In this issue

04 The evolving role of the board in cybersecurity risk oversight
New regulatory and reporting developments at the federal, state and global levels have made cybersecurity risk oversight more challenging. We highlight these developments and offer keys for effective board oversight of cyber risk management.

08 Audit committee reporting to shareholders in 2017
Our annual review of Fortune 100 proxy materials shows a continued rise in voluntary audit-related disclosures. We provide the details and sample language for select disclosures.

12 PCAOB adopts final standard to significantly change the auditor’s report
The final standard requires auditors to report information about critical audit matters and audit tenure. Find out what you need to know.
The evolving role of the board in cybersecurity risk oversight

Cybersecurity continues to be front and center on board agendas. Every time a cyber attack hits the headlines, board members and other stakeholders are reminded of the possible material threat such incidents pose. New regulatory and reporting developments at the federal, state and even global levels have made cybersecurity risk oversight even more challenging.

Board members seek assurances from management that their cyber risk management programs will reduce the risk of attacks and, when necessary, will detect, respond and recover from any attack that does happen. Investors, customers, business partners and regulators are looking for this information as well.

Evolving regulations

The European Union has adopted the General Data Protection Regulation (GDPR), which will take effect in May 2018. This regulation affects all companies doing business in the EU or collecting personally identifiable information (PII) from EU citizens.

The GDPR establishes enhanced individual privacy rights and places additional requirements on companies to notify the proper national authorities of a breach within 72 hours. It further requires specific data protection safeguards, particularly requiring the appointment of a senior-level data protection officer.

Failure to comply with the GDPR, once it takes effect next year, can result in fines of up to 4% of global revenue.

The future of US regulation is less clear, but board members should be aware of recent developments. Nationally, the Federal Deposit Insurance Corporation, the Federal Reserve and the Comptroller of the Currency issued a joint advance notice of proposed rulemaking (ANPR) last year regarding enhanced cyber risk management standards. These new standards would apply to the financial services sector – banks, other financial companies and those entities in adjacent sectors that serve them (e.g., cloud service providers).

The potential regulations outlined in the ANPR aim to increase the operational resilience of large, interconnected entities and decrease the impact on the financial system in the case of a cyber event experienced by any one organization.

The comment period for this ANPR closed early this year, and the final form of any joint regulation these agencies will
hand down is to be determined. Given the far-reaching list of organizations that will be affected by these rules, board members of nonfinancial services companies will want to be aware of their decision.

Regulators in several other sectors have also proposed or issued guidance. Additionally, there are 12 House and Senate committees with some jurisdiction over cybersecurity, so there is a chance we will see legislation regarding these issues as well.

At the state level, New York made a splash earlier this year with a significant regulation that affects the financial services sector, and now other states are looking to add their own unique regulations. It is a significant challenge for management and boards to navigate through this period of disparate and increasing regulations.

With significant changes pending, we do see common themes for board members to focus on:

- Understanding the cyber risks facing the organization and how they may affect the business
- Challenging the effectiveness of the organization's cybersecurity risk management program, and supporting the continued evolution of the program (e.g., promoting a risk-aware culture and a holistic risk management strategy, balancing cost and value derived)
- Understanding the IT assets that connect to the organization's network
- Monitoring the effectiveness of the organization's vendor risk management program
- Determining how well the monitoring and incident response programs work

Finally, President Trump issued an executive order on cybersecurity in May that could result in changes affecting a variety of companies. The order mandates a variety of reports on the state of cybersecurity throughout the government and the country. The findings of those reports could potentially lead to new requirements.

Cybersecurity risk is a fast-moving concern for organizations of all types and should be considered as part of the organization's enterprise risk management. Board members will continue to contend with this issue for years to come. Keeping abreast of regulatory developments and ensuring they have the information they need to evaluate risk and how it is addressed will be key to informed oversight now and into the future.

Other stakeholders

Regulators are not the only parties interested in ensuring that organizations minimize their risk of cyber attacks and related losses. Individuals and other stakeholders want to know their information is safe, and investors and business partners are also concerned about how cyber attacks would affect them.

Some institutional investors have been asking boards about their organizations’ cybersecurity risk management programs as a way to gauge the risk to their investments.

