Introduction

In our annual review of developments affecting audit committees, we consider the significant responsibilities the committee has in assisting the board in its oversight of the integrity of the company's financial statements; compliance with legal and regulatory requirements; the qualifications, independence, performance of the external auditor and the company's internal audit functions; risk management; and other assigned duties. We hope this summary of year-end issues for audit committees is useful to audit committee members as they prepare for discussions with the board, management and external auditors.
Financial reporting

Background

With the mandatory adoption dates of significant new accounting standards looming, and continued investor and regulatory scrutiny of public company disclosures, audit committees will be focused on helping to certify that management is on track with implementation plans and ready to make required disclosures on a timely and accurate basis. Throughout this year, the staff of the Securities and Exchange Commission (SEC) has been reminding companies to plan for action and appropriate disclosure on the new revenue recognition, lease and credit loss standards, most recently stating that companies should:1

Revenue recognition

The Financial Accounting Standards Board’s (FASB) new revenue recognition standard will be effective for calendar year-end registrants beginning in 2018. The standard requires several new disclosures that are intended to provide investors with information about the nature, amount, timing and uncertainty of revenue and cash flows from customers. Once they adopt the new standard, registrants may need to make more disclosures about the judgments and assumptions underlying revenue recognition within their management’s discussion and analysis (MD&A) of critical accounting estimates. Companies should re-evaluate the need for and sufficiency of their critical accounting estimate disclosures related to revenue recognition. The SEC staff will be carefully reviewing these disclosures and also the transition disclosures required under SAB 74, Disclosure of the Impact that Recently Issued Accounting Standards Will Have on the Financial Statements of the Registrant when Adopted in a Future Period.

Leases

The FASB's new leasing standard will be effective for calendar year-end registrants beginning in 2019. The standard requires lessees to recognize on their balance sheets an asset and liability for nearly all leases. The SEC staff explains that the standard will require several steps, including identifying relevant legal contracts, evaluating whether an arrangement is or contains a lease and applying the new leases standard to arrangements within its scope. These steps can potentially be time consuming and so implementation planning should be ongoing, if not concurrent, with revenue recognition.

Credit losses

The FASB’s new credit loss standard will be effective for calendar year-end registrants beginning in 2020. The standard changes the timing of credit loss recognition and requires additional disclosures that would facilitate assessment of management’s initial credit loss.

Further discussion

• Keep going and get going
• Address internal controls over financial reporting (ICFR) as new accounting standards are planned and implemented
• Provide transparent transition disclosures under Staff Accounting Bulletin No. 74 (SAB 74), Disclosure of the Impact that Recently Issued Accounting Standards Will Have on the Financial Statements of the Registrant when Adopted in a Future Period
• Prepare useful and complete disclosures as required by the new standards
• Use well-reasoned judgment in implementing the new standards

The SEC staff further said that audit committees should maintain the right “tone at the top” to create an environment and culture that supports the integrity of the financial reporting process and promotes management’s successful implementation of the new generally accepted accounting principles (GAAP) standards.
estimate for newly originated loans, as well as subsequent changes to those estimates. Application of the new standard may result in the earlier recognition of expected losses on loans.²

**Derivative settled-to-market treatment of centrally cleared contracts and hedge accounting**

In January 2017, certain clearing houses amended their rulebooks to legally characterize variation margin payments for over-the-counter derivatives they clear as settlements rather than collateral. Audit committees should make sure the impacts of these changes are reflected in the financial statements and clearly disclosed. Additionally, the FASB recently issued its amended guidance, Accounting Standards Update No. 2017-12 — Derivatives and Hedging (Topic 815): Targeted Improvements to Accounting for Hedging Activities. The new standard will impact current hedging practices and allow more hedging and risk management strategies to qualify for hedge accounting, along with other implications. Early adoption is permitted starting in the third quarter of 2017, and audit committees should inquire of management regarding their plans around implementation.

