Dan Goelzer

AUDIT COMMITTEE AND AUDITOR OVERSIGHT UPDATE

Update No. 95
November 2024

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

In This Update

PCAOB Adopts Pared Back Engagement Performance Metrics and Audit Firm Reporting Rules

On November 21, the Public Company Accounting Oversight Board adopted rules that will require registered accounting firms to disclose performance metrics regarding their larger audit engagements. The Board also adopted expanded firm operational and financial condition reporting. The Board proposed these

---

Dan Goelzer is a retired partner of Baker McKenzie, a major international law firm. He chairs a Big Four accounting firm's Audit Quality Advisory Council. From 2017 to July 2022, Dan was a Sustainability Accounting Standards Board member. The SEC appointed him to the Public Company Accounting Oversight Board as one of its founding members, and he served on the PCAOB from 2002 to 2012, including as Acting Chair from 2009 to 2011. Dan was on the Securities and Exchange Commission's staff for 16 years and served as SEC General Counsel from 1983 to 1990.

new requirements in April 2024 (see PCAOB Proposes Engagement Metrics and Audit Firm Operational and Financial Reporting, April 2024 Update) but they attracted critical comments from accounting firms and audit committees. In response to the comments, the Board eliminated some aspects of the proposals from the final requirements and modified others, although the fundamentals of the new disclosure regimes were not changed.

In the press release announcing the adoption of the new disclosures, PCAOB Chair Erica Y. Williams said: "The new requirements we are adopting today will make PCAOB oversight more effective and equip investors, audit committees, and others with clear, consistent, and actionable data related to audit firms and the engagements they perform." As Chair Williams's statement indicates, one of the Board's main justifications for both sets of new requirements is that the disclosures will provide audit committees with useful additional information to aid in their oversight and evaluation of the auditor.

Firm and Engagement Metrics

The new rules will require PCAOB-registered public accounting firms that audit accelerated filers or large accelerated filers to publicly report eight metrics relating to specific audit engagements or to the firm's audit practice. (In general, accelerated filers are companies with a public float between $75 and $700 million, while large accelerated filers are companies with a public float of $700 million or more.) Most of the metrics call for information at both a firm level and an engagement level, while several require only firm-level reporting. These eight metrics are:

1. Partner and Manager Involvement. Hours worked by senior professionals relative to more junior staff across all of the firm's large accelerated and accelerated filer engagements and on the audited company's engagement.

2. Workload (firm level only). For senior professionals who incurred hours on large accelerated or accelerated filer engagements, average weekly hours worked on a quarterly basis, including time attributable to all engagements, administrative tasks, training, and all other matters.

3. Training Hours for Audit Personnel. Average annual training hours for partners, managers, and staff of the firm, combined, across the firm and on the audited company's engagement.

4. Experience of Audit Personnel. Average number of years worked at a public accounting firm (whether or not PCAOB-registered) by senior professionals across the firm and on the audited company's engagement.

5. Industry Experience. Average years of experience of senior professionals in key industries audited by the firm at the firm level and in the audited company's primary industry at the engagement level.

6. Retention of Audit Personnel (firm-level only). Continuity of senior professionals (e.g., the impact of departures and reassignments) across the firm.

7. Allocation of Audit Hours. Percentage of hours incurred prior to and following an issuer's year-end across the firm's large accelerated and accelerated filer engagements and on the audited company's engagement.

8. Restatement History (firm-level only). Restatements of financial statements and management reports on internal control over financial reporting that were audited by the firm over the past three years.

Firms that serve as the lead auditor for at least one accelerated filer or large accelerated filer will be required to report the firm-level metrics annually on a new Form FM. For individual accelerated filer and large accelerated filer engagements, the engagement-level metrics must be reported on Form AP. Form AP, which must be filed for each public company engagement, will be renamed "Audit Participants and Metrics." In addition to the required metrics, firms will be allowed (but not required) to include a narrative

discussion to provide context and explanation for the metrics on both Form FM and Form AP. This narrative may not exceed 1000 characters (roughly 175 words) for each metric.

The final firm and engagement metrics differ from the April 2024 proposal in several respects. Among other things, proposed metrics relating to the use of specialists and shared service centers, quality performance ratings, internal monitoring, and audit hours devoted to risk areas were eliminated. The metric in the final rules related to training hours was added. In addition, the Board revised the terms of several of the metrics (e.g., the firm's restatement history was reduced from five to three years) and increased the length of the optional narrative explanation of metrics from 500 characters to 1000.

Firm Reporting

The Board also expanded the information that PCAOB-registered accounting firms must provide in their public annual reports (PCAOB Form 2) and in special reports (PCAOB Form 3) that must be filed when certain events occur (e.g., a change in the firm's name or criminal or regulatory proceedings against a partner or principal). Firm reporting will increase in six areas:

1. Financial Information.

    a. Registered firms will be required to include additional fee information in their annual report on Form 2. Firms will be required to report (1) the dollar amount (not just percentages, as currently required) of fees billed to issuer audit clients for audit services, other accounting services, tax services, and non-audit services; (2) fees billed to all clients for services; and (3) fees billed to broker-dealer audit clients. The Board retained the existing provision allowing firms to indicate whether they have estimated fee amounts and to describe the reasons for doing so.

    b. The largest registered firms will also be required to confidentially submit financial statements to the PCAOB, although those statements will not be required to be prepared in accordance with generally accepted accounting principles (GAAP). The financial statement requirement will apply to firms that issue audit reports for more than 200 public companies and have more than 1,000 personnel.

2. Governance Information. Registered firms will be required to report additional information regarding their leadership, legal structure, ownership, and other governance information in their annual report on Form 2. For example, firms will be required to report the names of their principal executive officer, of the individuals responsible for various components of the firm's system of quality control, and of the members of the firm's governing board or management committee.

3. Network Relationships. Registered firm annual reports will be required to include information about any network arrangement to which the firm is subject. This information includes (1) a brief description of the network relationship (e.g., the network structure and the relationship of the registered firm to the network); (2) whether the firm shares information with the network regarding its audits; (3) whether the firm is subject to inspection by the network; and (4) any other information the firm considers relevant to understanding how the network relationship relates to its conduct of audits.

4. Material Events Reporting. Registered firms that issue audit reports for more than 100 public companies will be required to report the occurrence of certain events that pose a material risk, or represent a material change, to the firm's organization, operations, liquidity, or financial resources, in a manner that it will affect its audit services. These events must be reported on Form 3, but, unlike current Form 3 reporting, will be nonpublic. The rule includes a non-exclusive list of reportable material events, such as a determination that there is substantial doubt about the firm's ability to continue as a going concern; entering into a financial arrangement that would materially affect the firm's liquidity; and entering into an agreement that would cause a material change to the firm's ownership or operations, such as "spinning off consulting business or severing a portion of the business for private equity involvement." Material events must be reported within 14 days of their occurrence or "more promptly as warranted."

5. Cybersecurity. The new rules also require registered firms to report "significant cybersecurity events" on Form 3. A "significant cybersecurity event" is defined as an event that significantly disrupted or degraded firm operations critical to the functioning of the audit practice or led to unauthorized access to information systems and networks in a way that resulted in substantial harm to critical audit-related operations. Significant cybersecurity events must be reported within five business days of the firm's determination that the event is significant. Like material events disclosure, cybersecurity events disclosure will be nonpublic.

6. Updated description of quality control policies and procedures. Any firm that registered with the Board before December 15, 2025 (the date that the PCAOB's new quality control standard, QC 1000, becomes effective) will be required to submit a statement of the firm's quality control policies and procedures to update the statement in their original, pre-QC 1000, registration application. This statement must be filed with the Board on a new form, Form QCPP. Firms that register after December 15, 2025, will be required to indicate in their registration application whether the firm has designed a quality control system in accordance with QC 1000. The purpose of Form QCPP is to require firms that registered prior to the QC 1000 effective date to make a similar statement.

