On the 2019 audit committee agenda

Audit committees can expect their company's financial reporting, compliance, risk and internal control environment to be put to the test in the year ahead. Among the top challenges and pressures: long-term economic uncertainty (with concerns about mounting trade tensions, resurging debt, and market valuations), technology advances and business model disruption, cyber risk, regulatory scrutiny and investor demands for transparency, and political swings and policy changes in the U.S., UK, and elsewhere.

Drawing on insights from our interactions with audit committees and business leaders over the past 12 months, we've highlighted seven items that audit committees should keep in mind as they consider and carry out their 2019 agendas:

- Take a fresh look at the audit committee's agenda and workload.
- Sharpen the company's focus on culture, ethics, and compliance.
- Understand how the finance organization will reinvent itself and add greater value in this technology and data-driven environment.
- Monitor management's progress on implementing new FASB standards as well as SAB 118 adjustments related to U.S. tax reform.
- Discuss the new reporting requirements for critical audit matters (CAMs) with the external auditor and reinforce audit quality by setting clear expectations.
- Give non-GAAP financial measures, other key operating metrics, and cybersecurity disclosures a prominent place on the audit committee agenda.
- Focus internal audit on the company's key risks beyond financial reporting and compliance.

Take a fresh look at the audit committee's agenda and workload.

We continue to hear from audit committee members that it is increasingly difficult to oversee the major risks on the committee's agenda in addition to its core oversight responsibilities (financial reporting and related internal controls and oversight of internal and external auditors). Aside from any new agenda items, the risks that many audit committees have had on their plates—cybersecurity and IT risks, supply chain and other operational risks, and legal and regulatory compliance—have become more complex, as have the committee's core responsibilities. Reassess whether the committee has the time and expertise to oversee these other major risks. Does cyber risk require more attention at the full-board level, or perhaps a separate board committee? Is there a need for a compliance or risk committee? Keeping the audit committee's agenda focused will require vigilance.

Sharpen the company's focus on culture, ethics, and compliance.

The reputational costs of an ethics or compliance failure are higher than ever. Fundamental to an effective compliance program is the right tone at the top and culture throughout the organization—one that supports the company's strategy and commitment to its stated values, ethics, and legal/regulatory compliance. This is particularly true in a complex business environment as companies move quickly to innovate and capitalize on opportunities in new

markets, leverage new technologies and data, and engage with more vendors and third parties across longer and increasingly complex supply chains. Closely monitor the tone at the top and culture throughout the organization with a sharp focus on behaviors, not just results. Help ensure that the company's regulatory compliance and monitoring programs are up-to-date and cover all vendors in the global supply chain and clearly communicate the company's expectations for high ethical standards. Focus on the effectiveness of the company's whistle-blower reporting channels and investigation processes through a #MeToo lens. Does the audit committee see all whistle-blower complaints and how they have been addressed? If not, what is the process to filter complaints that are ultimately reported to the audit committee? As a result of the radical transparency enabled by social media, the company's culture and values, commitment to integrity and legal compliance, and its brand reputation are on display as never before.

Understand how the finance organization will reinvent itself and add greater value in this technology and data-driven environment.

Over the next two years, we expect finance functions to undergo the greatest technological transformation since the 90s and the Y2K ramp-up. This will present important opportunities for finance to reinvent itself and add greater value to the business. As audit committees oversee and help guide finance's progress in this area, we suggest several areas of focus.

First, recognizing that the bulk of finance's work involves data gathering, what are the organization's plans to leverage robotics and cloud technologies to automate as many manual activities as possible, reduce costs, and improve efficiencies? Second, how will finance use data and analytics and artificial intelligence to develop sharper predictive insights and better deployment of capital? The finance function is well-positioned to guide the company's data and analytics agenda—and to consider the implications of new transaction-related technologies, from blockchain to cryptocurrencies. As historical analysis becomes fully automated, the organization's analytics capabilities should evolve to include predictive analytics, an important opportunity to add real value. Third, as the finance function combines strong analytics and strategic capabilities with traditional financial reporting, accounting, and auditing skills, its talent and skill sets must change accordingly. Is finance attracting, developing, and retaining the talent and skills necessary to deepen its bench strength and match its evolving needs? It is essential that the audit committee devote adequate time to understand finance's transformation strategy.

