

## The role of the audit committee

April 2018



# The role of the audit committee

**Oversight of financial reporting and related internal controls**

**Review of filings and earnings releases**

**Risk oversight**

**Oversight of the independent auditor**

**Ethics and compliance**

**Oversight of internal audit**

**Other interactions with management and the board**

**Audit committee external communications**

# The role of the audit committee

As an audit committee member, it is important to understand the rules relevant to your role. This section provides an overview of an audit committee's responsibilities in overseeing financial reporting and related internal controls, risk, and ethics and compliance. It also discusses the committee's role in overseeing the internal and independent auditors, as well as how the committee may interact with other members of management and external stakeholders. Finally, it highlights the committee's responsibilities with respect to disclosures in the proxy statement.

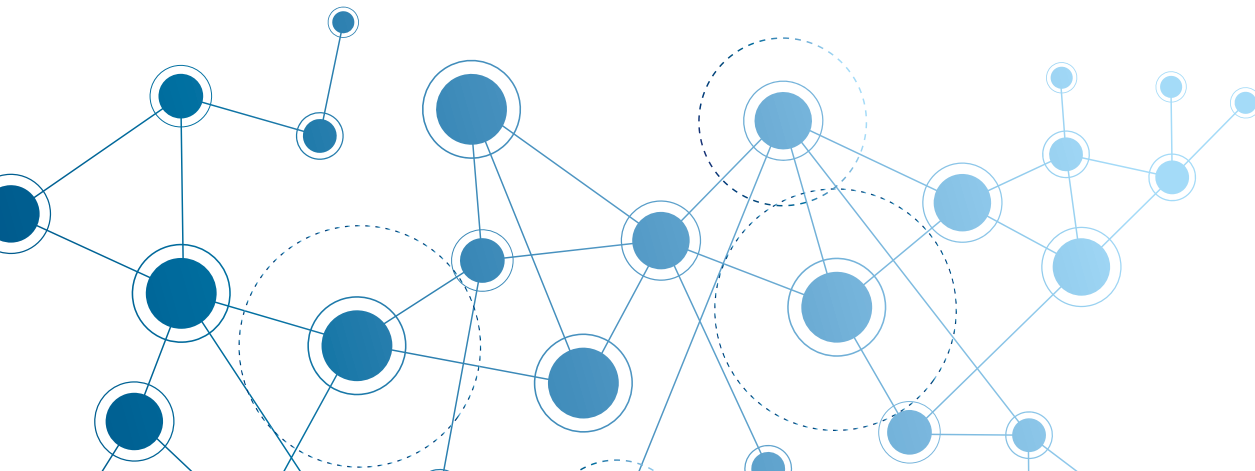
SEC, PCAOB, NYSE, and NASDAQ rules are highlighted where relevant, and we have noted leading practices, tools, and resources to help audit committee members execute their responsibilities.

## Oversight of financial reporting and related internal controls

The audit committee, management, and the independent auditor all have distinct roles in financial reporting. Management is responsible for preparing the financial statements, establishing and maintaining adequate internal control over financial reporting (ICFR), and evaluating the effectiveness of ICFR. The independent auditor is responsible for expressing an opinion on the fairness with which the financial statements present, in all material respects, the financial position, the results of operations, and cash flows in conformity with GAAP, and, when applicable, evaluating the effectiveness of ICFR.

To oversee ICFR successfully, the audit committee should be familiar with the processes and controls management has put in place and understand whether those processes and controls are designed and operating effectively. The audit committee should work with management, the internal auditors, and the independent auditor to gain the knowledge needed to provide appropriate oversight of this area.

Likewise, the audit committee is responsible for overseeing the entire financial reporting process. To do so effectively, it should be familiar with the processes and controls that management has established and determine whether they were designed effectively.



The audit committee's role is one of oversight and monitoring, and in carrying out this responsibility, the committee may rely on management, the independent auditor, and any advisers the committee might engage, provided its reliance is reasonable.

The audit committee should consider having management identify and discuss any significant accounting policies, estimates, and judgments made. A quarterly analysis of these areas may be useful to prepare for these discussions, and management should tailor the analysis to highlight changes and include new or unusual items. Because [Regulation S-X, Rule 2-07](#) requires the independent auditor to discuss the effects of alternative GAAP methods on the financial statements, the information presented by management should be corroborated by the independent auditor.

**NYSE requirements.** NYSE listing standards require the audit committee to review major issues regarding accounting principles and the presentation of the financial statements. These include significant changes in the company's selection or application of accounting principles, the adequacy of internal controls, and any special audit steps adopted in response to what the NYSE terms "material control deficiencies." These discussions can be held, generally with management, during the review of the quarterly financial statements to be filed with the SEC.

The audit committee is also required to review management's analyses of significant issues in financial reporting and judgments made in preparing the financial statements, including the effects of alternative GAAP methods. This discussion may also be held during the review of the quarterly financial statements. The audit committee also should review the effects of regulatory and accounting initiatives, as well as off-

balance-sheet transactions, on the financial statements. For example:

- Management and the audit committee should discuss pending technical and regulatory matters that could affect the financial statements, and the audit committee should be updated on management's plans to implement new technical or regulatory guidelines.
- The review of off-balance-sheet structures should also be a recurring agenda item, and may be conducted as part of the committee's review of management's discussion and analysis in the annual and quarterly reports. The exact frequency of these discussions will depend on the company's operations and preferences. Finally, the audit committee should consider reviewing off-balance-sheet transactions, or at least material ones, before they are executed.

**NASDAQ requirements.** NASDAQ requires disclosure of the audit committee's purpose, as set out in its charter, of overseeing accounting and financial reporting processes of the company and audits of the financial statements. See the **audit committee charter** section of this guide for details.

#### Fraud risk

In conjunction with risk oversight, the audit committee should be satisfied that the company has programs and policies in place to prevent and identify fraud. It should work with management to oversee the establishment of appropriate antifraud controls and programs and to take the necessary steps when fraud is detected. The audit committee should also be satisfied that the organization has implemented an appropriate ethics and compliance program and established a reporting hotline. See the **ethics and code of conduct** and **reporting hotline procedures** sections later in this guide for more information.

Audit committee members should be aware of three main areas of fraud risk:

- Financial statement fraud, which includes intentional misstatements in or omissions from financial statements
- Asset misappropriation, which may include check forgery, theft of money, inventory theft, payroll fraud, or theft of services
- Corruption, which may include schemes such as kickbacks, shell companies, bribes to influence decision makers, or manipulation of contracts.

One way the audit committee can help oversee the prevention and detection of financial statement fraud is by monitoring management's assessment of ICFR.

The audit committee should also have an awareness of the US Foreign Corrupt Practices Act (FCPA) and other non-US anticorruption laws that may be applicable (e.g., the UK Bribery Act). As the SEC and Department of Justice note in the [Resource Guide to the FCPA](#), anticorruption compliance "begins with the board of directors and senior executives setting the proper tone for the rest of the company." To that end, the audit committee should:

- Understand the company's obligations and responsibilities regarding anticorruption laws to which it is subject
- Determine whether the company has dedicated appropriate oversight, autonomy, and resources to its anticorruption compliance program; depending on the company's size, this could involve assigning an individual who is specifically charged with anticorruption compliance and has a direct reporting line to the committee

- Understand specific policies and procedures in place to identify and mitigate corruption-related risks
- Discuss with management specific corruption-related risks that have been identified, including allegations of corruption that may have been received through the company's monitoring and reporting mechanisms, as well as management's plans for responding to such risks
- Monitor any actual violations, including management's response.