Keys to effective board oversight of cyber risk management

Many boards task their audit committees with overseeing matters related to cybersecurity. In order for audit committees to be successful in managing these risks, they must have three things:

- **Clarity** with regard to the cyber risk management program
- **Confidence** in the program’s adequacy
- **Assurance** in the information that they receive

The audit committee needs particular clarity into the specific cyber risks the organization faces, the governance structure assigning accountability for key aspects of the program, how the program aligns with the organization’s identified risks and sector frameworks, as well as the “true maturity” of the program.
Finally, the board or assigned committee needs to be clear about how the cybersecurity risk management program aligns with the organization’s overall enterprise risk management program and its business objectives.

When discussing the “maturity” of the program, we see parallels to the implementation of Section 404 of Sarbanes-Oxley (SOX 404). In the initial period between the issuance of the standard and its implementation, most organizations were relatively confident in their internal controls and their ability to meet the SOX 404 requirements. They subsequently came to realize that their processes and controls were not fully mature in several areas:

- The processes and controls were not adequately documented or consistently applied across the organization.
- They were not built to respond to the organization’s key underlying risks.
- The compliance level was not adequate.

We believe that if boards look closely, many will find similar areas where the maturity of their cybersecurity risk management programs can be improved. As with the adoption of SOX 404, the effort required to adequately mature a program could be significant. Accordingly, the decision to undertake such a journey should be aligned with the overall risk to the organization.

Challenges to full clarity, confidence and assurance

Board members we talk to find that their prime challenge in this area is obtaining relevant, objective and reliable information, presented in business-centric terms. This affects board members’ ability to understand the risks facing their organizations and evaluate management’s response to these risks.

Consider the fact that most cybersecurity programs have been built in a piecemeal manner over time as cyber threat vectors and associated risks are identified (or as they evolve). As a result, the “maturity” of key components of the program and their alignment may vary considerably within an organization.

Organizations often conduct periodic assessments to try and address this concern, but the value of these efforts will vary based on the experience of the group performing the assessment, the scope of the assessment, and the depth and breadth of the procedures performed.

Finally, the members of management who brief the board on these matters tend to be highly technical professionals who are challenged to align their communications with the organization’s enterprise-wide risk management strategy and business objectives.
AICPA guidance as a possible measure

If these concerns strike a chord for board members, one possible solution has emerged in the form of the AICPA guidance for evaluating and reporting on an organization’s cybersecurity risk management program and underlying controls.

Use of the new AICPA guidance is completely voluntary – it is not required by any outstanding or proposed legislation or regulation. It contains a set of robust, business-centric evaluation criteria designed to ascertain the adequacy of the processes and controls implemented to address the organization’s cyber risks. It can be used to identify gaps, design remediation activities to fill those gaps or as part of a full attestation engagement.

The guide was developed after a review of a variety of frameworks, including the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), with which many board members are familiar.

Voluntary use of the AICPA guide could help board members ensure they have complete, useful information to fulfill their oversight role. It also can give board members a measure by which to compare their organizations’ risk management efforts. Finally, it offers answers to questions from investors and a possible differentiator to reassure customers and clients.

Questions for the board to consider

• How is the organization’s cybersecurity risk management approach aligned with or folded into its overall enterprise risk management process?

• Is the organization’s approach to cybersecurity risks and associated privacy issues aligned to the requirements of the European General Data Protection Regulation (GDPR), and will it be ready for the May 2018 enforcement deadline?

• How is the organization prepared to comply with the GDPR’s 72-hour cyber breach notification policy?

• How frequently is the maturity of the organization’s cybersecurity risk management framework being assessed and evaluated?

• How is the organization monitoring for new and potential cybersecurity regulatory changes and complying with new legal requirements?
Audit committee reporting to shareholders in 2017

Executive summary

For the sixth consecutive year, the EY Center for Board Matters reviewed audit committee-related proxy disclosures by Fortune 100 companies to examine trends in voluntary reporting and finds a continued increase in voluntary audit committee disclosures to shareholders. Year-over-year growth in voluntary audit-related disclosures in 2017 filings was similar to that seen in 2015 and 2016, indicating that companies and audit committees continue to reflect upon and make changes to the information that they communicate to shareholders.

As discussed in our previous reports, audit committees have significant responsibilities related to oversight of financial reporting at public companies. These responsibilities were codified in the Sarbanes-Oxley Act of 2002 (SOX or the Act), now in its 15th year. For more information about the impact of SOX, see our Sarbanes-Oxley Act at 15 publication.