Monitor management's progress on implementing new FASB standards as well as SAB 118 adjustments related to U.S. tax reform.

The scope and complexity of implementation efforts for the new FASB standards and the impact on the business, systems, controls, disclosures, and resource requirements should be a key area of focus.

With calendar year-end public companies reporting under the **revenue recognition standard** for 2018, the SEC staff has expressed concern that disclosures do not sufficiently address the significant judgments companies are making about performance obligations, timing of revenue recognition, licensing arrangements, and "gross versus net" presentation. These disclosures require the attention of the audit committee in connection with the company's 2018 10-K and 2019 filings. Also, for some companies, implementation of the revenue standard involved both manual processes and enabling technology and tools. Manual work-arounds should not become permanent. Audit committees will want to help ensure that any work-arounds are automated as soon as possible.

The 2019 effective date for the **leases standard** is almost here for public companies. Companies have had the opportunity to assess the implications of the FASB's technical corrections and amendments and are shifting their focus to the broader aspects of adoption, including internal control over financial reporting and disclosures. SEC staff continues to closely monitor SAB 74 transition disclosures for the new standard. These disclosures should be a focus area for audit committees in connection with the company's 2018 10-K.

The FASB's **credit impairment standard** will be effective in 2020 for public companies. Companies should be analyzing the implications of adoption and considering the adequacy of transition disclosures. While the nature and extent of preparations will vary, companies need to thoroughly evaluate the effect of the standard and determine what changes are necessary. Companies may need to collect more data and significantly change their systems, processes, and internal controls.

Finally, since the SEC staff issuance of **SAB 118**, many companies recognized provisional income tax amounts for the effects of the 2017 tax reform law and continue to adjust balances that were recorded provisionally as of December 31, 2017. Because the SAB 118 measurement period for provisional amounts cannot extend beyond one year, provisional amounts must be finalized by December 31, 2018, with the company's 2018 10-K.

Discuss the new reporting requirements for critical audit matters (CAMs) with the external auditor and reinforce audit quality by setting clear expectations.

In June 2017, the PCAOB adopted a new auditing standard to make the auditor's report more informative, by (among other things) expanding the audit report to include a discussion of CAMs that arose during the audit. The communication of CAMs is intended to provide information about audit areas that involved especially challenging, subjective, or complex auditor judgment and to explain how the auditors addressed these issues. The CAM requirements take effect for audits of fiscal years ending on or after June 30, 2019 for large accelerated filers. For all other entities for which the CAM requirements apply, the effective date is for audits of fiscal years ending on or after December 15, 2020.

CAMs might include some aspect of revenue recognition and other critical accounting policies and estimates, business acquisitions and other significant unusual transactions, and intangible asset impairment charges or other areas that involve estimation uncertainty. It's important to understand the content of the CAMs in the context of the disclosures appearing in the financial statements as we would not expect the audit report to be a source of incremental factual information about the company.

Take advantage of the time before the CAM reporting requirements take effect to discuss them with the auditors. Early dialogue will be key to a smooth and timely implementation. What would the CAMs look like if you had to report them for 2017 or 2018? Ask the audit partner how the company's CAMs would compare with industry peers. Multinational companies that report "key audit matters" under International Standards on Auditing should consider those for reference. There are differences between the definitions of a CAM and a key audit matter, but the comparison is helpful. Audit committees will want to develop a protocol for the audit committee to hear, as far in advance as possible, the issues the auditor intends to communicate as CAMs, what the auditor intends to say about them, and how the auditor's statements will compare to management's disclosures regarding the same issues.

And reinforce audit quality, which is enhanced by a fully engaged audit committee that sets the tone and clear expectations for the external auditor and monitors performance through frequent, quality communications and a rigorous performance assessment. (See the Center for Audit Quality's **External Auditor Assessment Tool**.)