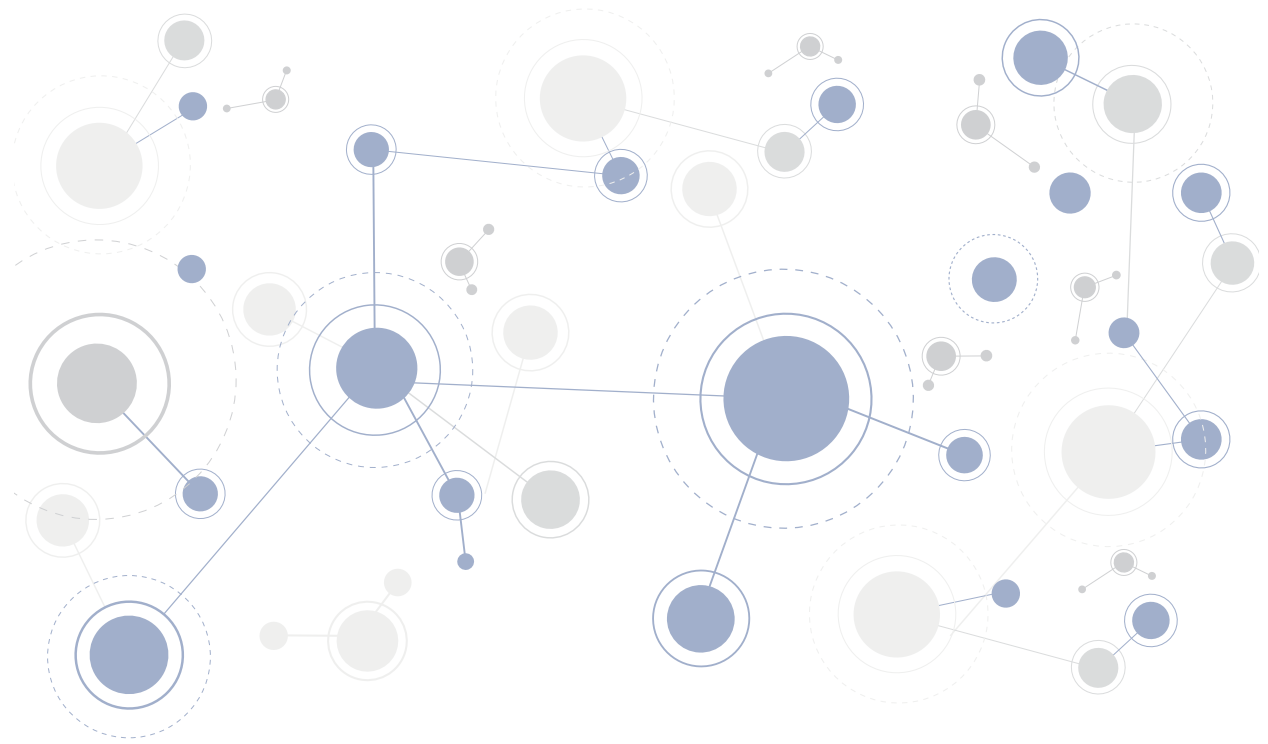
## Tools and resources



The [Anti-Fraud Collaboration](#) released a report titled [The Fraud-Resistant Organization](#) that identifies three central themes critical to fraud deterrence and detection.

**2013 COSO framework.** The 2013 Internal Control—Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) provides a formal structure for designing and evaluating the effectiveness of internal control. It emphasizes the role of the board—and, by delegation or regulation, the role of the audit committee—in overseeing internal control, which remains an essential aspect of effective governance. In particular, the framework highlights:

- The board's role in the control environment, including clarification of expectations for integrity and ethics, conflicts of interest, adherence to codes of conduct, and other matters
- The board's assessment of the risk that management could override internal controls and careful consideration of the possibility that management may override such controls
- The establishment and maintenance of open lines of communication between management and the board and the provision of separate lines of communication, such as whistleblower hotlines.



## Review of filings and earnings releases

The audit committee generally reviews earnings releases, SEC filings containing financial information, and other financial information and earnings guidance provided to analysts, ratings agencies, and others. The committee should consider how it will execute these responsibilities to satisfy itself that all information is presented fairly and in a transparent manner. This should include a focus on consistency of information, tone, and messaging across all financial communications.

The audit committee should confirm that an appropriate legal review has been completed to verify the completeness of disclosures, including any obligation to report on trends. This legal review should also consider compliance with the company's policies on forward-looking statements and the completeness of any related disclaimers.

**NYSE requirements.** NYSE listing standards require that the audit committee meet to discuss the company's annual audited financial statements and quarterly financial statements with management and the independent auditor. They also require the audit committee charter to address the committee's responsibility to discuss earnings press releases and the financial information and guidance provided to analysts and ratings agencies.

The commentary to the listing standards indicates that this discussion may be in general terms, and the audit committee may discuss the type of information disclosed and the type of presentation made. The commentary also indicates that the discussion should pay particular attention to any pro forma or adjusted non-GAAP financial information.

Note that SEC rules require the audit committee to recommend to the board that the audited financial statements be included in the company's annual report on Form 10-K.



**Two-thirds** of audit committees meet via conference call to discuss earnings releases, while **22%** review earnings releases at in-person meetings

Source: Deloitte 2016 Board Practices Report

## Questions for audit committees to consider



### Earnings guidance

The audit committee should discuss earnings guidance with management. Questions to consider include:

- When did management last evaluate its approach to providing earnings guidance? Is a change in approach warranted as a result of the current economic environment and other circumstances facing the company?
- How can pressures to meet expectations in the short term influence the quality of the company's reported financial results and management behavior?
- What practices do the company's competitors follow with respect to earnings guidance and other forward-looking information?
- What are management's reasons for providing or not providing earnings-per-share targets and other types of forward-looking information?
- How confident is management in its ability to forecast earnings accurately? Is the disclosure of a range of earnings estimates preferable to a specific target? Should the time frame for which estimates are provided be modified or are more frequent updates necessary?
- What are the company's long-term value drivers? What is the specific quantitative and qualitative information—be it financial or nonfinancial in nature—that best reflects these drivers? Is this information provided to investors and analysts on a forward-looking basis?
- Has management considered seeking input directly from shareholders regarding the types of forward-looking information they would find meaningful?
- Do current circumstances warrant enhanced audit committee review of earnings estimates and other forward-looking information before it is made public?
- If the company changes its approach to the provision of earnings guidance and forward-looking information, should the audit committee modify its practices for reviewing that information?

## Questions for audit committees to consider



### Non-GAAP measures

The SEC rules regarding the use of non-GAAP financial measures require, among other things, that disclosure of any material information containing non-GAAP financial measures must include the most directly comparable GAAP financial measures, that the GAAP measures must be disclosed with equal or greater prominence, and that the GAAP and non-GAAP measures must be reconciled. The SEC has recently taken a hard look at non-GAAP measures in response to concerns about their increased use and prominence. As a result, companies and audit committees should consider re-examining their use of non-GAAP measures and related controls and the disclosure of those measures. The audit committee should consider asking the following questions:

- Is the measure misleading or prohibited?
- Is the measure presented with the most directly comparable GAAP measure and with no greater prominence than the GAAP measure?
- Is the measure defined and described appropriately and clearly labeled as non-GAAP?
- Does the reconciliation between the GAAP and non-GAAP measure clearly label and describe the nature of each adjustment, and is each adjustment appropriate?
- Is there transparent and company-specific disclosure of the substantive reasons why management believes that the measure is useful for investors and the purpose for which management uses the measure?
- Is the measure prepared consistently from period to period in accordance with a defined policy, and is it comparable to that of the company's peers?
- Is the measure balanced (e.g., does it adjust not only for nonrecurring expenses but also for nonrecurring gains)?
- Does the measure appropriately focus on material adjustments and not include immaterial adjustments that would not seem to be a focus of management?
- Do the disclosure controls and procedures address non-GAAP measures?
- Does the audit committee oversee the preparation and use of non-GAAP measures?
- Does the audit committee have a clear understanding how non-GAAP measures impact compensation? Are the audit and compensation committees aligned on this?

## Tools and resources



Deloitte's publications [A Chance to Self-Correct: SEC Urges Companies to Take a Fresh Look at Their Non-GAAP Measures](#) and [A Roadmap to Non-GAAP Financial Measures](#) provide additional information, including ways for a company to assess the appropriateness of its non-GAAP measures and control considerations.

Additionally, in March 2018, the Center for Audit Quality issued [Non-GAAP Measures: A Roadmap for Audit Committees](#), a guide intended to help audit committees enhance their oversight of these measures used by company management. The roadmap provides key considerations for audit committees, including leading practices to assess whether a company's non-GAAP metrics present a balanced representation of the company's performance.