**Pay ratio disclosures**

The SEC finalized a rule that will require most registrants to provide pay ratio disclosures for the first time in 2017 proxy statements. While compensation committees have taken the lead on addressing the pay ratio disclosure requirement, audit committees should work with the compensation committee to help establish the reasonableness of the estimates and methodologies used to calculate the pay ratio, and also inquire about any disclosure controls and procedures developed to address the disclosure requirement.³

**SEC comment letter trends**

The SEC staff continues to question registrants’ disclosures related to significant judgments and estimates, including those related to segment reporting, goodwill impairment, income taxes and revenue recognition. Audit committees should understand SEC staff comments and trends to inform their oversight of financial reporting, especially as the SEC continues to encourage registrants to streamline disclosures and make them more meaningful. Some of the SEC focus areas are highlighted below.

**Focus on non-GAAP financial measures**

Since the SEC staff released updated Compliance and Disclosure Interpretations (C&DIs) to provide more explicit guidance on when non-GAAP measures may violate SEC rules, many of the staff’s comments have focused on compliance with the updated interpretations in earnings releases as well as registrants’ periodic reports. Audit committees should continue monitoring compliance with updated C&DIs and have their organizations exercise caution when disclosing non-GAAP financial measures.

**Management’s discussion and analysis (MD&A)**

The SEC staff has increased its focus on performance metrics, including whether registrants have disclosed key operating metrics monitored by management and how those metrics correlate to material changes in the results of operations. The SEC staff also continues to focus on the discussion of critical accounting estimates in MD&A, requesting more insight and robust analysis than what is required to be disclosed in the significant accounting policies note to the financial statements. Along these lines, the SEC staff may ask a registrant to disclose key performance indicators in its SEC filings if it provides those metrics in other communications (e.g., websites, press releases, analyst presentations) to help investors view the registrant through the eyes of management.

As always, audit committees should ask management whether additional MD&A disclosures are needed to address the expected implications of geopolitical factors and economic trends, such as fluctuations in regulations, energy prices, interest rates and foreign currency exchange rates.
Registrants may need to enhance disclosures of risk factors, market risk disclosures, critical accounting estimates or known trends and uncertainties in MD&A (and related language regarding forward-looking disclosures) to address expected changes in operations, financial results, liquidity or financial statement measurements that could reasonably be materially affected by these developments.

**Cybersecurity**

SEC Chairman Jay Clayton and leading SEC staff have been encouraging more robust cybersecurity disclosures and have recommended that registrants consider the guidance in CF Disclosure Guidance: Topic No. 2, *Cybersecurity* (published in 2011) when evaluating whether to disclose information about risks and incidents involving cybersecurity. The SEC has further indicated that registrants must take their cybersecurity disclosure obligations seriously and failure to do so may result in enforcement action. Boards and audit committees should make sure that organizations disclose all material cybersecurity risks or cyber incidents and have a plan in place for potential disruptions.

**Focus on integrated risk and controls**

ICFR is not effective if a “material weakness” exists at the end of a company’s fiscal year-end. The SEC and Public Company Accounting Oversight Board (PCAOB) each stress that audit committees, management and external auditors need to appropriately assess whether a “significant deficiency” in ICFR should actually be defined as a material weakness. SEC enforcement actions explain the need for audit committees to appropriately address significant deficiencies that are reported to them.\(^4\)

Besides this, many companies will need to make certain that their ICFR appropriately incorporates the implementation of the new GAAP standards noted above, as well as other emerging issues and new regulations impacting their financial reporting. Audit committees should discuss with management the processes and systems that support the quarterly CEO and CFO certifications on ICFR, and should actively support a culture and environment that promotes the integrity of financial reporting through strong ICFR and other programs.

---

**Questions to consider**

1. What changes to ICFR have been designed and what key actions have been taken by management to implement the new revenue recognition, lease, credit loss and other FASB standards in process? What key actions are needed to improve readiness for implementation and disclosure?

2. What is the company’s plan for periodically updating the disclosures under SAB 74 on the effect of new accounting standards?

