Governance & Securities Alert

Weil

From the Public Company Advisory Group of Weil, Gotshal & Manges LLP

January 8, 2019

Financial Reporting in 2019:

What Management and the Audit Committee Need to Know (and Ask)

By Cathy Dixon, Ellen Odoner and PJ Himelfarb

Top officials and staff from the SEC, the PCAOB and the FASB gathered in mid-December in Washington, D.C. at the 2018 AICPA Conference on Current SEC and PCAOB Developments to provide year-end accounting, auditing and disclosure guidance to corporate management, audit committees and outside auditors. In this Alert, we focus on key takeaways for management, as preparers, and the audit committee, as overseers, of the 2018 annual report on Form 10-K and ongoing financial reporting in 2019. Specifically, we discuss the regulators' expectations for enhanced disclosure and related controls in the following areas:

- Escalating risks around cybersecurity, Brexit and the transition away from LIBOR
- "New GAAP" and the end of SAB 118 provisional income tax accounting
- Non-GAAP financial measures, which remain on the SEC's radar screen
- Identification and disclosure of material weaknesses in internal control over financial reporting (ICFR)

We also discuss the "dry runs" that regulators are encouraging the audit committee, outside auditor and management to make together in preparation for the impact of the PCAOB's new critical audit matters (CAMS) standard, which will apply to the fiscal 2019 audit of calendar-year large accelerated filers. We then venture a few predictions about what else to expect in 2019 based on the SEC and PCAOB regulatory agendas. We conclude with selected questions for use by audit committees in their dialogues with management and the outside auditor, as well as in their own annual self-evaluations.

I. Escalating Risks: Cybersecurity, Brexit and LIBOR

As discussed below, the SEC has called out three areas of risk—cybersecurity, Brexit and the transition away from LIBOR—for particular attention by public companies this year. This emphasis should not, however, distract a company from addressing other emerging or evolving risks that also may be of significance to it given its particular industry or other circumstances. Consider, for example, the impact of uncertainties in U.S. trade relations with China, disparate global regulatory approaches to addressing climate change and other evolving environmental risks, energy price volatility or other issues "ripped from the headlines."

Cybersecurity Risks

Under SEC Chairman Jay Clayton, the SEC is shining a wide-angle spotlight on corporate cybersecurity, equating its importance to businesses in the 21st century to the transformational effects of electricity in the 20th. The SEC's guidance takes three forms.

***Interpretive Guidance*:** In February 2018, the SEC issued an Interpretive Release that expands on the principles-based disclosure guidance issued by the staff in 2011. In addition, the release details the SEC's expectations regarding the effective design and implementation of controls to assure timely disclosure of material cyber risks and breaches to the investing public and to prevent insider trading during the highly sensitive period between initial detection of potentially material breaches and the company's release of any required disclosures. Finally, the guidance emphasizes the importance of board oversight of how management addresses cybersecurity risk and, in an attempt to use "sunlight" to influence corporate behavior, calls for proxy statement disclosure of the board's oversight role with respect to cybersecurity risk management if cyber risk is considered material (more on materiality below). We expect the SEC to be scrutinizing 2019 proxy statements for this disclosure and challenging companies that do not include it to explain why their boards do not believe that cybersecurity is a material risk warranting board or board committee-level oversight.

***Investigative Report*:** In October 2018, the SEC issued an Investigative Report into whether nine unidentified companies that were the *victims* of cyber attacks themselves may have *violated* the federal securities laws by failing to "devise and maintain adequate internal accounting controls that reasonably safeguard company and, ultimately, investor assets from cyber-related frauds." Rather than bring enforcement actions, the SEC used the report to highlight the need for companies to reassess and recalibrate internal controls, particularly employee training, in light of cyber risks. The frauds to which these companies fell victim—resulting in mostly unrecovered losses ranging from $1 million to over $45 million—involved spoofed or manipulated emails from fake executives or fake vendors (so-called "business email compromises") directing payments to foreign accounts. The SEC pointedly noted that these frauds were not technologically sophisticated – rather, they relied on weaknesses in policies and procedures and human vulnerabilities that rendered the control environment ineffective.[1]

"Message" Enforcement Cases: Lastly, the SEC has sought to drive its message home through a number of enforcement cases. Yahoo (now Altaba) paid $35 million to settle charges that it misled investors by failing to disclose in a timely manner one of the world's largest customer data breaches. Cases are pending (see here and here) against employees of Equifax (including the former CIO of a business unit and a former software engineering manager) who were charged with illegal insider trading prior to the company's public disclosure of a massive data breach. And there have been hints in recent media reports of more governmental inquiries in the pipeline arising from other major cyber attacks on large public companies.

"Fair Warning": These developments—reinforced by observations made by Chairman Clayton and other SEC staff members during the AICPA conference—serve as "fair warning" not only of SEC staff scrutiny of cyber-related disclosures through the Division of Corporation Finance review and comment process in 2019, but also of future enforcement actions targeting insider trading as well as internal accounting control and disclosure violations under the federal securities laws.