## Questions for audit committees to consider



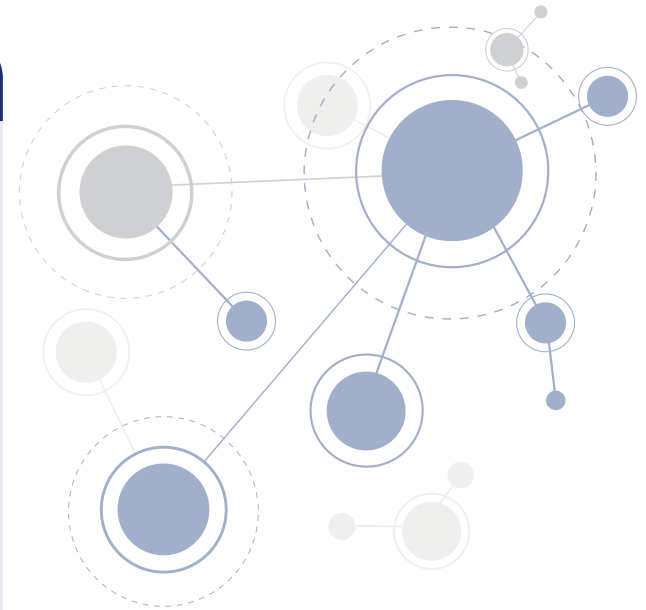
### Related-party transactions

NASDAQ and NYSE listing standards each contemplate that the audit committee of a listed company, or another independent body of the board, will review all related-party transactions. In some instances, this responsibility is assigned to the audit committee. The following questions may help the audit committee assess its process for approving related-party transactions:

- What process will the committee follow in reviewing and approving related-party transactions? Is this process documented?
- Will special meetings be called as potential transactions arise, or is there a process to review transactions between scheduled meetings?
- What information does the committee need to make an informed judgment about the appropriateness of a transaction?
- Who will be responsible for presenting this information?

For each transaction brought for approval, the committee may consider asking:

- What are the business reasons for the transaction? Are these reasons in line with the company's overall strategy and objectives?
- When and how will the transaction have to be disclosed? How will investors view the transaction when it is disclosed?
- Which insiders could benefit from the transaction and in what way?
- What impact will the transaction have on the financial statements?
- Are any outside advisers needed to help understand the implications of the transaction?





## Risk oversight

Given the dynamic business environment, which creates an ever-changing risk landscape, boards should make sure the risk oversight function is well defined and effective. The board plays a critical role in understanding and influencing management's processes for identifying, assessing, and continually monitoring risks. The board should clearly define which risks the full board should discuss regularly versus the risks that can appropriately be delegated primarily to a board committee. While many boards have a defined risk governance structure in place, it is important to continually assess the structure as companies face new risks.

A leading practice is for management to maintain a list of all enterprise-wide risks, which are then mapped to specific board committees with the expertise to oversee them. For example, human resource and compensation risks may be delegated to the compensation committee for oversight, and the audit committee should have a key role in overseeing financial risks. In many instances, the full board takes direct responsibility for and regularly discusses the company's most strategic risks, which include risks that could disrupt and materially impact the company's business strategy. Committee charters should be updated to align with the defined risk governance structure.

For companies outside the financial services industry, where many companies have separate board risk committees, any risks not assigned to a specific committee during this process are often delegated to the audit committee. While it may be appropriate for the audit committee to take responsibility for reviewing the guidelines, processes, and policies management has in place to identify, assess, and manage risk, boards should take care not to overburden the audit committee

## Questions for audit committees to consider



### Risk oversight

When the board or audit committee is considering the effectiveness of the company's enterprise risk management—the process of planning, organizing, leading, and controlling activities to minimize the effect of downside risk on the organization—it may consider the following questions:

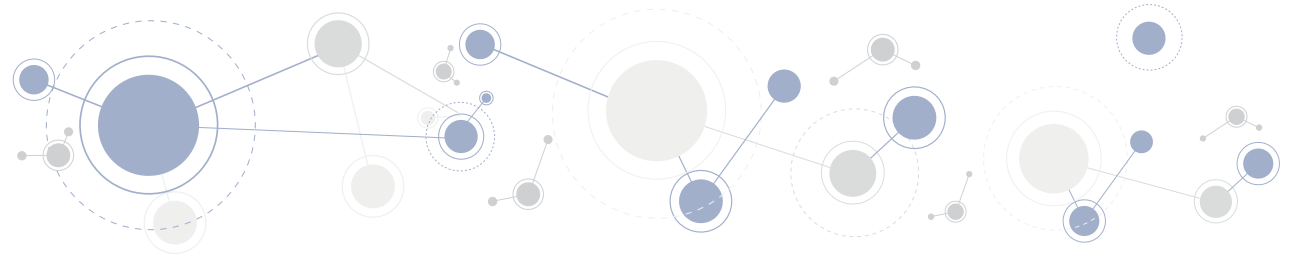
- Which board committees are responsible for various aspects of risk governance? Has the risk governance structure been defined?
- How do the various board committees oversee risk? Is there appropriate coordination and communication between all relevant stakeholders?
- Does the board consider the relationship between strategy and risk? What are the potential internal and external risks to the success of the strategy?
- Does management provide the board with the information needed to oversee the risk management process effectively?
- What are the company's policies and processes for identifying, assessing, and continually monitoring the major financial risk exposures on an integrated, enterprise-wide basis?
- Has management assigned owners for each risk that has been identified?
- How might the company's compensation programs encourage inappropriate focus on short-term financial performance? Are the audit committee and compensation committee aligned on such risks?
- What mechanisms does management use to monitor emerging financial risks? What are the early warning mechanisms, and how effective are they? How, and how often, are they calibrated?
- Which framework has management selected for the financial risk management program? What criteria were used to select it?
- What is the role of technology in the risk management program? How was it chosen, and when was it last evaluated?
- Is cyber risk receiving adequate time and focus on the audit committee agenda?

with risk oversight responsibilities. The NYSE listing standards further define the audit committee's role in discussing policies with respect to risk assessment and risk management:

While it is the job of the CEO and senior management to assess and manage the listed company's exposure to risk, the audit committee must discuss guidelines and policies to govern the process by which this is handled. The audit committee should discuss the listed company's major financial risk exposures and the steps management has taken to monitor and control such exposures. The audit committee is not required to be the sole body responsible for risk assessment and management, but, as stated above, the committee must discuss guidelines and policies to govern the process by which risk assessment and management is undertaken. Many companies, particularly financial companies, manage and assess their risk through mechanisms other than the audit committee. The processes these companies have in place should be reviewed in a general manner by the audit committee, but they need not be replaced by the audit committee.<sup>1</sup>

The SEC considers risk oversight a primary responsibility of the board and requires disclosure of its role in this area. Disclosures include whether the entire board is involved in risk oversight; whether certain aspects are executed by individual board committees; and whether the employees responsible for risk management report directly to the board. Such disclosures informs shareholders' understanding of the board's process for overseeing risk.

<sup>1</sup> NYSE listing standards, [303A.07 Audit Committee Additional Requirements](#).



## Tools and resources



Deloitte's publications, [Risk Committee Resource Guide for Boards](#); [Risk Intelligent Governance: Lessons from State of the Art Board Practices](#); and [Bank Board Risk Governance: Driving Performance through Enhanced Risk Oversight](#), provide additional information for boards and audit committee members on risk oversight.

### The audit committee's potential role in overseeing cyber risk

It is often challenging for even the most tech-savvy business leaders to keep up with the scope and pace of developments related to big data, social media, cloud computing, IT implementations, cyber risk, and other technology matters. These developments carry a complex set of risks, the most serious of which can compromise sensitive information and significantly disrupt business processes. Cyber risk is often at the top of the agenda for management and boards at companies of all sizes and industries. The pervasiveness of cyber risk significantly increases concerns about financial information; internal controls; and a wide variety of risks, including the reputational risks that can result from a cyber incident. Oversight of a successful cyber risk management program requires proactive engagement and is most frequently the responsibility of the full board. In some organizations, a level of oversight may be delegated to a risk committee or the audit committee.