3. Did the entity consider the impacts of changes in revenue recognition patterns on cost and margin recognition, as well as other effects of the new standard, such as financial covenants, incentive plans, etc.? What disclosures has management provided or considered on these changes?

4. Has the organization considered the guidance in CF Disclosure Guidance: Topic No. 2, *Cybersecurity*, and reassessed its risk management governance and related disclosures around cybersecurity risks to address any developments in operations and the evolving nature of cyber threats?

5. What new disclosure controls has management implemented to address compliance with new SEC staff guidance?

---

**Additional references**

- SEC Comments and Trends: An analysis of current reporting issues
- Financial reporting development resources are available on EY AccountingLink
Boards and audit committees should make sure that organizations disclose all material cybersecurity risks or cyber incidents and have a plan in place for potential disruptions.
Tax

Background

Tax policy (including any potential implications to reporting) and tax controversy are high on the list of issues that audit committees should follow closely in the coming year. Geopolitical uncertainty is shifting tax compliance risk from emerging markets to developed economies, with the US, UK and Australia making the top five tax risk jurisdictions, together with China and India.

EY’s recent tax survey finds that income taxation is undergoing a fundamental shift on a global scale, and the primary driver is the explosion of new transparency and reporting measures on the global landscape in recent years. In addition to rapid changes to tax policy and enforcement brought by base erosion and profit shifting (BEPS) and the digital revolution, a wave of political uncertainty and “unknowns” – such as the tax implications of Brexit and the question of how, and whether, the United States will enact tax reform – have prompted businesses to analyze the potential impact these events could have on their tax strategy and business operations.

Further discussion

Global focus on base erosion and profit shifting (BEPS)

While the Organisation for Economic Co-Operation and Development’s (OECD) October 2015 release of the final BEPS reports may have moved the project from the theoretical stage to the real world, for many organizations the BEPS era still remains uncertain. While there has been some clarity in certain areas – notably with the new country-by-country reporting (CbCR) obligations introduced under Action 13 of the BEPS Action Plan – many businesses still have a sense of uncertainty around how the implementation phase will unfold.

In view of the depth and breadth of the BEPS recommendations and their disparate impact on different industries, there is no one-size-fits-all approach to dealing with BEPS. However, audit committees should make certain that their organizations have protocols in place to continuously monitor tax law changes in the countries of operation and have an understanding of the expected impact of such changes on the organization’s tax provision.

In order to reduce risk and controversy, audit committees should certify that their organizations have a robust dispute management system, as well as clear and consistently applied tax and transfer pricing policies in place.

The future of tax reporting and transparency

The enhanced transparency measures and new reporting requirements have had profound implications for businesses’ tax compliance and reporting functions, audits and controversies, and reputational risk. These have increased the need for companies to develop a comprehensive and robust approach to managing tax risk and associated controversy.

Tax administrations are harnessing the power of digitization to make better use of limited resources and extract more value from the information they receive. Tax authorities are making strategic use of data analytics to make compliance and audit determinations and are increasingly sharing this data with tax authorities in other jurisdictions. This exposes businesses to more risk if their people, processes and systems are dated or out of sync with government requirements and expectations. Audit committees should confirm that tax departments are equipped to operate in the new era of digital tax by embracing enterprise initiatives and transformations that facilitate enhanced data management and compliance.
US tax reform

The US Congress is expected to focus much of its time in the coming months on tax reform. Republicans in the House of Representatives began the legislative process by releasing their long-awaited tax reform bill on November 2, and the Senate was expected to soon follow suit. Republican congressional leaders have said their goal is to enact reform by year-end, although the complexities involved and the tight legislative schedule could push the process into 2018. The US tax reform legislation under debate would include lower tax rates for corporations, pass-through businesses and individuals, a territorial international tax system, a temporary provision allowing for immediate expensing of certain capital investments, some limitation on interest deductions for corporations, and fewer targeted tax incentives. Any new legislation would likely require companies to take steps such as marking their deferred tax assets and deferred tax liabilities to the reduced corporate tax rate(s), recomputing their effective tax rates for base changes such as the potential repeal of the Section 199 deduction and reduced interest deductions, calculating the toll charge on unremitted earnings and, quite possibly, calculating a global minimum tax.