What to Do Now:

- Re-evaluate the adequacy of the company's cybersecurity disclosures at fiscal year-end in light of the new guidance. The tone of the guidance makes clear that the SEC will view with skepticism and the benefit of "20/20 hindsight" a company's conclusion that a particular cyber risk is not "significant" or that a particular cyber incident is not "material" and therefore does not warrant timely and appropriate disclosure. In reaching conclusions about significance and materiality, the guidance directs companies to weigh factors such as the importance of any information that has been, or could be, compromised and the range of potential ensuing harm – to reputation, customer and vendor relationships and financial performance, as well as the potential for litigation and regulatory investigations and proceedings.

- ***When a significant cyber risk has been identified but has not yet materialized:*** Disclose the risk in a meaningful, company-specific way. For example, does the company maintain personally identifiable information about its customers (and, if so, is it encrypted)? Are trade secrets important to the business? Is the company vulnerable to the IT systems of key business partners? Avoid speaking solely in the future tense if, as is true for many, the company has had a history of breaches (albeit non-material).
- ***When an incident has occurred:*** The severity and ramifications of a cyber incident may take time to evaluate and unfold. Once an incident has been judged to be material, the SEC encourages companies to disclose it promptly, perhaps via Form 8-K. Recognize that disclosure should evolve over time as the financial consequences of the incident are quantified and other consequences become clear. And as the disclosure evolves, connect the dots among all relevant sections of a periodic report (in the case of a 10-K, business, legal proceedings, the loss contingencies footnote to the financial statements, MD&A and disclosure controls and procedures).
- ***Important note*:** Real-time documentation of materiality judgments will be critical in responding effectively to SEC staff questions—whether raised in the context of the Division of Corporation Finance review process or a Division of Enforcement inquiry—relating to what senior management and the board knew, when they knew it, and how materiality was assessed in light of the totality of relevant facts and circumstances, including but not limited to prior breaches.

- Re-evaluate the company's disclosure controls and procedures, insider trading policy, Regulation FD compliance policy and code of ethics to ensure that they reflect the heightened significance of cyber risks and incidents, and that they work together to facilitate timely analysis by responsible personnel and disclosure of cyber incidents to investors, and foreclose opportunities for illegal insider trading. The SEC has provided a specific "to do list" in this regard:
  - ***Disclosure controls and procedures*:** Refine disclosure controls and procedures, as necessary, to make sure that cyber breaches flagged by IT or other technical personnel "on the ground" will be quickly relayed to appropriate senior management charged with making materiality determinations and disclosure decisions.
  - ***CEO/CFO certifications*:** Take the adequacy of cyber-related controls and procedures specifically into account in the CEO/CFO certification process and disclosures about control effectiveness. This may require changes in existing Disclosure Committee processes and/or committee membership.
  - ***Code of ethics and compliance policies*:** Refresh the company's code of ethics, insider trading policy and Regulation FD compliance policy, along with related employee training, so that they highlight cyber breaches in a consistent way as potentially material events within the strictures of the policy or code.
  - ***Insider trading procedures*:** The SEC's February 2018 interpretive guidance states that "issuers would be well served by considering how to avoid the appearance of improper trading during the period following a [cyber]incident and prior to the dissemination of disclosure." As the fact pattern reflected in the SEC's Equifax charging documents suggests, one practical way to implement the SEC's advice is to ensure that the company's "event-driven" trading window closure processes are sufficiently flexible to permit such closures to be imposed not only between the time a cyber breach is judged to be material and the time it is disclosed to the public, but also – for personnel who have detected or otherwise become aware of a cyber-attack as well as for executive officers and directors—at the threshold stage of initial detection when the materiality of the incident is still being assessed and disclosure decisions have not yet been made. Provided the company's disclosure controls and procedures also are designed and operate effectively to expedite the transmission of initial breach information promptly to the key materiality decisionmakers within the company, such prophylactic measures should help the company not only to avoid the appearance of impropriety but also to prevent potentially illegal insider trading (including tipping).
- Reassess the sufficiency of the company's system of internal accounting controls, particularly those focused on the safeguarding of company assets and the adequacy of the company's accounting books and records, to make

sure that these controls are attuned to what the SEC has described as the "growing global problem … of cyber scams" and "related human vulnerabilities" to such common fraudulent tactics as spoofing and phishing. The SEC has underscored the critical role that training plays in implementing effective cyber-risk controls. Keep in mind that the company's outside auditor likewise will be assessing the effectiveness of these controls in connection with the upcoming integrated audit of the fiscal 2018 financial statements and ICFR.

- Last but certainly not least, prepare disclosure for this year's proxy statement describing how the board, directly or through one or more committees, oversees the management of cybersecurity risk. This may prompt a fresh look by some boards at how oversight is conducted, whether committee responsibilities should be clarified (and reflected in committee charters) and whether the board could benefit from additional cyber expertise and/or resources.