In recent years, investors, regulators and other stakeholders have taken a closer look at the important role of boards — and audit committees in particular — in supporting high-quality financial reporting and have sought greater transparency around the audit and oversight of financial reporting. This interest in transparency may be due in part to the fact that, even as the obligations of audit committees have expanded over the years, required audit committee disclosures have not; rather, disclosure obligations in this area pre-date SOX.

Companies and audit committees have responded to this interest by voluntarily providing enhanced audit-related disclosures, even without a change in regulatory requirements. While transparency has increased at a steady pace over the past three years, several recent and upcoming regulatory developments, such as the Public Company Accounting Oversight Board’s (PCAOB) revised standard on the auditor’s report and the U.S. Securities and Exchange Commission’s (SEC) ongoing disclosure effectiveness project, may contribute to further consideration of audit-related disclosures in the coming years.¹

This document examines key audit-related proxy disclosures from 2012 to 2017 in order to promote discussion regarding audit committee communications with stakeholders. Due to investor interest in board composition and activities, it also provides a snapshot of how certain characteristics of audit committees have changed from 2012 to today.
Findings

Our research into 2017 proxy materials showed similar increases in voluntary audit-related disclosure as in the past several years, with steady growth in certain areas. We conducted this analysis by looking at the proxy materials of 75 companies on the 2017 Fortune 100 list that filed proxy statements each year from 2012 to 2017 for annual meetings through August 15, 2017 (companies that have not yet held their 2017 annual meeting are excluded).1 Highlights from our findings include:

Disclosure of audit oversight responsibilities

- The percentage of companies that explicitly stated that the audit committee is responsible for the appointment, compensation and oversight of the external auditor has nearly doubled since 2012, increasing to 87% in 2017, up from 81% in 2016 and 45% in 2012.

Auditor assessment disclosures

- The percentage of companies disclosing the factors used in the audit committee’s assessment of the external auditor’s qualifications and work quality increased from 48% in 2016 to 56% in 2017. In 2012, 17% of companies made such disclosures.

Disclosure of interactions with auditor

- The level of disclosure about the topics discussed by the auditor and audit committee continues to be low, with only 3%-4% of companies providing such information between 2012 and 2017. It will be interesting to observe whether these numbers change in the years ahead following the adoption of the PCAOB’s new auditor reporting standard (assuming the SEC adopts the standard), which will require auditor disclosures regarding critical audit matters discussed with the audit committee.

Disclosure regarding lead audit partner selection

- While in 2012 only 1% of companies disclosed that the audit committee was involved in the selection of the lead audit partner, this rose to 75% in 2017. In 2016, it was 69%.

Independence-related disclosures

- The percentage of audit committees that explicitly stated in the audit committee report that they are independent from management rose from 59% in 2016 to 64% in 2017.

- Since 2012, the percentage of companies that state that the audit committee considers non-audit fees and services when assessing auditor independence rose dramatically, from 15% in 2012 to 84% in 2017.

Fee-related disclosures

- Disclosures relating to audit fees have changed substantially since 2012, when none of the Fortune 100 companies disclosed that the audit committee is responsible for fee negotiations with the auditor. In 2017, 32% of the companies did so, compared to 27% in 2016.

- In 2017, 43% of companies provided an explanation for a change in fees paid to the external auditor (including audit, audit-related, tax and other fees), while 31% did so in 2016 and 11% in 2012. Breaking this figure down further:

  - Our research shows that companies tend to provide explanatory disclosures more frequently when audit fees rise and are less inclined to do so when they decline. In 2017, of the companies that paid audit fees that were more than 5% higher than in 2016, 29% provided an explanation for the fee increase. For companies that paid audit fees that were more than 5% lower than in 2016, only 9% provided explanatory disclosures.