The final firm reporting rules differ from the April proposal in several respects. Among other things, the Board eliminated the proposed requirement that large firm financial statements be prepared under either GAAP or the International Financial Reporting Standards; eliminated the proposed requirement that firms report the names of all persons who report directly to the firm's principal executive officer; retained the current 30-day deadline of filing Form 3 (except for the new the material events and cybersecurity disclosures); and limited material events disclosure to firms that audit more than 100 public companies.

Effective Dates

Firms that audit more than 100 public companies will be required to begin firm and engagement metrics reporting for periods beginning on October 1, 2027. Other firms will begin reporting one year later.

Firms that audit more than 200 public companies and have more than 1,000 personnel will be required to comply with the new firm reporting requirements (except for Form QCPP) beginning on March 31, 2027. Other firms will begin reporting one year later. Form QCPP will become effective on December 15, 2025, with a filing deadline of January 14, 2026.

Dissent

Board Member Christina Ho dissented from the adoption of both the firm and engagement metrics requirements and the firm reporting rules. See Statement on the Firm & Engagement Metrics Adopting Release - Will This Unusually Rushed Auditing Standard Suffer the Same Fate of the Auditing Standard 2? (November 21, 2024) and Statement on the Firm Reporting Adopting Release – Extremism in the Name of Investor Protection (November 21, 2024). Board Member Ho described the Board votes on these two matters as "unprecedented" because "[n]ever in the history of the PCAOB has the Board rushed to adopt new standards and rules in the middle of a historic transition to new SEC leadership, let alone adopt standards and rules that are not ready." She added, "Political expediency is not evidence-based policymaking. Haste naturally harms work product quality, which will not escape any keen eyes."

Among other criticisms, her statements point to the CAQ's audit committee and investor surveys which found that most audit committee members and investors believe that the information already available to assess audit quality meets their needs. See CAQ Surveys Audit Committee Members and Investors on Engagement Performance Metrics, September-October 2024 Update. For example, as to the performance metrics rules, she characterizes the Board majority as "blithely ignoring, or at best, downplaying audit committee and investor commenters, who are among the intended users, of which more than a super-majority have stated that they have all or most of the information they need to assess audit quality." Ms. Ho also expressed concern about the pace of Board standard-setting, which she described as "continuing to force feed the auditing profession with a voluminous number of standards within the limited funnel of a

couple years," and predicted that the result would be to increase audit fees, reduce capital formation, reduce competition, and intensify the accounting talent shortage. She also contended that the new requirements would "add tremendous strain on personnel and financial resources of small firms" and that "the collective implementation of all the new PCAOB standards will detract focus from audit quality."

Audit Committee Takeaways

The PCAOB releases adopting these new disclosure requirements make clear that they are intended to benefit audit committees by providing them with additional information to support their oversight of the company's auditor. However, as Ms. Ho's statement describes, the comments submitted to the Board on the proposals are mixed, at best, as to whether audit committee members think the added information will be useful. As she suggests, it appears that these projects could have benefitted from further study and input. Of course, because of the upcoming changes in SEC membership – and quite possibly in the make-up of the PCAOB – as a result of the Presidential election, any delay would likely have been fatal to these controversial proposals.

Whatever views audit committee members may hold now, it is certainly possible that, once performance metrics reporting begins, most committees will find the new information useful, at least as fodder for discussion with their engagement partner. Understanding the relevance of the metrics to the performance of a specific audit engagement will require a sophisticated understanding of the full context of the audit and how particular metrics relate to that audit. Mandatory performance metric reporting will not begin until 2027. Audit firms and audit committees should use the next three years to gain a better understanding of the metrics and the significance of each to the company's audit.

PCAOB Puts NOCLAR on Hold but Reminds Auditors of Their Illegal Acts Responsibilities

On November 15, Accounting Today reported that the PCAOB will not take further action this year on its controversial proposal to expand the auditor's responsibilities to consider client noncompliance with laws and regulations (NOCLAR). According to a PCAOB staff spokesperson, the Board "will continue engaging with stakeholders, including the SEC, as we determine potential next steps." The Board's regulatory agenda describes the next action on the proposal as "TBD pending analysis" of comment letters and other input the Board has received and lists the anticipated timing of the next action as 2025. Previously, the agenda indicated that the next action would be adoption and that it would occur in 2024.

Although changes in the auditing standards related to audit client law violations are off the table for now, on November 12 – three days before announcing the deferral of NOCLAR -- the Board issued Spotlight: Auditor Responsibilities for Detecting, Evaluating, and Making Communications About Illegal Acts (November 2024) (Illegal Acts Spotlight). This staff paper reminds auditors of their responsibilities under the law and current PCAOB standards to detect, evaluate, and communicate illegal acts.

NOCLAR

The proposed NOCLAR standard would expand the auditor's obligation 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. Auditors would have to identify the laws to which the company is subject, look for and evaluate information suggesting any possible noncompliance, and communicate with management and the audit committee when they uncover such information, before determining whether a violation occurred or had a financial statement impact. See PCAOB Proposes to Expand Auditor Responsibility for Financial Statement Fairness and for Legal Compliance (May-June 2023 Update).

While investors generally supported NOCLAR, auditors, public companies, and audit committees were opposed. Many of these commenters argued that NOCLAR would require auditors to delve into legal compliance issues as to which they lacked competence and that were unlikely to materially impact the financial statements. There was also concern that requiring auditors to conduct a broad inquiry into compliance with a wide spectrum of laws and regulations would significantly increase audit costs. See Audit Committee Members Weigh in on NOCLAR Proposal, August-September 2023 Update.

The impending change in the regulatory environment in the wake of the Presidential election appears to be the reason for the Board's decision to step back from NOCLAR. PCAOB standards require SEC approval before taking effect, and the SEC must invite and consider public comment before acting on a Board standard. Even if the Board had approved NOCLAR, it is not clear that the Commission could have acted on the standard before SEC Chair Gensler's departure.

Illegal Acts Spotlight

While NOCLAR is likely dead, at least in the form the PCAOB proposed in 2023, auditors already have significant responsibilities to detect and report on illegal acts. The Illegal Acts Spotlight states that, under the federal securities laws and current PCAOB auditing standards, auditors have a responsibility to --

(1) Detect illegal acts.

(2) Evaluate information indicating that an illegal act has or may have occurred.

(3) Determine whether it is likely that an illegal act has occurred, and, if so, to consider the possible effect of the illegal act on the financial statements of the company.

(4) Make appropriate communications about illegal acts, unless "clearly inconsequential," to management, the audit committee, and, in some circumstances, the SEC.

Below is a synopsis of the discussion in the Illegal Acts Spotlight of these responsibilities.

- Detecting Illegal Acts

  Section 10A of the Securities Exchange Act requires audits to include "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." Under the PCAOB standards, the auditor's responsibility to detect and report misstatements from illegal acts that have a direct effect on financial statement amounts (e.g., violations of tax or pension laws) is the same as for misstatements caused by error or fraud. Auditors are also required to be aware of the possibility that illegal acts with an indirect financial statement effect may have occurred. (Violations with an indirect effect are those that relate "more to a company's operations than its financial reporting.") If specific information comes to the auditor's attention about a possible illegal act that could have a material indirect effect on the financial statements, the auditor must determine whether the illegal act occurred.

  The Illegal Acts Spotlight describes procedures that auditors employ for detecting potential illegal acts. These include inquiries of management, the audit committee, internal or external legal counsel, internal audit, and others. Auditors also review board and committee minutes, correspondence from regulators, legal expenses, and matters arising through the company's compliance function. The auditor is required to ask management and the audit committee whether they have received tips or complaints regarding the company's financial reporting.