Brexit Risks

At the AICPA conference, Chairman Clayton expressed concern that the possible adverse effects of the United Kingdom's impending exit from the European Union, or "Brexit," are either not well understood or are underestimated. The Division of Corporation Finance will be focusing on the adequacy of company risk factors, MD&A "known trends and uncertainties" and other Brexit-related disclosures in the upcoming reviews of annual reports on Form 10-K (or 20-F) and other periodic and current reports filed in 2019. Division Director William Hinman indicated that his staff has already reviewed a 100-company sample and determined that the quality of risk factor disclosures varied widely (ranging from mere boilerplate to more thoughtful and company-specific). He encouraged companies to consider disclosure in the 10-K of information that the board of directors has been evaluating in the context of ongoing Brexit scenario planning as the deadline of late March 2019 rapidly approaches amidst a flurry of UK-EU negotiations.

What to Do Now:

Evaluate carefully and, if material, make risk factor or other forward-looking disclosure of the anticipated impact of Brexit on licensing agreements, regulatory approvals, taxes, supply-chain relationships, financing and/or risk-mitigation (swaps) arrangements, and any other aspect of the company's global business operations that might be affected by various "hard", "soft" or other reasonably foreseeable Brexit scenarios. Review board presentations as a useful input for disclosure decisions about Brexit (and other) risks. Because the facts on the ground are changing quickly as the UK government struggles to reach a compromise with EU officials before the late March 2019 deadline, be prepared to update and revise "early warning" disclosures as necessary or appropriate throughout the coming year.

Risks Arising from the Transition Away from LIBOR

The SEC has been monitoring the progress of the global transition away from the London Inter-Bank Offered Rate, or LIBOR, which serves as a short-term interest rate benchmark for many commercial and financial contracts in the United States and elsewhere, including corporate debt, floating-rate mortgages and a broad variety of interest-rate swaps and other derivatives. As the Federal Reserve and other central banks around the world work to find suitable replacements for LIBOR by the anticipated January 1, 2022 deadline, the SEC and FASB are concerned that companies outside the banking sector may not be thinking about the potential accounting and other financial reporting implications of this transition for existing contracts that will still be outstanding beyond 2021 (companies may not be aware, for example, that FASB recently issued an accounting standard that would allow reliance, for hedge accounting purposes, on an alternative benchmark interest rate tied to the Secured Overnight Financing Rate, or SOFR). The Division of Corporation Finance has announced that it will prioritize this area in the 2019 review and comment process.

What to Do Now:

Companies should be reviewing all financial instruments and other contracts and/or assets that carry interest rates based on LIBOR and maturity dates that extend beyond 2021, with a view to mitigating future commercial and/or

legal risk. With respect to existing, long-term LIBOR-based obligations, are there alternative benchmarks or fallback provisions that will kick in if and when LIBOR becomes unavailable? What amendment and related contractual provisions apply in the event that negotiation of a change is deemed advisable? Does the company intend to incur new LIBOR-linked contractual obligations in the next 12 to 24 months? Any company with debt securities, swaps or other contractual obligations extending beyond 2021 that use LIBOR as an interest-rate reference point should consider carefully the need for "early warning" disclosures in the risk factor, MD&A and other relevant portions of their upcoming 10-Ks and subsequent 10-Qs.

II. What's New Regarding New GAAP and Income Tax Accounting

During the AICPA conference, senior SEC accountants warned of the need for effective ICFR to address the risk of material misstatement associated with an extended period of pre-adoption implementation and post-adoption application of various New GAAP standards. Chief among them are (1) the new revenue recognition accounting standard (ASC 606) adopted by many calendar-year reporting companies effective January 1, 2018; (2) the new lease accounting standard (ASC 842) that becomes effective for many calendar-year reporting companies in 2019; and (3) the new accounting standard for current expected credit losses (ASC 326), perhaps better known as "CECL," which becomes effective for many calendar-year reporting companies in 2020. The end of the SAB 118 grace period for income tax accounting also requires new and effective ICFR.

Revenue Recognition – Post-Adoption Observations

For many companies, the fiscal 2018 financial statements will reflect the first full year of revenue accounting under ASC 606 that will be subject to audit. While the SEC accounting staff has been pleased with companies' pre- and post-adoption implementation efforts, the staff is continuing to raise comments intended primarily to gain a better understanding of how management is exercising the substantial judgment permitted under the new, principles-based standard. Companies should anticipate staff comments in 2019 requesting more information on the most difficult assumptions and estimates underlying financial statement footnote disclosures relating to: (1) whether performance obligations embedded in contracts are separately identifiable (e.g., are promised goods and services distinct?); (2) whether the company is acting as a principal or agent in connection with a particular revenue arrangement; (3) when control over a product or service shifts to the customer (e.g., should revenue be recognized at a point in time or over the life of the contract?); and (4) whether the company has properly disaggregated separate revenue streams.