Endnotes


## Trends in audit committee disclosures

<table>
<thead>
<tr>
<th>Category</th>
<th>Topic</th>
<th>2017 % of total</th>
<th>2016 % of total</th>
<th>2015 % of total</th>
<th>2014 % of total</th>
<th>2013 % of total</th>
<th>2012 % of total</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Disclosures in the audit committee report</strong></td>
<td>Statement that the audit committee is independent</td>
<td>64%</td>
<td>59%</td>
<td>60%</td>
<td>56%</td>
<td>52%</td>
<td>55%</td>
</tr>
<tr>
<td></td>
<td>Name of the audit firm is included in the audit committee report</td>
<td>77%</td>
<td>76%</td>
<td>75%</td>
<td>75%</td>
<td>76%</td>
<td>76%</td>
</tr>
<tr>
<td><strong>Audit committee composition</strong></td>
<td>Audit committee with one financial expert (FE)</td>
<td>17%</td>
<td>28%</td>
<td>27%</td>
<td>32%</td>
<td>29%</td>
<td>29%</td>
</tr>
<tr>
<td></td>
<td>Audit committee with two FEs</td>
<td>35%</td>
<td>21%</td>
<td>27%</td>
<td>29%</td>
<td>51%</td>
<td>37%</td>
</tr>
<tr>
<td></td>
<td>Audit committee with three or more FEs</td>
<td>48%</td>
<td>51%</td>
<td>47%</td>
<td>39%</td>
<td>20%</td>
<td>33%</td>
</tr>
<tr>
<td><strong>Audit committee responsibilities re: external auditor</strong></td>
<td>Explicit statement that the audit committee is responsible for appointment, compensation and oversight of external auditor</td>
<td>87%</td>
<td>81%</td>
<td>80%</td>
<td>69%</td>
<td>56%</td>
<td>45%</td>
</tr>
<tr>
<td><strong>Identification of topics discussed</strong></td>
<td><strong>Topics discussed by the audit committee and external auditor</strong></td>
<td>3%</td>
<td>3%</td>
<td>4%</td>
<td>4%</td>
<td>4%</td>
<td>4%</td>
</tr>
<tr>
<td><strong>Fees paid to the external auditor</strong></td>
<td>Statement that the audit committee considers non-audit fees/services when assessing auditor independence</td>
<td>84%</td>
<td>81%</td>
<td>81%</td>
<td>77%</td>
<td>77%</td>
<td>15%</td>
</tr>
<tr>
<td></td>
<td>Statement that the audit committee is responsible for fee negotiations</td>
<td>32%</td>
<td>27%</td>
<td>24%</td>
<td>15%</td>
<td>7%</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td>Explanation provided for change in fees paid to external auditor</td>
<td>43%</td>
<td>31%</td>
<td>23%</td>
<td>21%</td>
<td>16%</td>
<td>11%</td>
</tr>
<tr>
<td><strong>Assessment of the external auditor</strong></td>
<td>Disclosure of factors used in the audit committee's assessment of the external auditor qualifications and work quality</td>
<td>56%</td>
<td>48%</td>
<td>40%</td>
<td>32%</td>
<td>20%</td>
<td>17%</td>
</tr>
<tr>
<td></td>
<td>Statement that audit committee involved in lead partner selection</td>
<td>75%</td>
<td>69%</td>
<td>65%</td>
<td>48%</td>
<td>15%</td>
<td>1%</td>
</tr>
<tr>
<td></td>
<td>Disclosure of the year the lead audit partner was appointed</td>
<td>16%</td>
<td>12%</td>
<td>11%</td>
<td>8%</td>
<td>3%</td>
<td>3%</td>
</tr>
<tr>
<td></td>
<td>Statement that choice of external auditor is in best interest of company and/or shareholders</td>
<td>73%</td>
<td>72%</td>
<td>63%</td>
<td>47%</td>
<td>20%</td>
<td>3%</td>
</tr>
<tr>
<td><strong>Tenure of the external auditor</strong></td>
<td>Disclosure of the length of the external auditor tenure</td>
<td>67%</td>
<td>65%</td>
<td>64%</td>
<td>56%</td>
<td>32%</td>
<td>27%</td>
</tr>
<tr>
<td></td>
<td>Statement that the audit committee considers the impact of changing auditors when assessing whether to retain the current external auditor</td>
<td>60%</td>
<td>55%</td>
<td>49%</td>
<td>33%</td>
<td>16%</td>
<td>3%</td>
</tr>
<tr>
<td><strong>Accessibility of audit committee charters from proxy statements</strong> (link in proxy statement goes directly to)</td>
<td>Audit committee and/or all committee charters</td>
<td>12%</td>
<td>12%</td>
<td>16%</td>
<td>16%</td>
<td>11%</td>
<td>8%</td>
</tr>
<tr>
<td></td>
<td>Company main website</td>
<td>39%</td>
<td>37%</td>
<td>39%</td>
<td>40%</td>
<td>41%</td>
<td>44%</td>
</tr>
<tr>
<td></td>
<td>Company site for investor relations</td>
<td>24%</td>
<td>24%</td>
<td>24%</td>
<td>27%</td>
<td>27%</td>
<td>25%</td>
</tr>
<tr>
<td></td>
<td>Company site for corporate governance</td>
<td>25%</td>
<td>27%</td>
<td>21%</td>
<td>17%</td>
<td>21%</td>
<td>23%</td>
</tr>
</tbody>
</table>