In companies where the audit committee holds some responsibility for cyber risk management, the committee should first obtain a clear understanding of the specific areas it is expected to oversee. In those organizations, the audit committee, in its capacity of overseeing financial risks and monitoring management's policies and procedures, may have expertise and be asked to play a significant strategic role in monitoring management's preparation for and response to cyber threats, coordinating cyber risk management initiatives and policies, and confirming their efficacy. Those audit committees may take the lead in monitoring cyber threat trends, regulatory developments, and major threats to the company. Other responsibilities may include setting expectations and accountability for management, as well

as assessing the adequacy of resources, funding, and focus on cyber risk management activities.

For those audit committees charged with this oversight, engaging in regular dialogue with the chief information officer, chief information security officer, and other technology-focused leaders can help the committee determine where attention should be focused. Although cyber risk is frequently on the full board's agenda, audit committees are increasingly receiving regular updates from relevant technology leaders, with some technology risk-related topic on almost every meeting agenda. The audit committee chairman can be a particularly effective liaison with other groups in enforcing and communicating expectations regarding cyber and financial risk mitigation.

*We need to arm corporate boards with a mechanism to thoughtfully assess management's assertions about the design and effectiveness of their organizations' cyber defenses.*

**Sarah Bloom Raskin, Former Deputy Secretary of the US Department of Treasury, at the PCAOB's 10th annual International Institute on Audit Regulation event in Washington, DC**

#### To which groups has the board allocated the majority of tasks connected to the following areas of risk oversight? (Respondents could select multiple groups for each risk.)

	The "big" picture	Reputational risks	Financial stability risk	Cyber risks	Compliance risks	Talent risks	Incentive risks
The full board	96%	86%	47%	41%	22%	46%	21%
Audit committee	5%	9%	51%	51%	69%	2%	5%

Source: 2016-2017 NACD Public Company Governance Survey, National Association of Corporate Directors

## Cybersecurity risk management



In April 2017, the AICPA released its cybersecurity risk management attestation reporting framework, which is intended to expand cyber risk reporting to address the marketplace need for greater stakeholder transparency. This reporting framework establishes a standardized reporting mechanism to provide a broad range of users with useful information about an entity's cybersecurity risk management program to support informed and strategic decision making. It consists of the following components:

- Management's description of the entity's cybersecurity risk management program
- Management's assertion on the presentation of the description and the operating effectiveness of the controls to achieve the cybersecurity objectives
- Practitioner's report on the presentation of the description and the operating effectiveness of the controls to achieve the cybersecurity objectives.

Leveraging a unified approach for performing and reporting on an entity's cyber risk management program and related controls could help boards and audit committees effectively execute their oversight responsibilities with respect to cyber risk.

See Deloitte's [Cybersecurity risk management assessment](#) page.

## Enhanced cybersecurity disclosure guidance



The SEC issued interpretive guidance on February 21, 2018, that largely refreshes the SEC's 2011 staff guidance related to cybersecurity disclosure obligations. The [latest guidance](#) does not establish any new disclosure obligations but rather presents the SEC's views on how its existing rules should be interpreted in connection with cybersecurity threats and incidents. It also expands on the initial concepts discussed, concentrating more heavily on cybersecurity policies and controls, most notably those related to cybersecurity escalation procedures and the application of insider trading prohibitions. The guidance also addresses the importance of avoiding selective disclosure, as well as considering the role of the board of directors in risk oversight. The release applies to public operating companies, including foreign private issuers, but does not address the specific implications of cybersecurity for other regulated entities under the federal securities laws, such as registered investment companies, investment advisers, brokers, dealers, exchanges, and self-regulatory organizations.

The new guidance clarifies the SEC's view on the role of the board of directors in overseeing cybersecurity risk. If the risk is material to a company's business, the discussion of the board of directors' role in the risk oversight function should include the nature of its responsibilities for overseeing the management of this risk. The SEC believes that "disclosures regarding a company's cybersecurity risk management program and how the board of directors engages with management on cybersecurity issues allow investors to assess how a board of directors is discharging its risk oversight responsibility in this increasingly important area."

For more information about the latest guidance, refer to Deloitte's *Heads Up: [In the Spirit of Full Cybersecurity Disclosure](#)*.



## The audit committee's role in M&A

The audit committee has an important role in M&A, both before and after a transaction.

### **Before the deal is done: Due diligence**

Although due diligence is largely management's responsibility, the audit committee can provide critical oversight in areas such as risk analysis, internal controls, and even the basic financial information on which the terms are based. Weakness in a target's internal control systems can create unpleasant surprises that, in the absence of due diligence, may not be discovered until it is too late. This could be a critical factor when management is required to evaluate the post-integration controls in accordance with the Sarbanes-Oxley Act. While target financial information may be prepared with the best of intentions, and may even be audited, audit committee oversight can provide greater comfort that the financial information is accurate and complete. Other areas of due diligence oversight include tax, insurance, and Foreign Corrupt Practices Act compliance.

Audit committees can and should satisfy themselves that the due diligence process is thorough and that the board is fully informed of related risks before the transaction is approved. They can do this in much the same way they address day-to-day matters: ask questions, identify areas of risk to consider, and provide guidance on how to solve problems.

### **Post-merger integration oversight**

While post-merger integration is sometimes overlooked in the excitement of closing a deal, it can be critical to the success or failure of the transaction. The audit committee has a vital role to play here, too.

One area of audit committee focus is the melding of internal control systems and processes so they are stable on Day 1 or as soon as possible thereafter. SEC rules adopted under the Sarbanes-Oxley Act require public companies to integrate disclosure controls as well as controls over financial reporting. Failure to do so can have significant consequences. Even when both parties have high-quality systems, processes that do not work well together may create control problems, leading to reportable deficiencies or even material weaknesses.

Other areas of audit committee responsibility include oversight of talent integration in the financial and accounting areas and monitoring that computer systems and technology platforms can communicate with each other from the outset.

For additional information, read Deloitte's [On the Board's Agenda: Post-Merger Integration](#).



## Special requirements for financial institutions

Following the enactment of the Dodd-Frank Act in July 2010, the Federal Reserve Board issued a new regulation setting forth enhanced prudential standards for large banking organizations, including risk committee requirements. Specifically, all bank holding companies (BHCs) with total consolidated assets of \$10 billion or more are required to maintain a risk committee that approves and periodically reviews the risk management policies of the BHC's global operations and oversees the operation of the BHC's global risk management framework. More stringent requirements apply to BHCs with total consolidated assets of \$50 billion or more. The corporate governance requirements state that the risk committee must:

- Have a formal, written charter that is approved by the BHC's board of directors
- Meet at least quarterly, or more frequently if needed, and fully document and maintain records of its proceedings, including risk management decisions.

Moreover, the risk committee at each BHC with total consolidated assets of \$50 billion or more is required to:

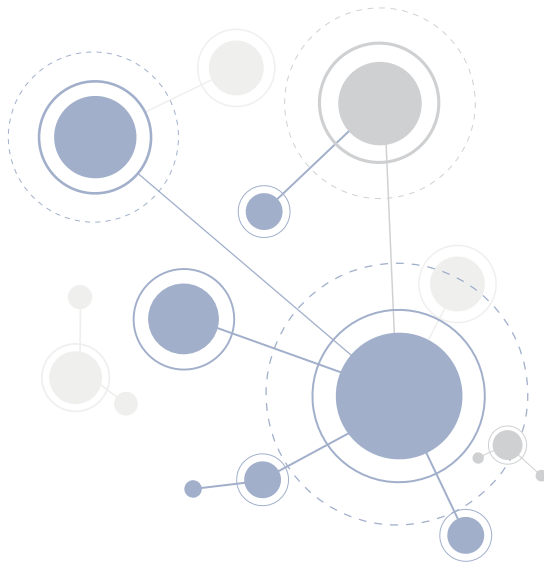
- Be an independent committee of the board of directors that has, as its sole and exclusive function, responsibility for the risk management policies of the BHC's global operations and oversight of the operation of the BHC's global risk management framework
- Report directly to the BHC's board of directors
- Receive and review regular reports not less than quarterly from the BHC's chief risk officer.