- Evaluating Illegal Acts

  If the auditor becomes aware of a possible illegal act, the PCAOB's standards require the auditor to obtain an understanding of the nature of the act and the circumstances in which it occurred and to

evaluate its effect on the financial statements. Similarly, under Section 10A, if the auditor "detects or otherwise becomes aware of information indicating that an illegal act (whether or not perceived to have a material effect on the financial statements of the issuer) has or may have occurred," the auditor is required "to determine whether it is likely that an illegal act has occurred."

If the auditor concludes that an illegal act has or is likely to have occurred, the auditor must consider the effect act on the amounts in the financial statements (including contingent monetary effects, such as fines, penalties, and damages) and on the disclosure in the financial statements. The auditor's assessment of the materiality of any effects on the financial statements, including disclosures, requires consideration of both quantitative and qualitative factors. The PCAOB's standards also require the auditor to consider the implications of an illegal act on other aspects of the audit, such as the reliability of management representations and the effectiveness of ICFR.

- Making Communications About Illegal Acts

  Unless the act is "clearly inconsequential," the auditor is required to inform management of an illegal act that comes to the auditor's attention and to assure that the audit committee is informed. Under Section 10A, the auditor is also required to communicate directly to the board of directors, if the auditor concludes that (1) the illegal act has a material effect on the financial statements; (2) senior management has not taken timely and appropriate remedial actions; and (3) the failure to take remedial action is reasonably expected to warrant departure from the standard auditor's report or the auditor's resignation. The auditor is also required to notify the SEC of the illegal act if the auditor has made this communication to the board and the company fails to inform the Commission.

Audit Committee Takeaways

In light of the potential increased audit costs and impacts on compliance procedures and relationships with legal counsel, most audit committees will be relieved that the PCAOB does not plan to adopt its NOCLAR proposal, at least in the near term. It is possible that, even under new, post-inauguration leadership, the Board will continue to consider changes to the auditor's responsibilities regarding company noncompliance with laws and regulations. Audit committees should monitor developments in this area.

Audit committees may want to review the Illegal Acts Spotlight to refresh their understanding of the existing audit requirements regarding illegal acts. Having deferred the NOCLAR proposal, the Board could decide to step up its inspection focus on auditor compliance with these requirements. Audit committees may want to discuss with their engagement partner how the current standards affect the company's audit and whether the engagement team anticipates any changes in its procedures regarding the possibility of illegal acts.

SEC Sanctions Four Companies for Misleading Solar Winds Breach Disclosures

The Securities and Exchange Commission has filed enforcement actions against four companies alleging that each made misleading disclosures concerning the impact on the company of the cyberattack on SolarWinds Corp.'s Orion software. One of the companies was also charged with failing to maintain adequate disclosure controls and procedures. In announcing these actions, Sanjay Wadhwa, Acting Director of the SEC's Division of Enforcement, said: "As today's enforcement actions reflect, while public companies may become targets of cyberattacks, it is incumbent upon them to not further victimize their shareholders or other members of the investing public by providing misleading disclosures about the cybersecurity incidents they have encountered." SEC Charges Four Companies With Misleading Cyber Disclosures (SEC Press Release, October 22, 2024).

These actions arise from the 2020 cyberattack on SolarWinds in which Russian hackers inserted a vulnerability into Orion, SolarWinds's IT monitoring and management software product. The four companies charged were Orion users. (For a description of the SEC's case against SolarWinds, see A Shift in the

Winds: Court Rejects SEC's Use of Internal Control Authority to Police Cybersecurity, August 2024 Update.) The gist of the SEC's charges is that, after learning that the threat actor behind the SolarWinds/Orion hack had accessed their systems, each of the four companies either made materially inaccurate disclosures that minimized the impact on the company or failed to update risk disclosures that were no longer accurate due to the unauthorized access.

Avaya Holdings Corp.

The SEC's order against Avaya finds that the company stated in a 2021 quarterly report on Form 10-Q that its investigation resulting from the SolarWinds/Orion breach had uncovered "evidence of access to a limited number of Company email messages" but that there was "no current evidence of unauthorized access to our other internal systems." The order finds that this statement was misleading because, among other things, it omitted to attribute the breach to a nation-state threat actor; omitted to disclose "the long-term unmonitored presence of the threat actor in Avaya's systems," and failed to mention that the breach included "access to at least 145 shared files some of which contained confidential and/or proprietary information."

Without admitting or denying the Commission's findings, Avaya consented to an order that it cease and desist from future disclosure violations and pay a civil money penalty of $1 million.

Check Point Software Technologies Ltd.

The SEC's order against Check Point finds that the company's 2021 and 2022 annual reports on Form 20-F included only generic cyber risk disclosure, despite the company's awareness, beginning in December 2020, of unauthorized activity in its network resulting from the SolarWinds/Orion breach. For example, its 2021 and 2022 Form 20-Fs stated that the company "regularly face[s] attempts by others to gain unauthorized access through the Internet or to introduce malicious software to our information technology (IT) systems" and that "From time to time we encounter intrusions or attempts at gaining unauthorized access to our products and network. To date, none have resulted in any material adverse impact to our business or operations."

The order finds that Check Point's risk disclosure was misleading because, among other things, it omitted disclosure of "how the company's cybersecurity risk had increased due to the SolarWinds Compromise-related activity in its network" and was generic and not tailored to Check Point's particular risks "because the relevant disclosures were identical to the 2020 cybersecurity risk factor disclosure, and therefore failed to reflect the changes in Check Point's cybersecurity risks between 2020 and 2021 * * * as a result of its investigation of the SolarWinds Compromise-related activity."

Without admitting or denying the Commission's findings, Check Point consented to an order that it cease and desist from future disclosure violations and pay a civil money penalty of $995,000.

Mimecast Limited

The SEC's order against Mimecast finds that three reports on Form 8-K that the company filed in 2021 concerning its investigation into the impact of the SolarWinds/Orion breach "negligently created a materially misleading picture of the [SolarWinds] Compromise, providing quantification regarding certain aspects of the Compromise but not disclosing additional material information on the scope and impact of the incident."

For example, the March 16, 2021 Form 8-K stated: "The investigation revealed that the threat actor accessed and downloaded a limited number of our source code repositories, as the threat actor is reported to have done with other victims of the SolarWinds Orion supply chain attack. We believe that the source code downloaded by the threat actor was incomplete and would be insufficient to build and run any aspect of the Mimecast service. We found no evidence that the threat actor made any modifications to our source code nor do we believe that there was any impact on our products." The order finds that this disclosure was misleading because the Form 8-K "omitted that the threat actor had exfiltrated 58% of its exgestion

source code, 50% of its M365 authentication source code, and 76% of its M365 interoperability source code, representing the majority of the source code for those three areas."

Without admitting or denying the Commission's findings, Mimecast consented to an order that it cease and desist from future disclosure violations and pay a civil money penalty of $990,000.

Unisys Corporation

The SEC's order against Unisys finds that the company filed annual reports on Form 10-K for 2021 and 2022 that described its risks from cybersecurity events as hypothetical, despite knowing that it had experienced two SolarWinds-related intrusions involving exfiltration of gigabytes of data. For example, the 2021 and 2022 Form 10-Ks stated that the cyberattacks "could" result in the loss or the unauthorized disclosure of information and that "[i]f our systems are accessed without our authorization" the company could experience data loss and suffer damage. These disclosures were unchanged from the 2019 Form 10-K. However, beginning in December 2020, Unisys had information indicating that the SolarWinds threat actor had compromised its network in several respects. As a result, Unisys's cyber risk disclosure "inaccurately described the existence of successful intrusions and the risk of unauthorized access to data and information in hypothetical terms."