Notes: Percentages based on total disclosures for audit committees each year. Data based on the 75 companies on the 2017 Fortune 100 list that filed proxy statements each year during 2012-17 and held annual meetings through 15 August 2017.
Disclosure observations and sample language from Fortune 100 proxy statements

**Topics discussed by the audit committee and external auditor**
Companies making these disclosures indicated that the audit committee raised certain topics with their external auditors other than those required by regulations.

**Sample language**
“Management, the internal auditors and the independent auditors also made presentations to the audit committee throughout the year on specific topics of interest, including the company’s: (i) enterprise risk assessment process; (ii) information technology systems and controls; (iii) income tax strategy and risks; (iv) derivatives policy and usage; (v) benefit plan fund management; (vi) 20XX integrated audit plan; (vii) updates on completion of the audit plan; (viii) critical accounting policies; (ix) assessment of the impact of new accounting guidance; (x) compliance with the internal controls required under Section 404 of SOX; (xi) ethics and compliance program; (xii) risk management initiatives and controls for various acquisitions and business units; (xiii) strategy and management of the implementation of new systems; and (xiv) cybersecurity.”

**Explanation provided for change in fees paid to external auditor**
Most companies provide an explanation for the types of services included within each fee category. The companies highlighted in this row explained the circumstances for the change.

**Sample language**
“... year-over-year increase largely driven by the ABC acquisition.”

**Disclosure of factors used in the audit committee’s assessment of the external auditor qualifications and work quality**
Companies that included this information provided examples of the criteria used in auditor assessments.

**Sample language**
“In evaluating and selecting the company’s independent registered public accounting firm, the Audit Committee considers, among other things, historical and recent performance of the current independent audit firm, an analysis of known significant legal or regulatory proceedings related to the firm, external data on audit quality and performance, including PCAOB reports, industry experience, audit fee revenues, firm capabilities and audit approach, and the independence and tenure of the audit firm.”

**Statement that the audit committee considers the impact of changing auditors when assessing whether to retain the current external auditor**
These companies indicated that the audit committee considered alternatives to retaining the incumbent external auditor.

**Sample language**
“The Committee engages in an annual evaluation of the independent public accounting firm’s qualifications, assessing the firm’s quality of service, the firm’s sufficiency of resources, the quality of the communication and interaction with the firm, and the firm’s independence, objectivity and professional skepticism. The Committee also considers the advisability and potential impact of selecting a different independent public accounting firm.”

---

**Characteristics of Fortune 100 audit committees – 2017 vs. 2012**
The composition of boards is a current area of great interest to many institutional investors. Below is data regarding the composition and activities of audit committees in 2017 as compared to 2012. While the data in several areas did not change, notable exceptions included:

- Increases in the percentage of audit committee members that are identified as financial experts (66% in 2017 vs. 59% in 2012) and those that are women (26% in 2017 vs. 19% in 2012).
- Degree of turnover in audit committee chairs (41%), as well as the percentage of audit committees (85%) that gained new members between 2012 and 2017.