Leases – SAB 74 Disclosures are Critical

Despite company concerns about problems with software vendors and other implementation difficulties experienced in 2018, both SEC and FASB staff stated unequivocally at the AICPA conference that the 2019 lease accounting effective date will not be deferred. This means that the upcoming 10-K offers affected companies their last meaningful pre-adoption opportunity to alert investors to any anticipated material effects on the financial statements after adoption. Division of Corporation Finance reviewers will be checking the adequacy of such disclosures in financial statement footnotes and MD&As.

CECL is on the Near Horizon, and Will Affect Many Non-Financial Companies

Effective for many companies in the first quarter of 2020, the new credit losses standard (ASC 326) will shift recognition of credit losses away from the current "incurred loss model" to an "expected loss model" that will require loss estimates to be made for financial assets within the scope of the standard over their contractual terms based on "reasonable and supportable forecasts and historical information." Senior FASB staff speakers observed at the AICPA conference that, while financial institutions will be most directly affected, companies in numerous other sectors will be covered by ASC 326 and should be working now on their implementation plans.

The staff of the SEC's Office of Chief Accountant advised that they are reviewing existing SEC guidance on loan loss allowance determinations (e.g., SAB 102) to ensure alignment with ASC 326, and otherwise are monitoring the resolution of questions raised through the FASB's Transition Resource Group and an upcoming roundtable.

Moreover, the staff has emphasized its continued willingness to consult with companies in connection with their 2019 implementation initiatives. Observing that OCA consultation submissions have shifted from scoping questions to more specific application questions, the SEC's Chief Accountant sees this as "a positive sign that companies are making progress on implementation."

Provisional Income Tax Accounting: The SAB 118 Grace Period Ends

December 22, 2018 marked the end of the one-year measurement period under SAB 118 that gave companies the flexibility either (1) to make and adjust "reasonable estimates" of the effects of the December 2017 Tax Cuts and Jobs Act in applying ASC 740 for each reporting period; or (2) to disclose that they were unable to make such an estimate. Now, in the upcoming 10-K, companies will have to finalize their accounting for the effects of the Tax Act in accordance with ASC 740.

Companies should ensure that their controls and procedures relating to income tax accounting have been adjusted for the loss in flexibility afforded by SAB 118. In addition, it may be worthwhile to consider whether, for purposes of this year's 10-K, the continued absence of definitive U.S. Treasury Department guidance with respect to important provisions of the Tax Act warrant treatment of income tax accounting as a Critical Accounting Estimate in the MD&A and/or identification as a significant accounting policy in the financial statement footnotes.

What to Do Now:

SEC Chief Accountant Wes Bricker has divided the challenges of New GAAP into three components: (1) establishing appropriate controls and procedures over the transition from an existing to a new accounting standard; (2) maintaining appropriate controls and procedures over ongoing application of the new standard; and (3) communicating the effects of the new standard to investors at transition and on an ongoing basis. While not technically New GAAP, these challenges also apply to necessary modifications to the application of existing GAAP to accommodate changes in the regulatory environment; for example, to take into account the continuing effects of the Tax Act as interpreted by federal tax authorities. Chief Accountant Bricker has repeatedly emphasized (see here and here) the importance of audit committee oversight in fostering rigorous approaches by management to each component.

III. Non-GAAP Financial Measures

Non-GAAP financial measures, as well as key performance indicators, remain on the SEC's radar screen. And the SEC means business, as illustrated by a settlement announced the day after Christmas with ADT Inc. stemming from the company's alleged failure to comply with the "equal or greater prominence" requirements of the SEC's non-GAAP disclosure rules. More on this below.

Division of Corporation Finance staff continue to comment on non-GAAP financial measure disclosures made in earnings releases, webcast earnings calls and other investor presentations, and have been known to scour corporate investor relations pages and read analyst and media reports to assess the consistency of a company's non-GAAP disclosures over time and by comparison with the GAAP-mandated disclosures made in the financial statements filed as part of 10-Ks and 10-Qs. The Division's accounting staff expects transparency with respect to how management uses a particular non-GAAP financial measure in running the company's business. This is particularly important as GAAP itself evolves – management may decide to change its non-GAAP disclosure practices (for example, some have done so as a result of adopting ASC 606 (see previous Alert here), and should anticipate staff scrutiny of the company's explanations for such change both within and outside the four corners of reports filed with or furnished to the SEC.