See the [Federal Reserve's final rule](#) and [Deloitte's practical guide](#) to the rule for additional requirements and guidance.

Soon after the Federal Reserve Board finalized its EPS framework, the Office of the Comptroller of the Currency (OCC) issued heightened standards applicable to national banks, insured federal savings associations, insured federal branches of foreign banks with total consolidated assets of \$50 billion or more, and OCC-regulated institutions with total consolidated assets of less than \$50 billion if that institution's parent company controls at least one other covered institution.

Among other things, each covered institution is required to establish and adhere to a formal, written risk governance framework that is designed by independent risk management and approved by the board of directors or the board's risk committee.

See the OCC's [heightened standards](#) for additional requirements and guidance.



## Oversight of the independent auditor

Audit committees of listed companies are directly responsible for the appointment, compensation, and oversight of the independent auditor, including the resolution of any disagreements with management. It is optimal for the audit committee, management, the internal auditors, and the independent auditor to work together in a spirit of mutual respect and cooperation.

The audit committee and the independent auditor typically meet at least quarterly to thoroughly discuss a wide variety of matters, including the company's financial reporting, internal controls, and the audit, from planning to conclusion of the audit. These discussions should also include educational and evaluative topics. Executive sessions with the independent auditor are a way to maintain open communication and identify concerns, and they are required for NYSE-listed companies.

### Auditor communications

The NYSE, NASDAQ, and PCAOB outline communications that are required between the audit committee and the independent auditor. Many of these communications are focused on the responsibility of the audit committee to oversee the independent auditor.

**NYSE requirements.** NYSE listing standards require the audit committee to communicate with the independent auditor in the following ways:

- Meet with the independent auditor to review and discuss the company's annual audited financial statements and quarterly financial statements, including disclosures in management's discussion and analysis

- Periodically, meet separately with the independent auditor, management, and the internal auditors
- Obtain a formal written communication from the independent auditor regarding independence and other matters annually
- Review with the independent auditor any audit problems or difficulties and management's response
- Set clear hiring policies for employees or former employees of the company's independent auditor.

**NASDAQ requirements.** NASDAQ listing standards require the audit committees of listed companies to obtain a formal written statement from the independent auditor consistent with PCAOB Ethics and Independence. [Rule 3526, Communication with Audit Committees Concerning Independence.](#)

**PCAOB requirements.**<sup>1</sup> Some communications between the auditor and the audit committee are driven by standards the auditor must follow in conducting the audit. There are a number of PCAOB standards that require communications with the audit committee. The primary one is [Auditing Standard No. 1301 \(AS 1301\), Communications with Audit Committees.](#) The communications under this standard can be oral or written, but must be made in a timely manner and prior to issuance of the auditor's report. The standard addresses communications relevant to different phases of the audit, from the auditor's engagement through the issuance of the auditor's report. It also requires communications relevant to various aspects of the company's accounting and reporting, as well any disagreements between the auditor and management.

<sup>1</sup> The PCAOB requirements encompass the items the independent auditor is required to communicate to the audit committee by [SEC's Regulation S-X, Rule 2-07, Communication with Audit Committees.](#) The SEC stated in its release adopting this rule that it expects these discussions to occur prior to filing Form 10-Q or Form 10-K.

## Summary of PCAOB required communications

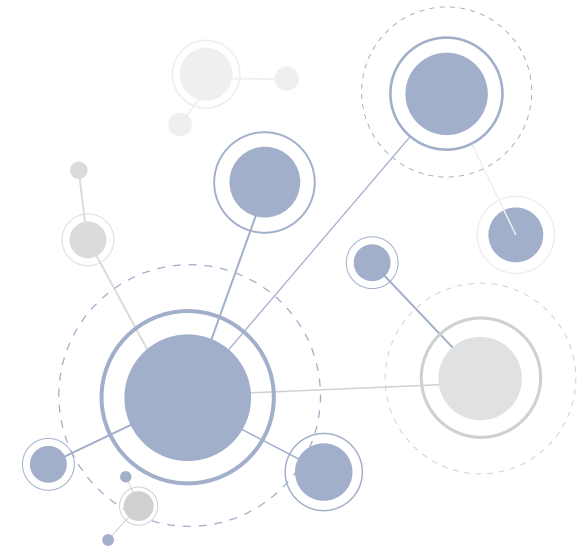


### Communications required by AS 1301

- Significant issues discussed with management before the auditor's appointment or retention
  - An understanding of the terms of the audit
  - Information relevant to the audit
  - Overview of the audit strategy, timing of the audit, and significant risks
  - Results of the audit, including:
    - Significant accounting policies and practices
    - Critical accounting policies and practices
    - Critical accounting estimates
    - Significant unusual transactions
  - Auditor's evaluation of the quality of the company's financial reporting
  - Other information in documents containing audited financial statements
- Difficult or contentious matters about which the auditor consulted
  - Management consultations with other accountants
  - Going-concern matters
  - Uncorrected and corrected misstatements
  - Material written communications
  - Departure from the auditor's standard report
  - Disagreements with management
  - Difficulties encountered in performing the audit
  - Other matters

### Communications required by other PCAOB standards or rules

- Material weaknesses and significant deficiencies in internal control ([AS 2201](#))
- Representations of management ([AS 2201](#))
- Fraud and illegal acts ([AS 2401](#) and [2405](#))
- Communications in connection with interim reviews ([AS 4105](#))
- Preapproval of services ([Rules 3524](#) and [3525](#))
- Independence matters ([Rule 3526](#))
- Related parties ([AS 2410](#))
- Auditing fair-value measurements and disclosures ([AS 2502](#))





### PCAOB adopts changes to the auditor's report

The SEC approved the standard requiring changes to the auditor's report on October 23, 2017. In a statement announcing its approval of this standard that significantly modifies the auditor's reporting model, Chairman Jay Clayton stated his strong support for the objective of the rule, namely for the auditors to provide investors with meaningful insights into the audit. Chairman Clayton highlighted the important role of the audit committee and noted that the SEC and PCAOB will monitor the results of the new standard's implementation, including consideration of any unintended consequences.

The new auditor reporting standard will significantly modify the auditor's reporting model while retaining the current "pass/fail" opinion of the existing auditor's report. The primary changes include:

- Standardized ordering and inclusion of section headers, with the opinion section appearing first
- Enhanced descriptions of the auditor's role and responsibilities, including a statement regarding independence requirements
- Communication of critical audit matters (CAMs)
- Disclosure of auditor tenure—the year in which the auditor began serving consecutively as the company's auditor.

A CAM is defined as a matter communicated, or required to be communicated, to the audit committee that:

- Relates to accounts or disclosures that are material to the financial statements
- Involves especially challenging, subjective, or complex auditor judgment.

The new requirements will be phased in, with CAM disclosure effective for large accelerated filers for audits of fiscal years ending on or after June 30, 2019, and for all other audits to which the requirement applies for fiscal years ending on or after December 15, 2020. The remaining changes apply to auditor reports issued for fiscal years ending on or after December 15, 2017.

Although the standard will be implemented in accordance with phased-in effective dates, management and audit committees will most likely want to start to consider the implications of the new requirements and discuss them with their auditors. Potential questions regarding CAMs may include:

- What matters could be CAMs?
- How will management and the audit committee engage with the auditor as CAMs are identified and the auditor's descriptions of the CAMs are developed and finalized?
- How will the timing of auditor communications with management and the audit committee accommodate the discussion of CAMs?
- How do the auditor's statements regarding CAMs compare to management's disclosures regarding the same matters?

Deloitte's [Heads Up](#) provides additional information on the new rule.

*I strongly support the objective of the rule to provide investors with meaningful insights into the audit from the auditor. CAMs are designed to provide investors and other financial statement users with the auditor's perspective on matters discussed with the audit committee that relate to material accounts or disclosures and involve especially challenging, subjective, or complex auditor judgment. Investors will benefit from understanding more about how auditors view these matters.*

**Jay Clayton, SEC Chairman**

### Auditor independence

The SEC and PCAOB rules govern the independence of accountants who audit or review financial statements and prepare attestation reports filed with the SEC. The rules recognize the critical role of audit committees in financial reporting, their unique position in monitoring auditor independence, and their direct responsibility for the oversight of the independent auditor. Although most audit firms are rigorous in monitoring and enforcing these independence requirements, it is important that audit committee members be aware of them as well.