Give non-GAAP financial measures, other key operating metrics, and cybersecurity disclosures a prominent place on the audit committee agenda.

Comment letters from the SEC staff continue to focus on the use of non-GAAP financial metrics in earnings releases, SEC filings, and investor presentations. Following 2016 staff guidance to help financial statement preparers and audit committees evaluate the usefulness and acceptability of non-GAAP financial information, the SEC staff sent over 150 comment letters questioning companies' use of non-GAAP financial measures, and the SEC initiated a number of enforcement actions. While the SEC staff credited companies with heeding the SEC's guidance, they have been critical of company disclosures regarding other key operating metrics.

While 2018 has seen fewer SEC comment letters on non-GAAP financial measures, the SEC remains focused on both non-GAAP financial measures as well as the use of other key operating metrics and continues to emphasize the importance of audit committee oversight in this area. In May 2018 public remarks at Baruch College, SEC Chief Accountant Wes Bricker commented on audit committee involvement in the review and presentation of non-GAAP measures and other key operating measures: "Audit committees that clearly understand non-GAAP measures presented to the public—and who take the time and effort in their financial reporting oversight role to review with management the preparation, presentation, and integrity of those metrics—are an indicator of a strong compliance and reporting culture. Audit committees can review the metrics to understand how management evaluates performance, whether the metrics are consistently prepared and presented from period to period, and the related disclosure policies. Audit committees that are not engaging in these processes should consider doing so. A demonstration of strong interest in these issues can have a positive effect on the quality of disclosure."

In February 2018, the SEC issued guidance regarding disclosures involving cybersecurity risk and incidents, and in October, the Commission released an investigative report cautioning companies to consider cyber threats when implementing internal accounting controls. The guidance and investigative report serve as reminders for companies to assess their internal accounting controls and disclosure controls and procedures in light of the current cyber risk environment.

Focus internal audit on the company's key risks beyond financial reporting and compliance.

As recent headlines demonstrate, failure to manage key risks—such as tone at the top; culture; legal/regulatory compliance; incentive structures; cybersecurity; data privacy; global supply chain and outsourcing risks; and environmental, social, and governance risks—can potentially damage corporate reputations and impact financial performance. The audit committee should work with the chief audit executive to help identify the risks that pose the greatest threat to the company's reputation, strategy, and operations and help ensure that internal audit is focused on those risks and related controls. Is the audit plan risk-based and flexible enough to adjust to changing business and risk conditions? Have there been changes in the operating environment? What are the risks posed by the company's digital transformation and by the company's extended organization—sourcing, outsourcing, sales, and distribution channels? Is the company sensitive to early warning signs regarding safety, product quality, and compliance? Is internal audit helping to assess and monitor the company's culture? Set clear expectations and help ensure that internal audit has the resources, skills, and expertise to succeed and help the chief audit executive think through the impact of digital technologies on internal audit.

About the KPMG Board Leadership Center
The KPMG Board Leadership Center champions outstanding governance to help drive long-term corporate value and enhance investor confidence. Through an array of programs and perspectives—including KPMG's Audit Committee Institute, the WomenCorporateDirectors Foundation, and more—the Center engages with directors and business leaders to help articulate their challenges and promote continuous improvement of public- and private-company governance. Drawing on insights from KPMG professionals and governance experts worldwide, the Center delivers practical thought leadership—on risk and strategy, talent and technology, globalization and compliance, financial reporting and audit quality, and more—all through a board lens. Learn more at kpmg.com/us/blc.

About the Audit Committee Institute
As part of the Board Leadership Center, KPMG's Audit Committee Institute focuses on oversight of financial reporting and audit quality and other issues of interest to audit committee members, including risk oversight, internal controls, and compliance. Learn more at kpmg.com/us/aci.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

Contact us

kpmg.com/us/blc
T: 1-800-808-5764
E: us-kpmgmktblc@kpmg.com