<table>
<thead>
<tr>
<th>Fortune 100 audit committees</th>
<th>2017</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Audit committee characteristics</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Independence</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>Size (number of committee members)</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Financial experts</td>
<td>66%</td>
<td>59%</td>
</tr>
<tr>
<td>Women audit committee members</td>
<td>26%</td>
<td>19%</td>
</tr>
<tr>
<td>Meeting frequency (number of meetings per year)</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>Board tenure (average number of years on board)</td>
<td>8</td>
<td>7</td>
</tr>
<tr>
<td>Age</td>
<td>63</td>
<td>63</td>
</tr>
<tr>
<td><strong>Changes since 2012</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit committees that experienced chair turnover</td>
<td>41%</td>
<td></td>
</tr>
<tr>
<td>Audit committees that added at least one new member</td>
<td>85%</td>
<td></td>
</tr>
<tr>
<td>Average percentage of new members on audit committees that added at least one new member</td>
<td>49%</td>
<td></td>
</tr>
</tbody>
</table>

**Questions for audit committees to consider**

- To what extent does the audit committee already provide voluntary audit or audit-related disclosures?
- Have investors expressed interest in greater transparency in the audit committee’s work in connection with broader company-investor engagement conversations?
- How has the role of the audit committee evolved in recent years (e.g., oversight of the ERM process, cybersecurity risk) – and to what extent are these changes being communicated to stakeholders via the proxy statement?
- What additional voluntary disclosures might be useful to shareholders related to the audit committee’s time spent on certain activities, such as company restructuring or financial statement reporting developments?
PCAOB adopts final standard to significantly change the auditor’s report

The standard requires auditors to report information about critical audit matters and auditor tenure.

What you need to know

• The PCAOB adopted a final standard that requires auditors to include significantly more information in their auditor’s reports. The standard is subject to approval by the SEC, and interested parties will have an opportunity to provide comments.

• The standard requires auditors to include in the report information about matters that they communicated or were required to communicate to the audit committee that relate to material accounts or disclosures and involved especially challenging, subjective or complex auditor judgment. These requirements are effective for annual periods ending on or after 30 June 2019 for large accelerated filers and 15 December 2020 for all other filers.

• The standard requires auditors to add information about auditor tenure, clarify the language about the auditor’s responsibilities and change the organization and format of the report. Those requirements are effective for audits of financial statements for annual reporting periods ending on or after 15 December 2017.

Overview

The Public Company Accounting Oversight Board (PCAOB or Board) adopted a final auditing standard aimed at making the auditor’s report more relevant and informative for investors and other financial statement users. The standard retains the pass/fail audit opinion but requires auditors to include in their reports:

• A discussion of critical audit matters (CAMs), which the standard defines as items communicated to the audit committee or required to be communicated to the audit committee that related to accounts or disclosures that are material to the financial statements and involved especially challenging, subjective or complex auditor judgment

• Information on auditor tenure

• A statement that auditors are required to be independent

• The phrase “whether due to error or fraud” in the description of the auditor’s responsibilities to obtain reasonable assurance about whether the financial statements are free of material misstatement

The standard, which is subject to approval by the Securities and Exchange Commission (SEC), also standardizes the format of the auditor’s report by requiring auditors to first state their opinion and include section titles. The final standard is substantially the same as the standard the PCAOB proposed in 2016.
The standard generally applies to audits conducted under PCAOB standards, but CAMs do not have to be communicated for audits of brokers and dealers reporting under the Securities Exchange Act of 1934 Rule 17a-5; investment companies other than business development companies; employee stock purchase, savings and similar plans; and emerging growth companies.

Other standard-setting bodies around the world have already made similar changes to the auditor’s report. International Standards on Auditing (ISA) require discussion of key audit matters (KAMs) in auditor’s reports on financial statements for periods ending on or after 15 December 2016. The European Union will require an expanded auditor’s report for periods ending on or after 30 June 2017.

Key considerations

Critical audit matters

The standard defines CAMs as matters communicated to the audit committee or required to be communicated to the audit committee related to accounts or disclosures that are material to the financial statements and that involved especially challenging, subjective or complex auditor judgment. In determining whether a matter involved especially challenging, subjective or complex auditor judgment, the auditor is required to take into account, alone or in combination, factors including:

- The auditor’s assessment of the risks of material misstatement, including significant risks
- The degree of auditor judgment related to areas in the financial statements that involved the application of significant judgment or estimation by management, including estimates with significant measurement uncertainty
- The nature and timing of significant unusual transactions and the extent of audit effort and judgment related to these transactions
- The degree of auditor subjectivity in applying audit procedures to address the matter or in evaluating the results of those procedures
- The nature and extent of the audit effort required to address the matter, including the extent of specialized skill or knowledge needed or the nature of consultations outside the engagement team regarding the matter
- The nature of audit evidence obtained regarding the matter