Legislation could move quickly, and there will be many moving parts to the tax policy discussions in the months ahead. Audit committees should make sure management is keeping up with developments, modeling company-specific outcomes and engaging in the process.

Audit committees should:

- Monitor tax policy changes and developments – both actual and potential – in key jurisdictions
- Make certain that management models the potential impact of tax reforms that might affect any aspect of company tax strategy
- Communicate and engage with local and global policymakers about the potential impact of tax policy changes to ensure that they understand the business implications of any legislation

Furthermore, as tax continues to be an area of frequent financial restatements, audit committees should continue to monitor the related accounting and internal control implications arising from any tax changes.

Questions to consider

6. How is the company informing itself and the audit committee on tax policy changes and opportunities?
7. Does the company have a strategy for managing tax risk and tax controversy? Has the strategy been communicated to the audit committee and full board?
8. Does the organization have a clear policy explaining the company’s approach to tax planning, and are the board and management prepared to defend it publicly?
9. Has management shifted focus from traditional compliance activities to real-time digital audit readiness activities – including considering changing technologies, processes and people to support this shift?

Additional references

- EY’s 2017 Tax Risk and Controversy Survey
- US tax reform
SEC developments

Background

2017 has been a transition year at the SEC, with Jay Clayton appointed as the new Chairman in May and the pending appointment of two additional commissioners. SEC priorities include cybersecurity and capital formation. One of the SEC’s many responsibilities is to oversee the PCAOB and appoint members to the PCAOB Board, which currently has several vacancies and members with expired terms. In August, the SEC announced it is seeking a new PCAOB chairman, and that current PCAOB Chairman James Doty, whose term expired in 2015, has agreed to stay at the PCAOB during the search process. In addition to the chair, the SEC can take action on up to three more Board seats by the end of 2017.

Further discussion

New SEC staff leadership and agenda considerations

In addition to cybersecurity, a key SEC priority is to encourage more companies to go public sooner, even as the private capital markets (and certain SEC rule changes in recent years) have evolved in ways that enable larger private companies to stay private longer. The Commission has taken some meaningful but small steps to do this, including allowing all companies to submit confidential draft registration statements. Another priority is to continue the SEC’s disclosure effectiveness project, which seeks to streamline and modernize disclosures. The SEC agenda also includes vigorous enforcement, with an undertaking to focus on individuals where appropriate, and examination programs and a review of market structure.

Two more appointments are expected to complete the Commission’s five-member composition in the coming months. Hester Peirce and Robert Jackson have been nominated as commissioners. They are expected to be confirmed before the end of the year. Audit committees and SEC registrants should keep abreast of the evolving SEC agenda and the impact that such changes have on the organization.

PCAOB developments

The Public Company Accounting Oversight Board adopted proposed rules, recently approved by the SEC, to expand the auditor’s report to include items such as auditor tenure and critical audit matters (or “CAMs”). Beginning in 2019, the auditors (rather than the audit committee or the company itself) are required to include a discussion of CAMs in their reports. The audit report must identify the CAM, describe the basis for the auditor’s determination that the matter is a CAM, describe how the CAM was addressed in the audit and identify the relevant financial statement disclosures that relate to the CAM. If no CAM is identified, the auditor must state that in its report.

The standard also requires auditors to disclose certain new information, including about auditor tenure, in auditor’s reports relating to financial reporting periods ending on or after December 15, 2017. These disclosures may raise questions from investors, particularly in cases of long auditor tenure. Accordingly, audit committees may want to consider disclosing more information about how they select and oversee the auditor.

In view of the PCAOB’s rules, companies and their audit committees should engage with their auditors about the CAM disclosure requirement and the processes that will be used or that may change in order for auditors to meet that requirement. Advance discussion about identification of and disclosures about CAMs can help to facilitate compliance with the standard and avoid surprises and potential delays in the SEC filing process.