The SEC independence rules address the following issues related to registrants.

**Financial interests.** The rule states that independence is impaired if the audit firm or certain of its people have a direct or material indirect financial interest in an audit client. Examples of prohibited financial interests include an investment in the audit client's debt or equity securities, certain loans, deposits not fully insured by the Federal Deposit Insurance Corporation, broker-dealer account balances not fully insured by the Securities Investor Protection Corporation, and certain individual insurance products.

**Employment relationships.** The rule states that independence is impaired if a current partner, principal, shareholder, or professional employee of the independent auditor has an employment relationship with, or serves as a member of the board or similar management or governing body of, the audit client. Former partners, principals, shareholders, or professional employees of the independent auditor cannot be employed in an accounting role or financial reporting oversight role—one who exercises more than minimal influence over the contents of accounting records or prepares them—at an audit client unless

they are fully separated from the independent auditor, financially and otherwise. Even if this separation is achieved, former members of the audit engagement team for an issuer cannot take a financial reporting oversight role for the issuer before completion of one annual audit subsequent to the engagement period when the individual was a part of the engagement team. Employment restrictions also apply to certain close family members of the independent auditor's personnel.

**Business relationships.** The rule prohibits an independent auditor from having a direct or material indirect business relationship with an audit client, or with persons associated with the audit client in a decision-making capacity, such as an audit client's officers, directors, or substantial stockholders. This prohibition does not preclude the independent auditor from providing permissible services to the audit client or purchasing goods or services from the audit client as a consumer in the ordinary course of business, commonly known as a vendor business relationship.

**Nonaudit services provided by auditors.** The rule sets forth 10 categories of services that impair the auditor's independence if provided to an audit client. The rule permits an auditor to provide other nonaudit services to an issuer if the services are preapproved by the audit committee. Permissible nonaudit services include due diligence for mergers and acquisitions, internal control reviews, and tax services that are not prohibited by the PCAOB.

In certain limited circumstances, the independent auditor may provide bookkeeping, design, and implementation of financial information systems; appraisal or valuation services; actuarial services; and internal audit outsourcing to a nonclient affiliate of an

audit client if "it is reasonable to conclude that the results of these services will not be subject to auditing procedures during an audit of the audit client's financial statements." This is referred to as the "not-subject-to-audit" exception.

The following nonaudit services are prohibited to the independent auditor:

- Bookkeeping or other services related to the accounting records or financial statements of the audit client
- Design and implementation of financial information systems
- Appraisal or valuation services, fairness opinions, or contribution-in-kind reports
- Actuarial services
- Internal audit outsourcing
- Management functions
- Human resources
- Broker-dealer, investment advisory, or investment banking services
- Legal services
- Expert services.

**The audit committee's administration of the audit engagement (preapproval).** The audit committee must preapprove permissible audit and nonaudit services to be provided to the issuer and its subsidiaries. Preapproval can be obtained directly or based on policies and procedures established by the audit committee that are detailed as to the type of service. These policies and procedures do not circumvent the need to inform the audit committee of the service, and the committee cannot delegate its preapproval responsibilities to management. It can, however, delegate preapprovals to one or more members

of the committee if the preapprovals are reported at the next scheduled meeting of the full committee.

Further, the PCAOB rules provide that an audit firm seeking preapproval of tax services or nonaudit services related to internal control over financial reporting must:

- Describe, in writing, the scope of the service. For tax services, the audit firm must describe, in writing, (i) the fee structure for the engagement, any side letter or other amendment to the engagement letter, or any other agreement between the firm and the audit client relating to the service; and (ii) any compensation arrangement or other agreement between the registered public accounting firm or an affiliate and any person other than the audit client with respect to promoting, marketing, or recommending a transaction covered by the service.
- Discuss with the audit committee of the issuer the potential effects of the services on the independence of the firm.

**Contingent fees and commissions.** The rule states that independence is impaired if the independent auditor provides any service or product to an audit client for a contingent fee or a commission, or receives a contingent fee or commission from an audit client. The PCAOB also has discretion to prohibit any other service that it determines, by regulation, to be impermissible. In addition to prohibiting the independent auditor from providing a service or product to an audit client for a contingent fee or commission, the PCAOB has issued rules prohibiting the independent auditor from:

- Marketing, planning, or opining in favor of the tax treatment of a confidential or aggressive tax transaction
- Providing tax services to persons in a financial reporting oversight role for an audit client.

**Partner rotation.** The rule requires the lead audit and engagement quality review partners to rotate after five years, at which time they are subject to a five-year “time-out” period. Audit partners who are significantly involved with senior management or the audit committee or who are responsible for decisions on accounting matters that affect the financial statements must rotate after seven years and are subject to a two-year time-out period. This includes audit partners who serve as the lead partner for significant subsidiaries. Significant subsidiaries are defined as those accounting for greater than 20 percent of an issuer’s revenues or assets. Other specialty partners, such as tax partners, are not required to rotate.

**Compensation of audit partners.** Under the SEC’s rule, an auditor is not independent if, at any point during the audit and professional engagement period, any audit partner receives compensation from selling engagements to provide the audit client with any services other than audit, review, or attest services.

For the purpose of this restriction, the SEC defines the term “audit partner” as the lead and concurring partners and other partners on the engagement team who have responsibility for making decisions on significant auditing, accounting, and reporting matters that affect the financial statements or who maintain regular contact with management or the audit committee. This includes all audit partners serving the client at the issuer or parent, with the exception of specialty partners, as well as the lead partner at subsidiaries whose assets or revenues constitute at least 20 percent of the consolidated assets or revenues.

#### **Evaluation of the independent auditor**

Inherent in the audit committee’s duty to appoint, compensate, and oversee the independent auditor is the idea that the audit committee will do some form of evaluation of the auditor.

The NYSE listing standards require the audit committee to review a report by the independent auditor describing its quality controls, results of investigations, and independence. The commentary accompanying this listing standard states that after reviewing the report and the independent auditor’s work throughout the year, the audit committee will be in a position to evaluate the auditor’s qualifications, performance, and independence. The commentary to this standard specifies that the “evaluation should include the review and evaluation of the lead partner of the independent auditor,” and “should take into account the opinions of management and the company’s internal auditors (or other personnel responsible for the internal audit function).”

Practices for evaluating the independent auditor range from highly formalized processes with extensive documentation to more informal assessments. Factors the audit committee may consider in developing an evaluation process include:

- **Frequency and timing of the evaluation.** Many audit committees perform the evaluation annually, immediately following the issuance of the Form 10-K and in conjunction with their decision to reappoint the independent auditor.
- **Parties involved in the assessment.** Although the SEC does not explicitly require the audit committee to formally evaluate the independent auditor, many committees conduct some form of evaluation to make decisions on the auditor’s initial appointment or annual reappointment. While the audit committee is responsible for the appointment, compensation, and oversight of the independent auditor, it may not be practical for the audit committee to oversee and coordinate the entire evaluation. In many instances, the audit committee delegates the coordination responsibility to internal

audit, the legal department, or another group in the company. The party responsible for coordinating the evaluation should obtain information not only from the audit committee, but also from senior financial management and the internal auditors. Depending on the size and structure of the company, it may be appropriate to obtain input from the management of significant operating locations or business units.

- **Form and nature of the assessment.**

Some independent auditors have assessment questionnaires for evaluating client service. Audit committees can use these questionnaires, tailor them to fit their needs, or create their own. The assessment can be done by having the relevant parties complete the questionnaire in writing or by holding interviews. They may also have a discussion about the experience the audit committee and others at the company have had in working with the independent auditor.