The Division's staff has also indicated that it is now drilling down, in the review and comment process, on whether companies are modifying, rather than supplementing, GAAP through the improper application of "individually tailored accounting principles." While acknowledging recent improvements in companies' compliance with basic

non-GAAP requirements, senior Division accountants made clear during the AICPA conference that they will continue to raise questions in 2019 on company-specific adjustments that appear to represent attempts to circumvent GAAP. Specific examples of non-GAAP usage the staff deems unacceptable have focused on the following efforts of improper "tailoring" of GAAP revenue accounting (ASC 606): (1) shifting from an accrual basis of accounting to a cash basis, to change the timing of recognition; (2) adjusting income tax effects for cash taxes paid, but not for temporary or permanent differences; and (3) adjusting revenue for sales-type or financing leases as if they were operating leases.

Companies should also remember that the "equal or greater prominence" requirement is alive and well. As a reminder, on December 26, 2018, the SEC announced a settlement with ADT Inc. based on the Commission's findings (which ADT did not admit or deny) that, in the headlines and other locations of its fiscal 2017 and Q1 2018 earnings releases, ADT provided non-GAAP financial measures such as "adjusted EBITDA," "adjusted net income" and "free cash flow before special items" without giving equal or greater prominence to the comparable GAAP financial measures.

What to Do Now:

Companies should have a written set of policies and procedures governing the use of non-GAAP measures that meet the standards currently outlined by the SEC staff and keep pace with regulatory developments. In particular, these should address the risk of "individual tailoring" by distinguishing between the permissible exclusion or inclusion of GAAP amounts, on the one hand, and the impermissible alteration of an accounting policy or GAAP-mandated methodology, on the other hand. The audit committee should actively oversee, through dialogue with management and the outside auditors, the company's construction and disclosure of non-GAAP measures in accordance with these policies and procedures.

IV. Identifying and Disclosing Material Weaknesses in ICFR

At the AICPA conference, SEC staff accountants highlighted the importance of identifying and communicating material weaknesses in ICFR to the investing public well before they become manifest in the form of an actual material misstatement requiring a restatement of the financial statements – that is, when such a misstatement is reasonably possible. Despite some observed improvements in the quality of management evaluations of the severity of internal control deficiencies, the SEC believes there is more that senior executives and the audit committee can and should do to strengthen the adequacy of and basis for management's assessment of the effectiveness of ICFR and, where management concludes that ICFR is not effective, the clarity of disclosure in management's report.

A recent SEC enforcement settlement with Primoris Services Corporation is instructive. According to the SEC's findings, which Primoris did not admit or deny, Primoris violated the recordkeeping and internal controls provisions of Sections 13(b)(2)(A) and (B) of the Securities Exchange Act of 1934 and Rule 13a-15(c) thereunder. At the end of 2014, Primoris learned that it had control deficiencies that affected its accounting for contingent cost estimates and it subsequently discovered three related accounting errors that had led it to record revenue in the wrong quarters. When it evaluated the effectiveness of its ICFR for the year, however, Primoris failed to assess the potential magnitude of the accounting misstatements that *could have* resulted from these control deficiencies; it only considered the magnitude of errors *actually* identified and did not consider either the total value of activity, or the entire class of transactions, *exposed* to the control deficiencies. Primoris concluded that it had a significant deficiency in its ICFR but not a material weakness, because it believed that certain compensating controls would have prevented or detected a material misstatement in its financial statements. But, according to the SEC, these compensating controls were either not tested in 2014 or not designed to identify errors in contingency cost accounting. Interestingly, this enforcement proceeding involved the company alone; it did not extend to the company's CEO and CFO in connection with the accuracy of their Sarbanes-Oxley certifications.

What to Do Now:

As the SEC urges through its *Primoris* order, companies should resist the temptation to focus solely on *actual* misstatements caused by a control deficiency without "considering whether it is reasonably possible that other financial statement areas could be impacted based on the root cause of the control deficiency."[2] Rather, take a holistic approach to assessing the severity of control deficiencies and use caution when relying on compensating controls to make a judgment call that evaluates a control deficiency as a significant deficiency (requiring disclosure to the audit committee) rather than a material weakness (requiring public disclosure).

When management does conclude that ICFR is ineffective, the related disclosure must be meaningful to investors. To ensure that investors have the information they need to understand the nature and cause of a disclosed material weakness, and to assess its potential impact on financial reporting, the SEC staff suggests that management and the audit committee (as well as the outside auditor) use the following questions as a starting point for analysis and discussion:

- Does the disclosure allow an investor to understand what went wrong in the control that resulted in a material weakness?
- Is it sufficiently clear from the disclosure what the impact of each material weakness is on the company's financial statements? For example, is the material weakness pervasive or isolated to specific accounts or disclosures?
- Are management's plans to remediate the material weakness sufficiently clear? For example, does disclosure of the remediation plans provide sufficient detail so that an investor would understand what management's plans are, and how these plans would address the identified material weakness?