The PCAOB continues taking steps to require greater disclosures by the external auditor. Beginning in 2017, PCAOB-registered audit firms are required to file Form AP to disclose: (1) the name of the lead engagement partner for each public company audit, and (2) the names, locations and extent of participation of other accounting firms that took part in public company audits, if
their work contributed 5% or more of the total audit hours. Audit committees should be aware of these disclosures and discuss any questions with its external auditors.

The PCAOB current standard-setting agenda also includes (1) auditing accounting estimates, including fair value measurements, (2) the auditor’s use of the work of specialists, (3) supervision of audits involving other auditors and (4) going concern.4

Treasury releases on financial regulatory reform

The Treasury department released the second in a series of reports outlining how regulations should be revisited according to the Trump Administration’s “core principles” on the financial system. This report focuses on capital markets rules overseen by the SEC, the Commodity Futures Trading Commission (CFTC), the Financial Industry Regulatory Authority (FINRA) and other regulatory bodies. If implemented, the recommendations would impact companies in a variety of areas, including by reducing redundant regulations for public companies and removing the pay ratio disclosure requirement. The report also recommends allowing more investors to access private markets. While the SEC and CFTC are independent financial regulators and so control their own rule-making agendas, the report likely will be carefully considered by agency leaders. Accordingly, boards and audit committees should continue to monitor these releases and reports.

Enhancing audit committee reporting

The 2017 proxy season saw continued growth in audit committee transparency. Continuing the trend of past years, investors, regulators, and other stakeholders are seeking enhanced disclosures from companies regarding the audit committee’s ownership and oversight of the relationship to its external auditor. This interest in transparency may be due, in part, to the fact that, even as audit committee obligations have expanded over the years, required audit committee disclosures have not; rather, audit committee disclosure obligations pre-date the Sarbanes-Oxley Act (SOX).

Companies are providing more robust disclosures and valuable perspectives on the activities of the audit committee, including its oversight of the external auditor. While transparency has increased steadily over the past three years, several recent and upcoming regulatory developments, such as the PCAOB’s revised standard on the auditor’s report and the SEC’s ongoing disclosure effectiveness project, may contribute to further consideration of audit-related disclosures in the coming years.

Questions to consider

10. Do the audit committee and management understand business, technology, industry and legal issues relating to cybersecurity, and is management prepared to meet the related operational and disclosure challenges, and effectively respond to a cyber incident?

11. What steps should the audit committee take to increase transparency around its oversight of the audit relationship, particularly in light of increased requirements for auditors to disclose certain information?

12. How has the role of the board or audit committee evolved in recent years (e.g., oversight of the enterprise risk management (ERM) process, cybersecurity risk) – and to what extent are these changes being communicated to stakeholders via the proxy statement?

13. 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?

Additional references

- To the point: SEC proposed modernizing and simplifying certain Regulation S-K disclosure requirements
- New SEC Chairman Jay Clayton outlines views in policy speech
- To the point: PCAOB adopts final standard to significantly change the auditor’s report
- Audit committee reporting to shareholders in 2017
- 2017 Proxy season review
Risk management

Background

Organizations today are challenged with managing a rapidly changing risk landscape as technology is disrupting every industry, the gig economy is becoming truly international and there is constant change in the geopolitical and economic landscape. Despite improvements in identification, assessment and reporting of risks, organizations recognize that opportunities still exist to further improve the linkage between risk management and business performance. Boards and audit committees are challenging whether management is truly engaging in conversations across the organization to identify and assess the risks that could positively or negatively impact an organization.

To succeed in today’s fast-moving business environment, organizations must take a strategic approach to risk management. Regardless of an organization’s stage of growth, the ability to effectively identify and manage risk is a vital element of success. Companies that are market leaders approach risks intelligently to help them reap benefits and accelerate growth. More than ever, boards, audit and risk committees play a vital role in bringing emerging-risk points of view to the companies they serve.