The order also finds that Unisys failed to design controls and procedures to ensure that information about potentially material cybersecurity incidents was recorded, processed, summarized, and communicated to management to allow timely decisions regarding required disclosures. The order describes instances in which Unisys's cybersecurity personnel became aware of cybersecurity incidents, but, since "Unisys's policies did not include adequate escalation procedures in the event of a cybersecurity incident," they did not report these incidents to senior management.

Without admitting or denying the Commission's findings, Unisys consented to an order that it cease and desist from future disclosure violations and from future violations of the requirement to maintain disclosure controls and procedures designed to ensure that information required to be disclosed is reported within the time periods in the Commission's rules. Unisys also consented to pay a civil money penalty of $4 million.

Statement of Dissenting Commissioners

Commissioners Peirce and Uyeda dissented from the issuance of these orders. Their statement asserts:

> "The common theme across the four proceedings is the Commission playing Monday morning quarterback. Rather than focusing on whether the companies' disclosure provided material information to investors, the Commission engages in a hindsight review to second-guess the disclosure and cites immaterial, undisclosed details to support its charges."
>
> * * *
>
> "The Commission needs to start treating companies subject to cyberattacks as victims of a crime, rather than perpetrators of one. Yes, the Commission must protect investors by ensuring that companies disclose material incidents, but donning a Monday morning quarterback's jersey to insist that immaterial information be disclosed — as the Commission did in today's four proceedings — does not protect investors. It does the opposite."

The dissenters analyze each of the four cases in detail. They argue that, in Avaya and Mimecast, the Commission is setting an unduly low bar for determining the materiality of information concerning cyber incidents. For example, in Mimecast, the Commission bases its changes in part on the company's failure to disclose the percentages of various types of source code that were exfiltrated. "By calling for disclosure of specific percentages and types of source code, the Commission ignores the reasonable investor standard embedded within the materiality concept and the types of information that such investor would consider important in making an investment decision." They also point out that the materiality analysis in these cases will affect how companies comply with the SEC's new cyber security disclosure rule. "To avoid being

second-guessed by the Commission, companies may fill their Item 1.05 disclosures with immaterial details about an incident, or worse, provide disclosure under the item about immaterial incidents."

Commissioners Peirce and Uyeda expressed similar concerns concerning the Check Point and Unisys cases, both of which involve risk disclosure. They argue that Unisys undermines the goal of encouraging shorter, more focused risk factor disclosure:

> "If the Commission does not exercise restraint, it could find a violation in every company's risk disclosure because risk factors cover a wide range of topics and are inherently disclosure of hypothetical events. Aggressive enforcement by the Commission may cause companies to fill their risk disclosures with occurrences of immaterial events, for fear of being second-guessed by the Commission. Such a result would frustrate the Commission's goal of preventing a lengthy risk factor section filled with immaterial disclosure." (footnotes omitted)

Audit Committee Takeaways

1. Material Aspects of a Cyber Incident.

For managements preparing cyber incident disclosures and for audit committees overseeing such disclosures, these cases offer insight into how the Commission applies the concept of materiality in the context of cyber security. In 2023, the Commission adopted rules governing cyber security incident disclosure. See SEC Adopts Cybersecurity Disclosure Rules, August-September 2023 Update. Under those rules, Item 1.05 of Form 8-K requires reporting companies to disclose any cybersecurity incident the company decides is material within four days of determining the materiality of the incident. The disclosure must describe the material aspects of the incident's nature, scope, timing, and impact or reasonably likely impact.

While the four new cases do not deal directly with Item 1.05, they reflect – as the dissenters point out -- an extremely broad view of the information that the Commission considers to be material regarding cyber security events. The finding in Mimecast that detail concerning exfiltrated percentages of specific types of source code should have been disclosed is especially striking. Avaya and Mimecast suggest that, in preparing Item 1.05 disclosure, it is safer to include technical details, rather than to present high-level conclusions about the nature and impact of a cyber event.

More generally, these cases highlight the risk of disclosure that seems to minimize or downplay the seriousness of a cyber incident. If the company concludes that an incident is material for purposes of Item 1.05, or otherwise warrants disclosure, it would be prudent not to state that its impact on the company will be limited, absent concrete facts that irrefutably support that conclusion.

2. Escalation of Cyber Incidents to Senior Management.

Unisys is the latest in a series of cases the Commission has brought in which it charged companies with disclosure control violations because they did not have procedures in place to assure that cyber security personnel promptly bring cyber incidents to the attention of senior management with responsibility for disclosure. See Shoot the Wounded! SEC Charges that Inadequate Cybersecurity is an Internal Accounting Control Violation, July 2024 Update and The SEC is Zeroing in on Disclosure Controls, April 2023 Update. Audit committees may want to discuss with management whether the company's disclosure controls include clear guidance concerning the circumstances in which cyber security staff should bring alerts or cyber incidents to the attention of those charged with making disclosure decisions.

3. Risk Factor Updating.

Mimecast and Unisys also underscore the relationship between risk factor disclosure and disclosure controls and procedures. See ESG Meets Disclosure Controls in an SEC Enforcement Action, February-March 2023 Update. The SEC seems to take the position that the occurrence of an event described in a risk factor requires updating or revision of the risk factor. (This issue is currently before the U.S. Supreme

Court in Facebook, Inc. v. Amalgamated Bank.) Managements and audit committees may want to consider whether the company has disclosure controls and procedures that capture and bring to senior management's attention any event that could be viewed as within the scope of any of the company's risk factors. If a risk is significant enough to be included in risk factor disclosure, there should be controls that ensure that information bearing on this risk comes to the attention of disclosure management so that consideration can be given to the need for additional or modified disclosure.

CAQ and IAA: Companies are Saying More About Their Board's Cyber and ESG Expertise

The Center for Audit Quality (CAQ) and Ideagen Audit Analytics (IAA) have released Audit Committee Transparency Barometer 2024 (Barometer 2024), the CAQ's eleventh annual analysis of the audit committee disclosures of companies in the S&P Composite 1500. Barometer 2024 reports that the "most dramatic increase in audit committee disclosures in 2024 is in cybersecurity and ESG - board expertise and oversight." However, many traditional audit-related disclosures have plateaued, and CAQ and IAA believe there is considerable room for improvement. (EY: Cybersecurity Disclosure Continues to Grow Along with Cyber Risks in this Update provides additional information on the increase in cybersecurity-related disclosure.)

Barometer 2024 tracks audit committee disclosures on thirteen topics, two of which include subtopics, and breaks down S&P 1500 disclosures between the S&P 500, the S&P MidCap 400, and the S&P SmallCap 600. For a discussion of last year's report, see CAQ Reports on Ten Years of Increasing Audit Committee Transparency, November-December 2023 Update. Highlights of Barometer 2024 are summarized below.

Directors Skills Matrix

Barometer 2024 added a new topic: whether the board of directors discloses a skills matrix. Eighty-five percent of the S&P 500 made such a disclosure, as did 75 percent of S&P MidCap companies and 62 percent of S&P SmallCaps. Barometer 2024 states that "[d]isclosing a board skills matrix is a best practice. Whether you are small, mid or large-cap, if you do not have a skills matrix disclosed, here is an opportunity to enhance your disclosure, consistent with your peers."

Frequent Disclosures

Aside from the skills matrix, the three most frequently disclosed topics have not changed since 2022. These top three disclosures are:

- Disclosure related to a discussion of how non-audit services may impact independence. In 2024, 85 percent of the S&P 500, 80 percent of S&P MidCaps, and 74 percent of S&P SmallCap companies made this disclosure. In 2023, the frequency of this disclosure was almost the same (S&P 500: 85 percent; S&P Midcaps: 82 percent, S&P SmallCaps:75 percent).