V. Critical Audit Matters: Dry Runs and Beyond

Commencing with their audit reports on the fiscal 2019 year-end financial statements of large accelerated filers, all PCAOB-registered public accounting firms will be required to include disclosure of any critical audit matters, or CAMs, arising from that year's audit. Many large companies and their outside auditors have responded to calls from senior SEC and PCAOB officials to engage in "dry runs" well in advance of the effective date of the PCAOB's new, principles-based auditing standard, AS 3101. SEC Chief Accountant Bricker observed during the AICPA conference, that "these dry runs are occurring with constructive dialogue among auditors and audit committees about the value of starting the conversation early in the audit cycle, keeping the discussion current for changes and close calls throughout the year, and building into the plan how and to whom a draft of the report will be provided in advance of completing the audit."[3] At the end of the day, Chief Accountant Bricker concluded, this "dialogue should help prevent mistakes in reports prepared [by the outside auditor] for investors next year."

AS 3101 defines a CAM as a matter communicated, or required to be communicated, by the outside auditor to the audit committee that both (1) relates to accounts or disclosures that are material to the financial statements and (2) involves "especially challenging, subjective or complex [areas of] auditor judgment." CAMs are not intended to duplicate the critical accounting estimates that are required to be disclosed in the MD&A because they involve the use of material accounting estimates and assumptions; nor are CAMs intended to serve as a "bad report card" for management. To the contrary, they function solely to illuminate for investors what issues keep the audit engagement partner up at night as the outside auditor discharges its independent "gatekeeper" duties under the federal securities laws.

What to Do Now:

Companies should use the opportunity before CAMs go "live" to think about ways to enhance their own disclosures and related control processes about audit-related matters that the outside auditor is likely to identify as CAMs. Additionally, companies and their audit committee can learn from the disclosure made by auditors of London Stock Exchange – listed companies, particular those in the same industry sector, of key audit matters (KAMs). KAMs are similar to CAMs in that they are issues that, in the auditor's professional judgment, were of most significance and

risk to the audit. Audit committees also may wish to consider whether it makes sense to amend their charters or expand volitional disclosures in the audit committee report to mirror the refinement and/or amplification of their financial reporting oversight role once AS 3101 comes into effect in connection with the fiscal 2019 annual audit cycle.

VI. What Else to Expect in 2019 from the SEC and PCAOB

As outlined in Chairman Clayton's recent Senate testimony, the SEC has an ambitious rulemaking agenda. Much of it relates to projects such as expanding public and private capital formation opportunities while protecting the interests of "retail" investors, market structure reform and proxy plumbing, to name just a few of the Chairman's stated priorities for 2019. That said, companies and their audit committee should expect the SEC to continue its efforts to improve corporate financial reporting and other disclosures through the following initiatives:

- Finalizing uncompleted Dodd-Frank Act rulemaking projects: The SEC just adopted rules which, effective for the 2020 proxy season, will require many of the largest U.S. public companies to describe any corporate policies and/or practices governing certain hedging activities by directors, officers and other employees. (If a covered company lacks such policies and/or practices, it must so indicate or state that such hedging is generally permitted.) Two other SEC Dodd-Frank compensation proposals, however, are on the relatively far horizon: (1) the relationship of executive compensation actually paid and corporate financial performance; and (2) national stock exchange listing standards and SEC disclosure requirements regarding a company policy to "claw back" incentive compensation paid to current and former executives in the event of a restatement of the financial statements due to material error.
- Addressing previously adopted Dodd-Frank implementing rules that have been invalidated by the courts, beginning with resource extraction and presumably followed by conflict minerals.
- Proceeding with careful consideration of public comments on pending proposals to simplify and streamline financial statement disclosures by issuers and affiliates relating to guaranteed or collateralized debt securities.
- Proposing amendments to Rule 3-05 and Article 11 of Regulation S-X relating to pro forma and other financial statement disclosures required in connection with "significant" acquisitions.
- Seeking public comment on the costs and benefits of the current quarterly reporting framework applicable to U.S.-based public companies, including such issues as whether quarterly earnings guidance practices prompt short-term managerial decision-making, whether investors would benefit from narrowing the gap between the timing of earnings releases and the filing of quarterly reports on Form 10-Q, whether the Form 10-Q disclosure requirements could or should be streamlined, and whether smaller issuers should be permitted to report less frequently than each quarter (e.g., on a semi-annual basis).

Even more important than these specific initiatives, expect the SEC to continue to prod companies to improve their disclosures under existing SEC rules and U.S. GAAP. Senior SEC officials made clear at the AICPA conference that accounting and enforcement staff will be monitoring the quality of corporate "early-warning" disclosures regardless of whether they are contained in SEC-filed documents or are disseminated to the investing public via other, less formal communications platforms such as corporate IR websites and social media. SEC accountants and enforcement staff will also continue to work closely with their PCAOB counterparts in policing such areas of common interest as auditor independence and compliance with "gatekeeper" responsibilities imposed by the federal securities laws and PCAOB-promulgated rules and audit standards.

