation.

- Confirmation of accounts receivable. For accounts receivable that arise from the transfer of goods or services to a customer or a financial institution's loans, the auditor should perform confirmation procedures or otherwise obtain relevant and reliable audit evidence by directly accessing information maintained by a knowledgeable external source. (Confirmation of accounts receivable has been presumptively required in the United States since 1939.) The new standard recognizes that there may be situations in which the auditor determines that confirmation or access to third party information is not feasible. In those cases, the auditor should document that determination and instead "should obtain external information indirectly by performing other substantive procedures, including tests of details." As discussed below, the auditor will also be required to communicate with the audit committee when it determines not to confirm accounts receivable, if accounts receivable is a significant audit risk.

- Negative confirmations. The standard states that the use of negative confirmation requests alone does not provide sufficient appropriate audit evidence. (A negative confirmation request is one in which the auditor requests a confirmation response only if the confirming party disagrees with the information provided in the confirmation request.) The standard includes examples of situations where the auditor may use negative confirmation requests to supplement other substantive audit procedures.

- Limited use of internal audit in the confirmation process. Under the new standard, the auditor must maintain control over the confirmation process to minimize the likelihood that information exchanged between the auditor and the confirming party is intercepted or altered. Specifically, the "auditor should (i) select the items to be confirmed, (ii) send confirmation requests, and (iii) receive confirmation responses." By implication, therefore, the auditor cannot delegate any of these three functions to the company's internal audit staff. A footnote to the standard states that the auditor "may use internal auditors to provide direct assistance in other aspects of the confirmation process."

- Performing Alternative Procedures. The standard identifies situations in which alternatives to confirmation should be performed by the auditor and includes examples of such alternative procedures.

The 2022 confirmation proposal included a requirement that the auditor communicate with the audit committee whenever the auditor determined that the presumption to confirm accounts receivable had been overcome and the auditor intended to use alternative procedures. Some commenters objected to this provision on the grounds that the requirement to communicate with the audit committee should be limited to situations in which accounts receivable presented a significant risk. The final standard addresses these concerns by requiring that the auditor communicate with the audit committee about the auditor's response to significant risks associated with cash or accounts receivable when the auditor did not perform confirmation procedures or otherwise obtain audit evidence by directly accessing information maintained by an external source.

Top Technology Risks that Keep Internal Audit Up at Night. Chief audit executives (CAEs) and IT audit leaders see cybersecurity as the top technology risk their companies face over the next year, followed by risks associated with third parties and vendors. Those are the findings of Navigating A Technology Risk-Filled Horizon, the eleventh annual Global Technology Audit Risks Survey conducted by consulting firm Protiviti and The Institute of Internal Auditors (IIA). Protiviti and IIA surveyed 559 IT professionals on the technology risks their companies face over the next 12 months and over the longer term.

Roughly half of the respondents (258) identified as CAEs or as IT Audit Directors. Looking only at the responses of this subset, the technology threat risks identified as at the highest level (5 or 4 on a scale of 1-5) in the next 12 months were:

- Cybersecurity (82 percent). Not surprisingly, 82 percent of CAES and technology audit leaders consider cybersecurity a high-risk area. (Seventy-five percent of all respondents cited cybersecurity as a top risk.)

- Third party/vendors (67 percent). The survey reports states: “Global events such as supply chain disruptions and regulatory changes, combined with the increased use of cloud services and other outsourced IT functions, have amplified the importance of vetting third-party providers. This screening extends beyond cost effectiveness to encompass compliance with security and data protection standards.”

- Data governance & integrity (64 percent). Data governance and integrity refers to the risks related to maintaining accurate, consistent, and reliable enterprise-wide data. The report observes that “[p]roper data governance is not just a compliance requirement -- it also represents the foundation for successful digital transformations and AI initiatives.”

- Transformations & systems implementations (62 percent). These threats include disruptions, unmet requirements, data loss, and other risks arising from major business or IT changes.

- IT talent management (60 percent). Protiviti/IAA describe IT talent management and the perceived threats associated with attracting, developing, and retaining skilled technology personnel as “in the middle of the pack compared to other risks.”

Only 28 percent of all respondents identified artificial intelligence and machine learning (including generative AI) as significant threat risk in the coming year. However, 54 percent view AI systems as a substantial risk in the next two to three years. CAEs and IT Audit Directors were somewhat more concerned about AI threats, with 33 percent of those respondents selecting AI as a significant near-term risk area.

A section of the survey report headed Protiviti Commentary offers this advice:

> “If you take only one action based on the findings of this research, consider increasing the frequency of your technology audits. If you can make another move, consider deploying (or increasing) the use of data analytics on technology audits.
>
> “These two activities correspond to a wide range of positive technology audit outcomes. These outcomes include more timely snapshots and deeper insights into both traditional and newly relevant technology risks. Additionally, they contribute to improved organizational preparedness and technology audit proficiency to address cybersecurity, regulatory compliance, data privacy and compliance, data governance, third-party risk management (TPRM), IT talent management, AI-related risk management, and more.”

CAEs typically report to the audit committee. Audit committees may want to consider using this report as a basis for discussion with their internal audit head concerning how he or she perceives the company's top technology risks in the near and medium term and what steps can be taken to address such risks.

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. The blog is available here. Recent posts include –

- The PCAOB Takes Aim at Negligent Auditors (Dan Goelzer, October 25, 2023)

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.