- **Assessment criteria.** The criteria for evaluating the independent auditor vary. Common criteria specific to the engagement team include technical competence; industry knowledge; frequency and quality of communication; cohesiveness as a team; demonstrated independence, objectivity, and professional skepticism; and the level of support provided to the audit committee in fulfilling its responsibilities. Audit committees may consider information about the characteristics of the audit firm itself, such as size, financial strength and stability, presence in key markets, approach to professional development, technological capabilities, nature of the audit approach, quality of thought leadership, and eminence in the marketplace. The results of the PCAOB inspection process and peer reviews may also be considered in the evaluation.

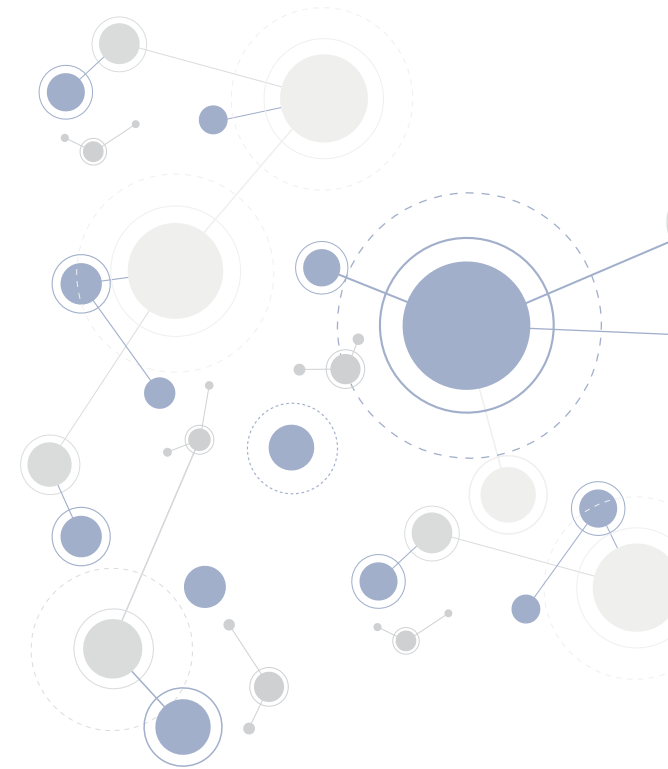
## Tools and resources

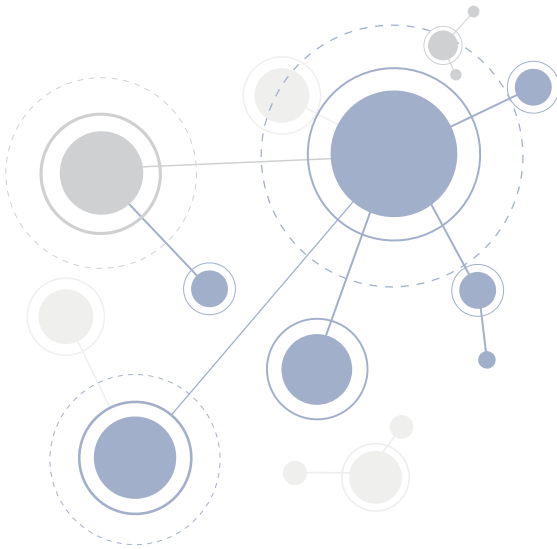


For additional information, read Deloitte's [\*Appointing, Assessing, and Compensating the Independent Auditor: The Role of the Audit Committee\*](#).

The Audit Committee Collaboration, a partnership of the Center for Audit Quality and US corporate governance and policy organizations, has issued an [\*External Auditor Assessment Tool\*](#) for audit committees. The tool assists audit committees in carrying out their responsibility of appointing, overseeing, and determining compensation for the independent auditor.

The PCAOB issued [\*Information for Audit Committees about the PCAOB Inspection Process\*](#) to help audit committees better understand the PCAOB's inspection process and how to gather information from their audit firms about inspections.





## Questions for audit committees to consider

### **Audit innovation**

With advances in technology, auditors are turning to innovation to enhance quality and drive value into the audit. In understanding how the independent auditor is using innovation, the audit committee may consider the following questions:

- How is the independent auditor leveraging innovation to enhance audit execution?
- What investments is the independent auditor making in audit innovation, and how do those investments translate to enhanced audit quality and value for the company?
- What insights is the independent auditor able to provide about the company and its financial and internal controls processes through the audit and with the use of new technologies, including audit analytics?
- What are some of the emerging technologies that the independent auditor is exploring for use in the audit? How may the company benefit from the independent auditor's use of these emerging technologies?
- With respect to innovation, how is the independent auditor differentiating itself from competitors to add value to the audit?

## Ethics and compliance

As highlighted by several court rulings and the US Federal Sentencing Guidelines for organizations, executives and boards of directors have special responsibilities for the oversight and management of ethics and compliance programs, an important component of which is a robust code of ethics or conduct.

The board should consider the audit committee's role in overseeing the company's ethics and compliance programs, noting that NYSE-listed companies are required to have the audit committee oversee legal and regulatory compliance.

### Ethics and code of conduct

A culture that embraces the importance of ethics and compliance can be established only if employees, officers, and directors understand the requirements of the code of ethics.

The SEC, the NYSE, and NASDAQ all require a code of ethics or a code of conduct. There are similarities among the requirements, but there are also differences.

**SEC requirements.** The SEC requires registrants to disclose whether they have written codes of ethics that apply to their principal executive officers, principal financial officers, principal accounting officers or controllers, or individuals performing similar functions. If they do not, they must explain why not. A company registered in the United States must disclose any changes to, or waivers from, the code of ethics that apply to the CEO or senior financial officers, generally within four business days after it amends its code of ethics or grants a waiver. The NYSE and NASDAQ listing standards have the same four-day rule.

The SEC rule defines a code of ethics as a written standard that is reasonably designed to deter wrongdoing and to promote:

- Honest and ethical conduct, including the ethical handling of actual or apparent conflicts of interest in personal and professional relationships
- Full, fair, accurate, timely, and understandable disclosure in the company's SEC filings and other public communications
- Compliance with applicable laws, rules, and regulations
- The prompt internal reporting of violations to parties identified in the code
- Accountability for adherence to the code.

Companies must include these disclosures in their annual reports and must make the code of ethics available to the public through one of the methods listed in [Item 406 of Regulation S-K](#).

**NYSE requirements.** NYSE listing standards require a code of conduct that covers not only senior financial officers, but all employees. Specifically, the websites of NYSE-listed companies must disclose the code of conduct applicable to employees, directors, and officers. Companies can determine their own policies, but the code must contain the items listed in [NYSE 303A.10](#), only some of which are required by the SEC.

**NASDAQ requirements.** NASDAQ listing standards require public disclosure of a code of conduct applicable to all employees, officers, and directors. NASDAQ's criteria for the code of conduct are consistent with the SEC's requirements.



# 86%

of audit committees receive a report on internal tips from a hotline or other reporting mechanism at least once a year



# 26%

of audit committees receive these reports at every committee meeting

Source: Deloitte 2016 Board Practices Report

In addition, each code of conduct must provide for prompt and consistent enforcement, protection for individuals who report questionable behavior, clear and objective standards for compliance, and a fair process for addressing violations.

Both the NYSE and NASDAQ listing standards permit companies to have more than one code of conduct as long as all directors, officers, and employees are covered by a code. For example, some companies have developed a separate code for directors, whose roles and responsibilities differ from those of officers and other employees.

**Common practices and considerations.** Those responsible for overseeing ethics and compliance should work with management to determine that the company's code of ethics or conduct complies with the applicable requirements. Companies may update the code in response to new issues or situations. Legal counsel should be consulted on modifications to the code.

Communication and training are critical to fostering an ethical culture. The code should be available to everyone in the organization, perhaps through inclusion on the company's intranet site and in the employee orientation program and manual. Some companies require individuals, including directors, to sign an annual certification noting that they have read, understood, and complied with the code. If an employee refuses to sign the certification, committees should encourage companies to take prompt and appropriate disciplinary action, up to and including termination. Communication of disciplinary actions taken in response to code violations is a common way of communicating to employees that violations are taken seriously.