The PCAOB's annual announcement of focus areas for staff inspections inevitably affects how outside auditors plan and conduct corporate audits and, therefore, gives management and the audit committee a preview of what areas of emphasis they can expect from the outside auditor. For 2019, the PCAOB has announced the following key areas of Staff inspection focus, which, unsurprisingly, dovetail with many of the messages conveyed by the SEC described in this Alert:

- The audit firm's system of quality control, described as "the foundation for executing quality audits"

- Independence of the auditor in both fact and appearance
- Recurring audit deficiencies relating to ICFR, revenue recognition, allowance for loan losses and other accounting estimates
- External considerations that increase the risks of material misstatement in the audit client's financial statements
- Assessment of and response to audit clients' cybersecurity risks and breaches
- The use and effectiveness of software audit tools
- The auditor's response to risks associated with digital assets
- Audit quality indicators, and whether auditors are discussing them with client audit committees
- Changes in the auditor's report, under AS 3101, relating to auditor tenure and CAMs
- Adjustment of audit processes as clients adopt or implement New GAAP standards

Audit committee chairs should expect a growing relationship with the PCAOB, even though the PCAOB has statutory authority only over audit firms. For the first time, members of the Inspections staff will be reaching out to the audit committee chair of each corporate audit client whose financial statements are selected for review in connection with the 2019 inspections cycle. Possible topics of discussion include the audit committee's experience with CAM dry runs, auditor independence, and new and recurring areas of audit deficiency identified during the inspection process.

* * *

While it is clear that the specific areas of risk-related disclosures and GAAP compliance discussed in this Alert will be under the regulatory microscope in 2019, it is important that companies and audit committees expect, in a proactive way, that others will emerge. This reality—that companies must engage in careful contingency planning for, and quickly adapt to, the unexpected or unforeseeable risk or event that materializes—highlights the importance of developing and maintaining robust corporate controls and procedures that will flag incipient or emerging risks or events on a "real-time" basis, communicate the relevant information promptly to responsible senior management for materiality analysis and timely disclosure, and thus enable companies to fulfill their Regulation FD and insider trading compliance obligations.

With that in mind, we provide below selected questions for use by audit committees in their dialogues with management and the outside auditor, as well as in their own annual self-evaluations.

Selected Oversight Questions for the Audit Committee

Identification and Disclosure of Cyber and Other Emerging Risks

- Has management reviewed last year's cyber risk factors in light of the Company's experience in 2018 and the SEC's recent guidance?
- Has management evaluated for risk factor disclosure purposes the significance of Brexit and LIBOR risks for the Company and tailored risk factor disclosure to the specific impact on the Company and its operations? Has management reviewed the documentation for LIBOR-based notes and will such documentation need to be amended?
- Are there other significant risks "ripped from the headlines" that management has evaluated for risk factor disclosure (e.g., incentives arising from US trade relations with China, environmental and other "sustainability" risks, energy price volatility)?
- Has the Disclosure Committee reviewed its processes to ensure they provide for open and rapid communications between technical personnel and senior management responsible for disclosure decisions when a cyber breach has been detected? Should someone from IT be added to the Disclosure Committee?
- Has the Company experienced financial losses due to spoofing and phishing? Whether or not it has experienced such losses to date, has the Company reevaluated the adequacy of employee training and other controls, such as enhanced payment authorization procedures and outgoing payment notification processes, to combat these types of fraud?
- Does the CEO/CFO certification process expressly take into account the adequacy of cyber – related controls? Do IT personnel need to be added to the subcertification tree?
- Have the Company's code of ethics, insider trading policy and FD compliance policy—and related employee training--been re-evaluated and refreshed to highlight the potential materiality of cyber breaches?
- Does the insider trading policy include procedures not only to close the trading window between the time a cyber incident is judged to be material and the time it is publicly disclosed, but also to ensure that IT and other personnel on the front lines of monitoring, preventing and detecting cyber breaches, and executive officers and directors, are barred from trading (including tipping) while the materiality of the incident is being assessed?
- ***In discussions with the outside auditor:*** What steps has the auditor taken to assess the effectiveness of the company's relevant cyber risk controls in connection with its integrated audit of the 2018 financial statements and ICFR? What are the auditor's findings and recommendations?

New GAAP

- Does the Company have appropriately trained and experienced personnel responsible for the design and operation of manual control activities, which apply when reasonable judgment and discretion is required (e.g., under the new revenue recognition standard)? If not, what is management's plan for attracting, developing and retaining such personnel?
- Where does management stand on its way to implementation of the new lease standard? What new controls are called for or in place? What disclosures does management anticipate making in the 2018 10-K and subsequent 2019 periodic reports as to the expected effects of the new standard once adopted?
- Where does management stand on its way to implementation of CECL? What issues does it foresee?
- ***In discussions with the outside auditor:*** How does the auditor assess the Company's Year 1 implementation of the new revenue recognition standard and related disclosure? How does the auditor assess the Company's progress in transitioning to the new lease accounting standard and CECL? Does the auditor believe the company's financial organization has sufficient competence to meet the demands of New GAAP?