- Disclosure of the length of time the auditor has been engaged. Seventy-three percent of the S&P 500, 61 percent of the MidCap 400, and 57 percent of the SmallCap 600 disclosed auditor tenure. Last year, 73 percent of the S&P 500, 60 percent of the MidCap 400, and 55 percent of the SmallCap 600 disclosed tenure.

- Disclosure that the audit committee is responsible for cybersecurity risk oversight. Sixty-four percent of the S&P 500, 53 percent of the S&P MidCap 400, and 50 percent of the SmallCap 600 disclosed that the audit committee had cybersecurity risk oversight responsibility. In 2023, 59 percent of the S&P 500, 50 percent of the S&P MidCap 400, and 40 percent of the SmallCap 600 made this disclosure. Audit committee cybersecurity responsibility disclosure has risen sharply in the past eight years. In 2016 only 11 percent of the S&P 500 (and 5 percent of Mid-Caps and 4 percent of SmallCaps) discussed audit committee oversight of cybersecurity risk.

Oversight of the External Auditor – Opportunities for More Robust Disclosure

Barometer 2024 characterizes its findings regarding auditor oversight disclosure as indicating that, despite "long-term improvement in disclosure rates" over the past 11 years, a plateau seems to have been hit. The report observes that "we continue to hear that investors want more, providing an opportunity for audit committees to enhance disclosures on key matters to effectively tell the audit committee's story to investors."

Barometer 2024 discusses three specific areas in which the authors see opportunities for audit committees to provide more thorough disclosure regarding their oversight of the external auditor.

- Discussion of audit committee considerations in appointing or reappointing the external auditor. Fifty percent of the S&P 500 included a discussion of the audit committee's considerations in appointing or reappointing the external auditor. This was up slightly from 2023 when 49 percent disclosed these considerations. For the S&P MidCaps, this disclosure fell slightly to 35 percent from 36 percent, while for SmallCaps it rose from 26 percent to 29 percent. Barometer 2024 states: "These disclosures demonstrate the audit committee's commitment to selecting and retaining a qualified external auditor, which is critical to promoting audit quality. Providing information regarding the factors considered, including pros and cons, and the unique considerations arising during the year, provides useful information and demonstrates the extent of the audit committee's engagement."

- Discussion about how the audit committee considers length of tenure. As noted above, audit firm tenure is a frequent disclosure. However, few audit committees discuss how tenure factors into reappointment decisions. In 2024, 13 percent of the S&P 500, 5 percent of S&P MidCaps, and 4 percent of S&P SmallCaps made this type of disclosure. These disclosure percentages are not significantly different than in 2023, although, before 2022, no S&P 1500 Composite company disclosed how tenure affected reappointment.

- Discussion of audit fees and their connection to audit quality. A third area in which disclosure is rare, but, in the view of the CAQ and IAA, should increase is how the audit committee evaluates the relationship between audit fees and audit quality. "Clear disclosures about how the audit committee evaluates audit fees in relation to audit quality highlight the audit committee's commitment to promoting audit quality. This is also an opportunity for the audit committee to discuss how it drives efficiencies in the audit and is focused on not only the cost of the audit, but also the quality." Currently, only 6 percent of the S&P 500 make disclosures related to the audit committee's view of the connection between fees and quality. For smaller companies, the frequency of such disclosure is even lower.

Other Cybersecurity and ESG Disclosures

Barometer 2024 notes that the role of the audit committee has expanded to include oversight of topics like cybersecurity and ESG reporting. This in turn should lead to an expansion in audit committee disclosure: "As cybersecurity, ESG, and other emerging topics are multi-faceted and evolving, how the board assigns oversight of these risks among its committees is helpful information for investors." The best disclosures include "the roles and responsibilities assigned to the audit committee, an explanation of why the audit committee is suited to oversee those topics, and discussion of why audit committee members are appropriate for the specific company."

As discussed earlier, audit committee responsibility for cybersecurity risk oversight is one of the most common disclosures. Other topics related to new responsibilities that have grown in disclosure frequency over the last several years are whether the board includes a cybersecurity expert, whether the audit committee is responsible for ESG oversight, and whether the board includes an ESG or sustainability expert.

- Board cybersecurity expertise. In 2024, 60 percent of the S&P 500 disclosed that the board had cyber expertise, as did 41 percent of Midcaps and 37 percent of SmallCaps. This reflects a significant increase in just the past year. In 2023, 51 percent of the S&P 500 disclosed having a cybersecurity expert on the board, as did 36 percent of the MidCap 400 and 28 percent of the SmallCap 600. In 2016, only 7 percent of the S&P 500, 4 percent of Mid-Caps, and 3 percent of SmallCaps disclosed having such an expert.

- Audit committee responsibility for ESG oversight. Disclosure that the audit committee is responsible for ESG oversight has also increased, although at a slower pace than cybersecurity responsibility disclosure. In 2024, 34 percent of the S&P 500, 20 percent of the S&P MidCap 400, and 15 percent of the S&P SmallCap 600 reported that the audit committee had ESG oversight responsibility. In 2023, the comparable figures were 29 percent (S&P 500), 17 percent (MidCap 400), and 12 percent (Small Cap 600).

- Board ESG/sustainability expertise. Disclosure that the board has an ESG or sustainability expert is also increasing. Fifty-nine percent of the S&P 500 disclosed such expertise in 2024, compared to 54 percent in 2023. At Midcap companies, this disclosure rose from 41 percent in 2023 to 50 percent in 2024; at SmallCaps, the increase was from 29 percent to 39 percent.

Disclosure Examples and Audit Committee Questions

An appendix to Barometer 2024 presents examples of effective disclosures from specific audit committee reports for each of the 13 disclosure topics tracked in the annual analysis. Another appendix contains a detailed pro forma description of an audit committee and its responsibilities, along with a model audit committee report. A final appendix, "Questions to Consider When Preparing Audit Committee Disclosures," lists questions to aid in drafting disclosure concerning the work of the audit committee. These questions are arranged under the 13 disclosure topics tracked in the Barometer 2024 report.

Audit Committee Takeaways

Barometer 2024 concludes with this point:

> "It is crucial for audit committees to tell their stories to clearly articulate the work that they do to protect investors through their oversight of the external auditor and emerging risks. Robust disclosures provide important information to investors about how the audit committee promotes audit quality and fulfills its responsibilities. While we know that significant progress has been made, we strongly encourage audit committees to seize this opportunity to enhance their disclosures by considering where further transparency can be provided regarding not just what the audit committee does, but how it does it."

Audit committees can use Barometer 2024 to benchmark their company's disclosures. Committees should also consider expanding their audit committee reports, particularly in the areas that Barometer 2024 flags for improvement. The disclosure examples and questions in the appendices are a useful source of ideas for committees that want to enhance their disclosures, although each committee should of course tailor its disclosure to its circumstances. Barometer 2024 states, "It's up to the audit committee to tell their unique story each year to provide transparency to investors as to how the audit committee is fulfilling its oversight responsibilities and promoting audit quality."

Deloitte Has Suggestions for Audit Committee Support of the New Internal Audit Standards

Deloitte's Center for Board Effectiveness has released Governing a relevant, effective, and valued internal audit function, a publication in its On the Audit Committee's Agenda series. This paper provides an overview of the Institute of Internal Auditors' new Global Internal Audit Standards (IIA Standards) and offers suggestions for how audit committees can support their implementation. In Deloitte's view, "For audit committees, understanding the new Standards and their implications is crucial to helping ensure that their

organization is leveraging the internal audit function effectively. By staying informed and proactive, audit committees can help their organizations navigate the complexities of the new Standards and achieve greater value from their internal audit activities."