The final rule requires auditors to evaluate the same population of items the PCAOB proposed in 2016. However, the standard doesn’t list required CAMs or set an expectation that certain items will be CAMs in all cases (e.g., matters considered significant risks may be CAMs in certain cases but not in others). As a result, for example, while revenue recognition is presumed to be a fraud risk and all fraud risks are significant risks under PCAOB standards, a matter related to revenue recognition that did not involve especially challenging, subjective or complex auditor judgment will not be considered a CAM under the standard. The standard also requires auditors to document in their workpapers their reasons for determining whether each matter communicated or required to be communicated to the audit committee is a CAM.

An auditor that does not identify any CAMs is required to include a statement to that effect in the “Critical Audit Matters” section of the auditor’s report. However, the Board said in the standard that it expects that, in most audits, the auditor will identify at least one CAM.
For each CAM, auditors are required to (1) identify the matter, (2) describe the principal considerations in determining that the matter was a CAM, (3) describe how the matter was addressed in the audit and (4) refer to the relevant financial statement accounts or disclosures.

Auditors could satisfy the requirement to describe how they addressed each CAM by (1) describing their response or approach that was most relevant to the matter; (2) providing a brief overview of procedures performed; (3) providing an indication of the outcome of those procedures; or (4) providing key observations with respect to the matter, or a combination of these elements. The final standard does not prescribe specific items to be included.

The definition of a CAM and the requirements to determine and describe a CAM are substantially the same as what the PCAOB proposed in 2016.

The Board did not make any changes to the standard in response to concerns we and others raised about the possibility that the auditor might have to disclose information that the company has not previously disclosed. However, in the adopting release, the PCAOB discussed the application of the standard to matters that don’t relate to accounts or disclosures that are material to the financial statements and therefore cannot be CAMs. The discussion included examples related to (1) a potential loss contingency that was communicated to the audit committee but was determined to be remote and was not recorded in the financial statements or disclosed, (2) a potential illegal act that the company wasn’t required to disclose and (3) the determination, by itself, that there is a significant deficiency in internal control over financial reporting.

**How we see it**
- The discussion of these items in the adopting release should help mitigate the possibility that auditors might disclose original information.
- The PCAOB’s definition of a CAM is largely aligned with the ISA definition of a key audit matter, but there are differences that may result in different outcomes.

The standard notes that the language used to communicate a CAM should not imply that the auditor is providing a separate opinion on the CAM or on the accounts or disclosures to which it relates. The standard says it also would not be appropriate for the auditor to use language that could call into question the auditor’s responsibility for the CAMs or the auditor’s opinion on the financial statements, taken as a whole.
If the SEC approves the standard, these requirements will be effective for annual periods ending on or after 30 June 2019 for large accelerated filers and reporting periods ending on or after 15 December 2020 for all other filers.

Other changes to the auditor’s report
The standard requires the auditor’s report to include the year the auditor began serving consecutively as the company’s auditor. The PCAOB said its intent is for the disclosure to reflect the entire relationship between the company and the auditor, including the tenure of predecessor accounting firms and predecessors to the company being audited. Auditors that are uncertain about the length of their relationship with a company must state that fact and provide the earliest year that they are sure of.

The standard also revises the language in the auditor’s report to add a statement that the auditor is required to be independent and add the phrase “whether due to fraud or error” to the description of the auditor’s responsibility to obtain reasonable assurance that the financial statements are free of material misstatement. In addition, it revises the format of the auditor’s report to require that the auditor’s opinion paragraph be the first section of the report and to require the use of section titles.

If the SEC approves the standard, these changes will be effective for audits of financial statements for annual periods ending on or after 15 December 2017.

How we see it
Determining auditor tenure may require research when there have been audit firm or company mergers, acquisitions or other changes in ownership structure.

What’s next
The final standard is subject to approval by the SEC, and interested parties will have an opportunity to provide comments. Management and audit committees should familiarize themselves with the requirements of the standard.

Endnotes
3 ISA 701, Communicating Key Audit Matters in the Independent Auditor’s Report, and ISA 700 (Revised), Forming an Opinion and Reporting on Financial Statements.
Looking for more?
Access additional information and thought leadership from the EY Center for Board Matters at ey.com/boardmatters.