Non-GAAP Financial Measures

- Borrowing from and expanding upon questions that former SEC Chair Mary Jo White encouraged audit committees to ask, with respect to each non-GAAP measure used or proposed to be used by the Company: [4]
  - What is management trying to accomplish by using the measure?
  - Does management use the measure consistently?
  - Does management use the measure internally?
  - What is the measure meant to communicate?
  - Does the measure change quarter to quarter to get management to its expectations or is it a true, consistent measure of company performance?
  - Is the measure given equal or lesser prominent disclosure to the GAAP measure?
  - Is the usefulness of the measure communicated to investors in an accurate and complete manner without resorting to boilerplate explanations?
  - Have the appropriate controls been applied to the calculation of the non-GAAP measure?
  - How does the Company's non-GAAP measure differ from approaches taken by other companies?

Identification and Disclosure of Material Weaknesses in ICFR

- Has management identified control deficiencies that did not cause a material misstatement in 2018 but reasonably could impact other financial statement areas?
- Is management relying on compensating controls to conclude that a deficiency would not have resulted in a material misstatement and therefore is a significant deficiency and not a material weakness? If so, were such controls tested this year and were they designed to address the controls that had the deficiencies?
- Have all significant deficiencies identified at the end of 2017 or during 2018 been remediated?

Audit Committee Self-Evaluation (with Respect to Cybersecurity)

- Is there clarity around the nature and scope of the audit committee's responsibility for oversight of the management of cyber risk? Is the committee's responsibility limited to oversight of the mitigation of the risk to financial reporting, or is the board looking to the audit committee to oversee cybersecurity risk management for the business more broadly?
- In either case, how well was this responsibility discharged during the reporting period? Looking forward, does the committee have adequate time on its agenda and adequate expertise and internal and external resources?
- How well has the audit committee monitored the processes in place to ensure timely escalation, evaluation and, where material, disclosure of a cybersecurity breach?
- Has the audit committee overseen contingency planning in the case of a failure of cyber controls to ensure that the contingency plan has been assessed and updated?
- Has the audit committee reviewed the proposed proxy statement disclosure relating to the board's oversight of cybersecurity risk management? If the audit committee has responsibility in this area, should it be discussed in the audit committee report?

ENDNOTES

[1] Although the SEC did not name the nine companies, Audit Analytics identified the likely subjects of the report. *See Derryck Coleman, SEC Registrants with Poor Cyber Controls* (Nov. 8, 2018), available here. Three of the nine companies disclosed in their periodic reports that the cyber breach rose to a material weaknesses in ICFR. Each of the three disclosed that it had remediated the material weaknesses by the end of the fiscal year. The range of disclosed remedial actions included: engagement of a consultant; resignation of the Chief Accounting Officer; strengthening of controls (*e.g.*, multi-factor authentication, verification procedures and approval authorities); and enhanced employee training about threats, policies and procedures.

[2] *See Tom W. Collens, Professional Accounting Fellow, Remarks before the 2018 AICPA Conference on Current SEC and PCAOB Developments* (Washington, D.C., Dec. 10, 2018), available here.

[3] *See Wesley Bricker, Chief Accountant, Statement in Connection with the 2018 AICPA Conference on Current SEC and PCAOB Developments* (Washington, D.C., Dec. 10, 2018), available here.

[4] *See* SEC Chair Mary Jo White, *Keynote Address at the 2015 AICPA National Conference: Maintaining High-Quality, Reliable Financial Reporting: A Shared and Weighty Responsibility* (Washington, D.C., Dec. 9, 2015), available here.

Please contact any member of Weil's Public Company Advisory Group or your regular contact at Weil, Gotshal & Manges LLP:

Howard B. Dicker	View Bio	howard.dicker@weil.com	+1 212 310 8858
Catherine T. Dixon	View Bio	cathy.dixon@weil.com	+1 202 682 7147
Lyuba Goltser	View Bio	lyuba.goltser@weil.com	+1 212 310 8048
Adé K. Heyliger	View Bio	ade.heyliger@weil.com	+1 202 682 7095
P.J. Himelfarb	View Bio	pj.himelfarb@weil.com	+1 202 682 7208
Ellen J. Odoner	View Bio	ellen.odoner@weil.com	+1 212 310 8438
Alicia Alterbaum	View Bio	alicia.alterbaum@weil.com	+1 212 310 8207
Kaitlin Descovich	View Bio	kaitlin.descovich@weil.com	+1 212 310 8103
Andrew Holt*	View Bio	andrew.holt@weil.com	+1 212 310 8807
Erika Kaneko	View Bio	erika.kaneko@weil.com	+1 212 310 8434
Elisabeth McMorris	View Bio	elisabeth.mcmorris@weil.com	+1 212 310 8523
Aabha Sharma	View Bio	aabha.sharma@weil.com	+1 212 310 8569

*Not yet admitted in New York