The Global International Audit Standards

The IIA released the new Standards on January 9, 2024, and they will become effective on January 9, 2025. The IIA Standards guide the professional practice of internal auditing and serve as a basis for evaluating and elevating the quality of the internal audit function. There are fifteen Standards organized into five Domains (I: Purpose of Internal Auditing, II: Ethics and Professionalism, III: Governing the Internal Audit Function, IV: Managing the Internal Audit Function, and V: Performing Internal Audit Services).

Domain I is not linked to any of the 15 standards. Domains II through V each consist of Principles (broad descriptions of a related group of requirements and considerations applicable to the domain) and between three and five Standards. Each Standard includes Requirements (mandatory practices for internal auditing), Considerations for Implementation (common and preferred practices to consider when implementing the Requirements), and Examples of Evidence of Conformance (ways to demonstrate that a Standard's Requirements have been implemented).

Attributes of an Effective Internal Audit Function

Deloitte's paper distills the IIA Standards into ten attributes that "demonstrate an effective internal audit function and promote internal audit activities being conducted with a high level of professionalism, consistency, and quality."

- Independence and objectivity. Internal audit should be independent of the activities it audits. Typically, internal audit has a direct reporting line to the audit committee. Internal auditors must maintain an unbiased mindset and avoid conflicts of interest.

- Governance and oversight. The internal audit function should have a strong governance framework including a clear mandate and support from the audit committee and senior management.

- Competence and professionalism. Internal auditors should possess the required qualifications, skills, and experience and participate in ongoing training and professional development.

- Risk-based approach. "Internal audit activities should be prioritized based on a comprehensive and dynamic risk assessment, focused on addressing the most significant risks of the organization and aligned with the organization's strategic objectives and risk profile."

- Balance of assurance and advisory services. Internal audit should provide both assurance and advice. A balanced approach to these two functions combines "the thoroughness of assurance services with the forward-looking perspective of and insights from advisory services."

- Resilience. "The internal audit function should be adaptive and agile, capable of responding to changes in the organization's risk profile and external environment."

- Use of technology. Technology and digital capabilities enhance the efficiency and effectiveness of internal audit activities.

- Effective communication and reporting, with a focus on value. "Internal audit reports should provide valuable insights and recommendations to management and the audit committee. Reporting should be clear, concise, and actionable."

- Quality assurance and improvement. The internal audit function should have a robust quality assurance and improvement program in place, including both internal and independent external assessments.

- Adherence to ethical standards. Integrity and objectivity in internal audit activities help establish trust among stakeholders. Internal auditors should adhere to a code of ethics that promotes integrity, confidentiality, and professional behavior.

Essential Activities of the Audit Committee and Senior Management

Domain III addresses governance of the internal audit function. Each Standard in Domain III includes essential conditions for board (i.e., the audit committee) and management support of effective internal audit. The chief audit executive (CAE) should discuss with the audit committee and senior management the importance of the essential conditions and "gain alignment" around fulfilling these conditions or understand the potential impact if there is disagreement about the essential conditions. The essential conditions in Domain III that are specific to the board/audit committee are:

- Governance framework. Audit committees should ensure that the internal audit function has a clear mandate and safeguard the function's independence and objectivity.

- Resource allocation. Audit committees should collaborate with senior management to provide adequate resources to the internal audit function and invest in continuous professional development).

- Communication and reporting. Audit committees should support open and transparent communication between the internal audit function, management, and the audit committee; share information to align the function with the organization's goals; and require reports to be clear, concise, and actionable).

- Support of the internal audit function. Audit committees should champion internal audit, demonstrate support through internal audit's positioning within the organization, and ensure there is a quality improvement and assurance program to support continuous improvement.

Deloitte provides more detail on each of these essential conditions. The paper notes: "It is important that audit committees understand these essential conditions and their implications in order to effectively oversee the internal audit function and help it add significant value to the organization."

Considerations for the Audit Committee in Supporting Adoption of the New Standards

Deloitte identifies five specific audit committee responsibilities that support the implementation and adoption of the IIA Standards:

- Oversight and guidance. The audit committee should provide oversight and guidance to the CAE regarding implementation, including alignment with the essential conditions.

- Resource allocation and readiness preparation. The audit committee should determine if internal audit has the required resources and discuss with the CAE any expected challenges to implementation. In light of the January 2025 effective date, internal audit should already be performing a readiness assessment and identifying required actions.

- Stakeholder communications. The audit committee should communicate with key stakeholders, including management and the external auditor, about the implications of implementing the new IIA Standards.

- Monitor performance and progress. The audit committee should understand the internal audit function's progress toward implementation and provide input to the CAE as to strategy, performance objectives, and performance measures.

- Maturity expectations. The audit committee should communicate to the CAE the committee's priorities for the internal audit function and ensure they are incorporated into internal audit's longer-term strategy, performance objectives, and performance measures.

Audit Committee Takeaways

Audit committees should familiarize themselves with the basics of the IIA Standards and monitor how the company's internal audit function is implementing them. Deloitte's paper provides a good overview of the objectives of the Standards and of the role that the audit committee can play. The CAE should already be assessing internal audit's current practices against the Standards and identifying actions necessary for implementation. As Deloitte points out: "While more mature internal audit functions may be more aligned with the new Standards, many internal audit functions are finding that they need to take some action for conformance." If the new IIA Standards have not previously been discussed with the CAE, the audit committee may want to get up to speed on what steps he or she is taking.

On the Update Radar: Things in Brief

SEC Charges that Personal Friendship with an Executive Undermined Director's Independence. The SEC has charged James R. Craigie, a former director of consumer goods packaging manufacturer Dwight & Church Co., Inc., with violating the proxy rules. The charges are based on allegations that Craige served as an independent director without informing the board of his close friendship with a company executive. The SEC's complaint states, "As a result of Craigie's concealment, Church & Dwight's proxy statements in 2021 and 2022 contained misstatements of material fact when they represented that Craigie was an independent director." These charges shed light on the circumstances in which, in the SEC's view, a personal friendship with a member of management is inconsistent with a director's independence.

Craigie was the CEO of Church & Dwight from 2004 to 2015 and served as a non-independent member of its board of directors from 2004 to 2019. After a cooling-off period following his retirement as CEO, the board determined that Craigie was independent as of January 2020, and he was elected as an independent director at the 2020 shareholders meeting. The board also determined that Craigie met the independence criteria in 2021 and 2022. Church & Dwight's proxy statements for those two years identified Craigie as an independent director.

The board based its determinations that Craige was independent on his responses to the company's annual D&O questionnaire. The questionnaire stated that, for a director to be independent, the board had to determine that the director had no material relationship with the company. The questionnaire listed "industrial, banking, consulting, charitable, and familial relationships" as examples of potentially disqualifying relationships. However, the questionnaire also asked whether a director had "any other relationship" with Church & Dwight or its management. In 2021, 2022, and 2023, Craigie answered "no" to this question.

The SEC alleges that Craige's questionnaire responses caused the 2021 and 2022 proxy statements to contain false and misleading information because, between January 2020 and March 2023, he maintained a close personal relationship with a member of Dwight & Church's executive team. Among other things –

- Craigie frequently vacationed with the executive and the executive's spouse, including six trips to eight countries. Craigie paid more than $100,000 for the executive and his spouse to join Craigie and his spouse on these international vacations. The executive also occasionally stayed at Craigie's apartment in Miami, and Craigie took the executive and his family on boat trips in New York, Connecticut, and Miami.