Further discussion

The evolution of Enterprise Risk Management (ERM)

In September 2017, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) released an update to its ERM framework that emphasizes the importance of considering risk in strategic planning and in driving performance. The revised framework also provides guidance on governance and oversight roles for ERM across organizations. Given the updated framework, boards and audit committees should revisit their organization’s approach to integrate ERM practices into all aspects of the business.

Boards can enhance ERM efforts by articulating and integrating risk appetite into strategic planning and determining that organizations have clear risk ownership/accountability, processes and operating models to provide a comprehensive view of risk.

Audit committees, given their expertise in financial reporting, can provide strong support to boards in overseeing risks, as well as overseeing ways to effectively enhance ERM programs. Although the full board has primary responsibility of risk oversight, audit committees often take responsibility for the monitoring of an effective risk management process, particularly in the absence of a risk committee. To further enhance risk monitoring efforts, audit committees can ensure their organizations are effectively utilizing quantitative analytics to incorporate future and predictive indicators to not only provide a clearer view of risk exposures, but also deliver forward-looking risk insights to expand considerations over emerging risks. Additionally, audit committees should revisit the internal audit mandate to assess ERM alignment for the right balance of cost, risk and value when assessing and responding to risks across three categories – strategic risks, preventable risks and external risks.

Strategic and external risks

Our most recent Global Governance, Risk and Compliance Survey suggests that organizations are primarily focused on financial, operational, regulatory and compliance risks, even though many large losses in the market are the result of mismanaged strategic risks and external risks, which include technology shifts, industry disruptions, and the risks of mergers and acquisitions. However, with increasing stakeholder demands and an ever-evolving business landscape, leading organizations are now focusing more of their time and efforts on managing the strategic and external risks with potential value creation. Audit committees play a unique role in the fact that they have an external perspective that can bring enhancement to the identification of risks, specifically external and strategy risks.
Leading audit committees will be vigilant in working with management teams to assess the seven main categories of external risks: political, cybersecurity, social, technological, legal/regulatory compliance, economic and environment. It will be important for boards to be involved in the process of validation of identified external risks that could disrupt the organization’s strategy. To do this, monitoring competitor activities and assessing the competition’s publicly reported risk factor statements can provide valuable insights to external risks and provide validation to the completeness of the identified risks.

Digital transformation
In order to fuel better performance in a digital world, leading companies are not only identifying and mitigating risk, but they are turning digital risks into competitive advantage to activate digital trust in the marketplace and for their customers. Companies increasingly need to consider the adoption of digital technologies to keep pace with competitive product advancements, as well as the ability to deliver them in different ways at lower costs. Digital transformation is not just about technology – it requires the right focus on risk management associated with it. While eliminating some risks, digital business can create new, or magnify existing, risks that present significant threats if not managed appropriately.

In this age of technology disruption, audit committees should focus on:

- Understanding the organization’s strategy and portfolio of emerging technology – balancing the portfolio for the greatest overall investment, risk and reward
- Improving enterprise risk governance and resilience
- Inquiring as to how the organization will embed security and controls in emerging technology efforts
- Understanding the risks associated with emerging technologies and how the organization will manage those risks
- Assessing the agility of the risk function to ensure that the right skill sets, processes and tools are in place to respond to new risks quickly and effectively
- Seeing whether the risk function is utilizing emerging technologies to optimize risk management and reporting

Evolving cybersecurity regulations
New regulatory and reporting developments at the federal, state and even global levels have made cybersecurity risk oversight even more challenging. Additionally, there is a growing focus on privacy. The European Union (EU) 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. Failure to comply with the GDPR, once it takes effect next year, can result in fines of up to 4% of global revenue. This regulation, along with existing rules in other jurisdictions, is creating challenges in managing complex, and potentially inconsistent, regulations around privacy and cyber. Boards are finding cyber risk needs to be governed in a different way, spanning not just the audit committee but the risk, technology and even the nominating and governance committee from a board skills’ perspective.

The American Institute of Certified Public Accountants (AICPA) issued Description Criteria for Management’s Description of an Entity’s Cybersecurity Risk Management Program and updated its Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy that, together, can be used by entities to describe their cybersecurity risk management programs and evaluate controls in these programs. 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
Questions to consider

14. Is the company’s risk management framework aligned with the organization’s strategy to better enable performance and inform decision-making?