- When Church & Dwight began a CEO succession process, Craigie allegedly shared confidential details about the process with the executive and took steps to better position the executive for succession.

The Commission also alleges that Craige actively concealed his relationship with the executive from the board. For example, he asked the executive not to mention one of their upcoming vacations to anyone at Church & Dwight. In addition, he offered to help the executive prepare a presentation to the board but told him "do not mention me at all as it would make me appear biased toward you as the next CEO."

In February 2023, Church & Dwight became aware of Craigie's relationship with the executive, and the board formed a special committee to assess Craigie's conduct. The special committee found that Craigie failed to disclose his close personal friendship with the executive and that he had disclosed confidential information about the CEO search. The board then determined that Craigie was no longer independent, and Church & Dwight made this disclosure in its 2023 proxy statement.

Without admitting or denying the allegations, Craigie agreed to an injunction against further violations of the proxy provisions, a civil penalty of $175,000, and an order barring him from serving as an officer or director of any public company for five years.

While the facts in this case are extreme, the Commission's action raises questions about the line between permissible and impermissible friendships between directors and members of management. Many directors might be viewed as having some level of personal relationship with one or more company executives. It is not possible to determine whether this case is simply a reaction to an unusual situation or whether it marks the beginning of SEC scrutiny of these types of relationships. However, directors should be inclusive in their D&O questionnaire responses concerning any personal friendships they may have with members of management, especially senior company executives.

PCAOB Releases 2020 Criticisms of Grant's Quality Control. On October 24, the Public Company Accounting Oversight Board released three previously nonpublic portions of Grant Thornton's 2020 inspection report. Board criticisms of a firm's quality control system appear in Part II of a firm's inspection report, and, under the Sarbanes-Oxley Act, Part II is nonpublic when the report is issued. If the firm does not, in the PCAOB's view, satisfactorily address a quality control criticism within 12 months, the Board makes the criticism public.

The three now-public quality control criticisms in Grant's 2020 inspection report are:

- Testing Controls. Grant's system of quality control does not provide reasonable assurance that the work performed by the firm's personnel to test controls will meet the requirements of the Board's auditing standards. In three audits, the inspectors concluded that Grant "did not sufficiently evaluate whether controls that it selected for testing that included a review element operated at a level of precision that would prevent or detect material misstatements because the firm did not evaluate the review procedures that the control owners performed, including instances in which the firm did not evaluate the procedures to identify items for follow up and the procedures to determine whether those items were appropriately resolved." In addition, the inspection team "identified instances in which the firm did not identify and test, or sufficiently test, controls over the accuracy and completeness of data or reports used in the operation of controls."

- Reliance on Data or Reports. The firm's system of quality control does not provide reasonable assurance that the work performed by the firm's personnel to establish a basis for reliance on company-prepared data or reports will meet the requirements of the PCAOB's standards. In four audits, the inspection team found that the firm "did not identify and test, or sufficiently test, controls over the accuracy and completeness of certain data or reports that the issuer used in the operation of controls that the firm tested." In addition, in these four audits, "the firm did not perform procedures to test the accuracy and/or completeness of certain data or reports that it

used in its substantive testing, or in the alternative, test, or sufficiently test, controls over those data or reports."

- Supervision of the Audit. Grant's system of quality control does not provide reasonable assurance that supervisory activities, including engagement partner reviews of audit work, will meet the requirements of the Board's auditing standards. This finding is based on the inspection team's identification of deficiencies in five audits that the engagement partner should have identified and appropriately addressed. In each of these audits, the engagement team identified a significant risk, including in some cases a fraud risk, in an area in which the inspection found a deficiency.

The date of Grant's 2020 inspection report is September 30, 2021. Therefore, the release of these portions of the report indicates that Grant failed to persuade the PCAOB that, as of September 30, 2022, it had satisfactorily remediated these three quality control deficiencies.

Audit committees of Grant clients may want to discuss with their engagement partner how the firm is addressing these matters, changes it has made since the PCAOB's determination that the deficiencies had not been remediated, and whether the deficiencies might have affected the company's audit.

California Tweaks its Climate Disclosure Law But Reporting Deadlines are Unchanged. The California legislature has passed, and Governor Newsome has signed, Senate Bill 219, which makes minor changes to California's far-reaching climate disclosure legislation. But, despite the Governor's request, the legislature declined to postpone the reporting deadlines. Litigation challenging the Constitutionality of the California requirements has also, at least so far, failed to delay implementation.

In late 2023, California enacted broad climate disclosure legislature. See California Outflanks the SEC on Climate Disclosure, October 2023 Update, and California Weighs in on Net Zero Disclosure, November-December 2023 Update. Among other things, the legislation requires every U.S. public or private entity with annual global revenue exceeding $1 billion that does business in California to annually report its Scope 1, 2, and 3 greenhouse gas (GHG) emissions and to obtain assurance from an independent third party on the reporting. This disclosure begins in 2026 for FY 2025 Scope 1 and Scope 2 emissions and in 2027 for FY 2026 Scope 3 emissions. In addition, companies doing business in California that have annual global revenue exceeding $500 million must prepare a biennial climate-related financial risk report. The first risk reports are due January 1, 2026.

While Senate Bill 219 does not extend the reporting deadlines, it does make technical changes that affect the disclosure requirements. These include:

- GHG emissions may be consolidated and reported at the parent company level. Subsidiaries that are reporting entities are not required to report separately.

- The California Air Resource Board (CARB) has until July 1, 2025 to write GHG emissions disclosure rules. The original legislation required CARB to adopt rules by January 1, 2025. Since reporting companies still must disclose their 2025 Scope 1 and 2 emissions in 2026, this means that these companies will have six fewer months to implement CARB's final rules.

- CARB has discretion as to the timing of Scope 3 emission disclosures. The original legislation required reporting companies to disclose their Scope 3 emissions 180 days after their Scope 1 and 2 emissions disclosure. Under the new law, CARB can set the Scope 3 reporting schedule.

- Reporting companies will not be required to pay a fee when filing climate disclosure reports.

The U.S. Chamber of Commerce has brought a lawsuit challenging the emissions disclosure requirements on First Amendment grounds. On November 5, a federal judge denied the Chamber's

motion for summary judgment and allowed the law to remain in effect while the case is pending. The court indicated it needed more information to determine whether the disclosure requirements are Constitutional.

Many mid-sized or larger U.S. companies will be required to submit a climate-related financial risk report in 2026 and to report their Scope 1 and 2 GHG emissions under CARB's as-yet-unannounced regulations. Audit committees that have not already done so should discuss with management whether the company is subject to the California climate disclosure requirements and, if so, whether it has processes in place to collect the information needed to comply. Audit committees of companies subject to the GHG emissions disclosure requirement should also consider how they will select an independent third party to provide limited assurance over those disclosures.

EY: Cybersecurity Disclosure Continues to Grow Along with Cyber Risks. The largest U.S. companies are disclosing more information about cybersecurity. That is the central finding of the 2024 edition of the EY Center for Board Matters's annual analysis of Fortune 100 company cybersecurity disclosures. Cyber disclosures: what companies shared about cyber risks in 2024 reports that every aspect of cybersecurity disclosure EY tracks has increased since 2018. Other findings include:

- Audit committees continue to oversee cyber. Eighty-one percent of Fortune 100 companies report that the audit committee has cybersecurity oversight responsibility, up from 61 percent in 2018. Thirteen percent assign cyber risk to a stand-alone risk committee, and 10 percent to a technology committee. (Some companies assign cyber risk to several committees.)

- Cyber expertise is in demand. Seventy-two percent of companies report seeking board-level cyber expertise. Almost the same percentage -- 71 percent – disclose cybersecurity background in at least one director biography, up from 34 percent in 2018.