15. Do the organization’s risk management practices incorporate forward-looking insights and use of data analytics to determine trends and predictive indicators?

16. Has management clearly articulated the aggregate risk to achieving its strategic goals and properly applied the organization’s risk tolerance to determine risk management priorities?

17. Are the company’s ERM processes integrated with existing business processes to drive value and better inform decision-making?

18. How is the organization’s cybersecurity risk management approach aligned with or embedded in its overall enterprise risk management process?

19. Is the organization’s approach to cybersecurity risks and associated privacy issues aligned with the requirements of the 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?

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

21. How is the organization monitoring for new and potential cybersecurity regulatory changes and complying with new legal requirements?

Additional references

- EY’s Governance, Risk, and Compliance Survey
- Enhancing the identification and response planning for external risks facing today’s organization
- Can digital uncertainty be transformed into trust?
- The evolving role of the board in cybersecurity oversight
- Governing cyber risk in financial services and other resources for the financial services industry

...
Audit committee effectiveness

As audit committees grapple with challenges and an evolving business landscape, many audit committees are seeking guidance to enhance their operating effectiveness to better serve as a strategic asset for the organization.

SEC Chief Accountant Wesley Bricker provided guidance for audit committees in a recent speech on how they can effectively discharge their oversight responsibilities. “Audit committees … play a critical role in contributing to financial statement credibility through their oversight and resulting impact on the integrity of a company’s culture and internal control over financial reporting (ICFR), the quality of financial reporting, and the quality of audits performed on behalf of investors,” he said. Mr. Bricker highlighted seven areas in which audit committees can improve in their oversight of a company’s financial reporting, echoing comments he and other SEC officials have made in recent years. The seven areas include:

- Understanding the business and operating environment, in particular the economic, technological and societal changes on corporate strategies
- Promoting diversity of thought and skill sets to enhance a board’s ability to monitor the quality of financial reporting and hold management accountable for poor performance
- Balancing the audit committee workload to ensure there are no additional risks arising from audit committee overload and allowing members to keep current on financial reporting developments
- Setting a positive tone at the top and internal control culture
- Understanding disclosure controls and procedures over non-GAAP financial measures and key operating metrics
- Monitoring corporate objectives, such as cost reductions, that could conflict with effective financial reporting and auditing
- Considering enhanced voluntary reporting

Audit committees should endeavor to review their performance throughout the year (including the performance of each committee member) to not only ensure that they meet the responsibilities set forth in their charters, but also to seek opportunities to enhance overall effectiveness.
21 questions for audit committees to consider

Financial reporting

1. What changes to ICFR have been designed and what key actions have been taken by management to implement the new revenue recognition, lease, credit loss and other FASB standards in process? What key actions are needed to improve readiness for implementation and disclosure?

2. What is the company’s plan for periodically updating the disclosures under SAB 74 on the effect of new accounting standards?

3. Did the entity consider the impacts of changes in revenue recognition patterns on cost and margin recognition, as well as other effects of the new standard, such as financial covenants, incentive plans, etc.? What disclosures has management provided or considered on these changes?

4. Has the organization considered the guidance in CF Disclosure Guidance: Topic No. 2, Cybersecurity, and reassessed its risk management governance and related disclosures around cybersecurity risks to address any developments in operations and the evolving nature of cyber threats?

5. What new disclosure controls has management implemented to address compliance with new SEC staff guidance?

SEC developments

10. Do the audit committee and management understand business, technology, industry and legal issues relating to cybersecurity, and is management prepared to meet the related operational and disclosure challenges and effectively respond to a cyber incident?

11. What steps should the audit committee take to increase transparency around its oversight of the audit relationship, particularly in light of increased requirements for auditors to disclose certain information?

12. How has the role of the board or 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?

13. 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?

Risk management

14. Is the company’s risk management framework aligned with the organization’s strategy to better enable performance and inform decision-making?

15. Do the organization’s risk management practices incorporate forward-looking insights and use of data analytics to determine trends and predictive indicators?

16. Has management clearly articulated the aggregate risk to achieving its strategic goals and properly applied the organization’s risk tolerance to determine risk management priorities?

17. Are the company’s ERM processes integrated with existing business processes to drive value and better inform decision-making?

18. How is the organization’s cybersecurity risk management approach aligned with or embedded in its overall enterprise risk management process?

19. Is the organization’s approach to cybersecurity risks and associated privacy issues aligned with the requirements of the 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?

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

21. How is the organization monitoring for new and potential cybersecurity regulatory changes and complying with new legal requirements?
**Endnotes**


---

**EY Center for Board Matters (CBM) contacts**

**Americas CBM Leader**
Stephen Klemash  
+1 412 644 7461  
stephen.klemash@ey.com

**Americas Regional CBM Leaders**

<table>
<thead>
<tr>
<th>Region</th>
<th>Contact</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canada</td>
<td>Fred Clifford</td>
<td>+1 416 943 2489</td>
<td><a href="mailto:fred.clifford@ca.ey.com">fred.clifford@ca.ey.com</a></td>
</tr>
<tr>
<td>Central</td>
<td>Julia Poston</td>
<td>+1 513 612 1557</td>
<td><a href="mailto:julia.poston@ey.com">julia.poston@ey.com</a></td>
</tr>
<tr>
<td>FSO</td>
<td>Paul Haus</td>
<td>+1 212 773 2677</td>
<td><a href="mailto:paul.haus@ey.com">paul.haus@ey.com</a></td>
</tr>
<tr>
<td>Israel</td>
<td>Ariel Horowitz</td>
<td>+972 3 6270939</td>
<td><a href="mailto:ariel.horowitz@il.ey.com">ariel.horowitz@il.ey.com</a></td>
</tr>
<tr>
<td>Northeast</td>
<td>Chris Bruner</td>
<td>+1 215 448 2289</td>
<td><a href="mailto:chris.bruner@ey.com">chris.bruner@ey.com</a></td>
</tr>
<tr>
<td>Latin America North</td>
<td>Lupita Castaneda</td>
<td>+52 555 283 8691</td>
<td><a href="mailto:guadalupe.castaneda@mx.ey.com">guadalupe.castaneda@mx.ey.com</a></td>
</tr>
<tr>
<td>Latin America South</td>
<td>Andre Ferreira</td>
<td>+55 11 2573 5250</td>
<td><a href="mailto:andre.ferreira@br.ey.com">andre.ferreira@br.ey.com</a></td>
</tr>
<tr>
<td>Southeast</td>
<td>Randall Duncan</td>
<td>+1 404 817 5281</td>
<td><a href="mailto:randall.duncan@ey.com">randall.duncan@ey.com</a></td>
</tr>
<tr>
<td>Southwest</td>
<td>Steve Macicek</td>
<td>+1 713 750 1253</td>
<td><a href="mailto:steven.macicek@ey.com">steven.macicek@ey.com</a></td>
</tr>
<tr>
<td>West</td>
<td>Lee Dutra</td>
<td>+1 415 894 8220</td>
<td><a href="mailto:lee.dutra@ey.com">lee.dutra@ey.com</a></td>
</tr>
</tbody>
</table>

---

**Looking for more?**

Access additional information and thought leadership from the EY Center for Board Matters at ey.com/boardmatters.
About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

About the EY Center for Board Matters

Effective corporate governance is an important element in building a better working world. The EY Center for Board Matters supports boards, committees and directors in their oversight role by providing content, insights and education to help them address complex boardroom issues. Using our professional competencies, relationships and proprietary corporate governance database, we are able to identify trends and emerging governance issues. This allows us to deliver timely and balanced insights, data-rich content, and practical tools and analysis for directors, institutional investors and other governance stakeholders.

© 2017 Ernst & Young LLP.
All Rights Reserved.
SCORE no. 06420-171US
CSG no. 1710-2470253
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com