- Dedicated cyber risk experts are engaging with the boardroom. Seventy percent of companies report that the Chief Information Security Officer provides the board with cyber risk information, up from 9 percent in 2018.

- Dedicated board time on cyber. Fifty-seven percent of the 100 companies report that the board meets with management on cybersecurity at least annually or quarterly. This is more than four times the level of similar disclosure in 2018.

- Preparedness exercises are common. Forty-seven percent of the companies report performing simulations, tabletop exercises, or response readiness tests, up from 3 percent in 2018.

EY also discusses the increase in cyber risk and attack sophistication. The report points out that, in 2023, cyber threat complaints to the FBI increased 10 percent and cyber attack losses increased 22 percent (to $12.5 billion annually). Thirty-two percent of cyber incidents involved an extortion scheme, such as ransomware. Company employees are a major source of vulnerability – more than two-thirds of breaches include employee involvement, such as phishing, behavior manipulation, or other methods to obtain and exploit employee credentials.

EY's report lists ten leading practices in board cyber risk oversight, including actions the board could take and questions to consider concerning each practice. EY also presents sample language from public cyber disclosures on such topics as board cyber expertise, board oversight activities, and response readiness.

The report concludes with this takeaway:

> "Leading boards prioritize cybersecurity oversight by embedding it in all appropriate board-level conversations, remaining engaged with a variety of voices from management and external experts, ensuring that relevant skills are in or accessible to the board room, and engaging in response

exercises — and incorporating lessons learned into company playbooks. Further, they stay current on the evolving regulatory environment and are increasingly transparent and timely in their cyber disclosures about how the company is identifying and addressing key cybersecurity risks."

Many audit committees play a central role in cybersecurity oversight. See CAQ and IAA: Companies are Saying More About Their Board's Cyber and ESG Expertise in this Update. Committees with responsibility in this area may find it helpful to review EY's report, especially the leading practices it describes and the related questions to consider.

PCAOB Investor Advocate Issues a Bulletin on Engagement with Audit Committees. The Public Company Accounting Oversight Board's Office of the Investor Advocate (OIAD) has issued an Investor Bulletin (OIAD Bulletin) describing PCAOB resources that investors "may consider as they engage with audit committees concerning the audit committees' dialogues with their independent auditors."

The OIAD Bulletin states that, since "effective and informed audit committees can be a force for elevating audit quality," investors may consider "outreach to audit committees to discuss the audit committees' audit oversight." The Bulletin points specifically to three documents:

- Spotlight: Audit Committee Resource. This paper, released in 2023, includes questions that the audit committee may wish to ask the company's auditor during the audit. See So Many Questions: PCAOB Suggests Questions Audit Committees Should Ask, July 2023 Update. The OIAD Bulletin highlights questions on auditing and accounting risk, audit firm independence, and critical audit matters.

- Spotlight: Staff Update and Preview of 2022 Inspection Observations. This staff Spotlight lists questions that audit committees should consider as they review inspection findings. See 2022 PCAOB Inspections Preview, June-July 2022 Update. The OIAD Bulletin highlights questions regarding whether the company's audit engagement has been inspected; if so, audit areas that required significant discussions with the PCAOB; and the results of inspections of other audit engagements headed by the company's engagement partner.

- Spotlight: Staff Priorities for 2024 Inspections and Interactions With Audit Committees. The 2024 staff priorities report suggests eleven inspection-related questions that audit committee members may want to consider or discuss with their auditor. See PCAOB 2024 Inspection Priorities: More Inspections and a Focus on Firm Culture, January 2024 Update.

The OIAD Bulletin concludes with this observation: "Overall, investors may consider inquiring of audit committees whether they are engaging in such discussions in their oversight of independent auditors, and if they are not, to encourage audit committees to do so." Audit committees, in turn, should be aware that investors may use the OIAD Bulletin as a source for questions to pose to the committee.

RSM Finds Middle Market Companies Preparing Cautiously for ESG Rules. According to an RSM survey, 75 percent of mid-sized companies have begun preparing to implement climate-related regulations. But a still-larger majority – 84 percent -- said they are "monitoring developments before acting on them." And 56 percent said their organization was waiting until after the U.S. presidential election before taking further action.

These are some of the findings of The RSM Middle Market Sustainability Survey 2024: US and Canada. The survey, which included 412 professionals at middle market companies and nonprofits in the United States and Canada, was conducted between August 27 and September 3, 2024. It targeted organizations with annual revenue of $40 million to $10 billion and respondents who influence their organization's sustainability or corporate social responsibility decisions. The sustainability regulations addressed in the survey were the SEC's climate-related disclosure rules (see SEC Adopts Landmark Climate Change Disclosure Rules, March 2024 Update); California's Climate Corporate Data

Accountability Act (see California Outflanks the SEC on Climate Disclosure, October 2023 Update); Canada's Fighting Against Forced Labour and Child Labour in Supply Chains Act; the European Union's Corporate Sustainability Reporting Directive (see E.U. ESG Disclosure Requirements Will Affect Many U.S. Companies, October 2023 Update); and the European Union's Corporate Sustainability Due Diligence Directive.

Key of the survey findings include:

- Challenges. The top five challenges respondents identified to compliance with sustainability regulations were training and educating staff (39 percent); understanding regulatory requirements (34 percent); managing supply chain compliance (32 percent); data collection and management (31 percent); and integrating new operations with existing ones (31 percent).

- Decarbonization plans. Just over half of survey respondents (54 percent) said their organization has a written decarbonization plan in place. Of those with written plans, 61 percent have a carbon-neutral plan, 49 percent have a carbon-offsetting plan, 39 percent have science-based targets, and 33 percent have net-zero plans.

- Executive responsibility. Almost three-quarters (71 percent) of respondents reported that their organization has a senior executive whose primary responsibilities include establishing and achieving a vision for sustainability. Seventy-seven percent of respondents said their organization has a dedicated project manager/project management team to support sustainability reporting.

- Budget. Sixty-nine percent of respondents reported that their organization has a budget dedicated to compliance with one or more of the sustainability regulations addressed in the survey. Of those who reported having such a budget, 79 percent expect the budget to increase in the next fiscal year; 21 percent anticipate it will increase substantially, while 58 percent think it will increase somewhat. When asked why they expect budget increases, factors mentioned included ensuring the ability to meet regulatory requirements, supporting business growth/expansion, responding to inflation/rising costs, and supporting strategic sustainability initiatives/investments.

- Technology. Forty-five percent of respondents reported using AI and machine learning for tracking and reporting on sustainability initiatives. Thirty-nine percent use data analytics platforms and 38 percent use supply chain management systems.

- External assistance. Most respondents (69 percent) believe they will need outside help to comply with ESG regulations and 34 percent have already hired external consultants for compliance preparation.

The high level of middle market preparedness for sustainability reporting reflected in RSM's survey results is somewhat surprising. Audit committees of mid-market public companies might want to consider how their organization compares with these findings. At the same time, the survey respondents' theme of wait-and-see before taking further action makes sense. As many respondents seem to have anticipated, the U.S. election outcome is likely to significantly impact the future of the SEC's climate disclosure rules.

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 --

- Enhanced Auditor Quality Control: Companies Will Feel the Effects (Dan Goelzer, September 20, 2024)

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.

Receipt of the Update by email distribution 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.

Update Nos. 89-present (March 2024 to present) and summaries are available here. Update Nos. 76-88 (August 2022 to February 2024) and summaries are available here. Update Nos. 60-75 (June 2020 to July 2022) are available here. Update Nos. 49-59 (January 2019 to May 2020) are available here. Updates prior to No. 49 are available on request.

An index to titles and topics in the Update beginning with No. 39 (July 2017) is available here.

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.