## Questions for audit committees to consider



### Ethics and compliance

To the extent the audit committee is charged with the responsibility to oversee ethics and compliance:

- Does the committee hear directly from the person who has day-to-day responsibility for ethics and compliance matters? Does this person have the ability to hold these discussions in an executive session?
- Do the ethics and compliance governance framework, organizational structure, and reporting lines provide sufficient independence for the audit committee to execute its responsibilities (e.g., does the chief ethics and compliance officer report directly or indirectly to the audit committee)?
- Does the ethics and compliance officer have adequate staff, technology, and other resources to do an effective job?
- Does the company regularly and systematically scrutinize the sources of ethics and compliance failures and react appropriately?
- How does management take action on reports? Is there evidence of employees being disciplined promptly, appropriately, and consistently?
- Does the reporting process keep the audit committee informed of ethics and compliance issues, as well as the actions taken to address them? Is ethics and compliance a regular item on the committee's agenda?
- What type of ongoing monitoring and auditing processes are in place to assess the effectiveness of the ethics and compliance program?
- Is the company's risk culture encouraging the right type of behaviors?

## Tools and resources



Deloitte's ethics and compliance resources offer additional information on establishing codes of ethics and robust ethics and compliance programs, including [Building World-Class Ethics and Compliance Programs: Making a Good Program Great](#), and [In Focus: Compliance Trends Survey](#), a collaboration between Deloitte and Compliance Week.

### Reporting hotline procedures

Companies often use hotlines as a mechanism to report a range of ethics and compliance issues, including potential violations of the code of ethics. A thorough, independent, and objective process should be established by management and the audit committee for investigating complaints. Companies use various procedures, but the most common method of receiving tips from inside and outside the organization is through a telephone and Web-based hotline administered by an internal department or a third party.

SEC regulations and the NYSE and NASDAQ listing standards require the audit committees of listed companies to establish procedures for:

- Receiving, retaining, and addressing complaints regarding accounting, internal controls, or auditing matters, whether from internal or external sources who wish to remain anonymous, as well as reporting a range of compliance matters, including violations of the code of conduct and allegations of fraud or corruption
- The confidential, anonymous submission of employee concerns regarding questionable accounting or auditing matters.

The audit committee should work with management to confirm that the appropriate members of management are aware of questions or complaints received from internal sources and third parties, including vendors, through the various reporting methods available. Responsibility for investigating questions or concerns and reporting back to the audit committee often falls on individuals in the ethics and compliance, internal audit, legal, or risk management departments.

The audit committee should also establish expectations with respect to the type of complaints that will be reported to them and how they will be communicated. Some complaints may warrant immediate communication, such as those involving senior management and significant dollar amounts. In addition to these immediate reporting situations, the audit committee should receive a regular analysis of the complaints received, including a root-cause analysis; their resolution; and the steps taken to avoid similar violations in the future. The audit committee should also determine which complaints warrant a discussion with the board.

A telephone and Web-based hotline monitored by an independent third party is common. If the hotline is administered internally, operators should have specific training on where to direct questions or complaints, including those related to human resources, as well as the ability to provide coverage 24 hours a day, 365 days a year and include an anonymous reporting option. Employees can be informed of reporting channels in the code of ethics, the employee handbook, human resources orientation, ethics training, and periodic communications. Instructions for submitting questions or complaints can be posted in company facilities and on intranet sites.

The company's public website is a natural vehicle for communicating the procedures to individuals outside the organization. As discussed in the code of ethics section, NYSE listing standards require companies to adopt codes of ethics and disclose them on their websites. NASDAQ-listed companies also must adopt and disclose codes of ethics, and many have chosen to post their codes on their websites. Telephone operators working in customer service and investor relations should be prepared to answer questions on how to submit concerns and

complaints regarding financial reporting.

Under the SEC's whistleblower programs, employees with knowledge of potential securities fraud who report original information to the government or a self-regulatory organization can receive a minimum of 10 percent and as much as 30 percent of monetary sanctions if the enforcement action results in fines of at least \$1 million.

Whistleblowers are not required to report issues first through internal company channels; however, those who do so are still eligible for the reward if the company reports the problem to the government or if the whistleblower does so within 120 days of notifying the company.

It is important for the audit committee to work with management and internal audit to understand:

- How hotlines are evaluated, tested, and audited to ensure calls are received, recorded, and managed in a consistent, confidential, accurate, and timely manner
- Opportunities to enhance internal whistleblowing systems and promote reporting mechanisms to all personnel
- The potential value of transaction monitoring tools to help promptly identify potential securities fraud issues such as bribery or financial statement fraud.

Companies with operations in different countries should be careful to comply with those countries' laws, as they may impose requirements, restrictions, and prohibitions different from those applicable in the United States.



*Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It can help an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluating and improving the effectiveness of risk management, control, and governance processes.*

#### **Institute of Internal Auditors**

## Oversight of internal audit

An effective relationship between the audit committee and the internal auditors is fundamental to the success of the internal audit function. It is important for audit committees to assess whether internal audit's priorities, such as monitoring critical controls and developing an audit plan focused on risks identified in the enterprise risk management program, are aligned with those of the audit committee. At some companies, internal audit evaluates and considers suggestions to improve operations and processes.

When the internal audit function reports to the audit committee directly, it allows the internal auditors to remain structurally separate from management and enhances objectivity. This also encourages the free flow of communication on issues and promotes direct feedback from the audit committee on the performance of the chief audit executive.

**NYSE requirements.** The NYSE listing standards require companies to have an internal audit function. Audit committees are required to oversee the internal audit function and to note this responsibility in their charters. Specific requirements include:

- The audit committee charter must include oversight of the internal audit function as one of its purposes.
- The audit committee's regular report to the board should include issues involving the performance of the internal audit function.
- The audit committee must meet separately with the internal auditors.

**NASDAQ requirements.** The audit committee oversees the accounting and financial reporting processes of the company. Although NASDAQ companies are not required

to have an internal audit function, for those that do, oversight of internal audit is often one component of overseeing accounting and financial reporting.

**Common practices and considerations.** The specific expectations for internal audit functions vary by organization, but may include:

- Objectively monitor and report on the health of financial, operational, and compliance controls
- Provide insight into the effectiveness of risk management
- Offer guidance regarding internal/compliance controls
- Act as a catalyst for positive change in processes and controls
- Deliver value to the audit committee, other directors, and management in the areas of controls and risk management to assist in the audit committee's assessment of the efficacy of programs and procedures
- Coordinate activities and share perspectives with the independent auditor.

In support of these expectations, the audit committee and the chief audit executive (CAE) should have a strong relationship characterized by open communication. The audit committee should challenge the CAE and the internal audit department by setting high expectations, communicating those expectations clearly, and holding the department accountable for meeting them. The CAE should be candid in raising concerns with the audit committee when they arise.

It is important for the audit committee to see that the internal auditors have appropriate independence and

stature and are visibly supported by senior management throughout the organization. They should support the CAE, providing guidance and assistance when he or she reports potential management lapses.

In addition to making themselves available when contacted by the CAE, members of the audit committee should engage with the CAE regularly to maintain a reporting relationship that is both substantive and communicative. Holding regular executive sessions with the CAE is common and is required for NYSE-listed companies. The audit committee should actively participate in discussing goals and evaluating the performance of the CAE; these responsibilities should not be delegated solely to the CFO or CEO.

The audit committee should understand and approve the annual internal audit plan and determine if the CAE has a sufficient budget and related resources to execute against it. In determining that resources are adequate, audit committees often consider whether the CAE and his or her staff are adequately compensated. As part of this review, they should review and evaluate the status of the enterprise-wide risk management program and the alignment of risks to the internal audit plan. The audit committee should also evaluate the progress and results of the internal audit plan against the original plans and any significant changes made subsequently.

[The International Standards for Professional Practice of Internal Auditing](#) established by the Institute of Internal Auditors (IIA) require internal auditors to maintain a certain level of independence from the work they audit. This means that an internal auditor should have no personal or professional involvement with the area being audited and should maintain an impartial perspective on all engagements. Internal auditors should have access

to records and personnel when necessary, and they should be allowed to employ appropriate investigative techniques without impediment.

Internal audit departments should also employ quality processes with a focus on continuous improvement. These processes should be periodically reviewed through self-assessment and/or external reviews. The IIA's standards require external assessments to be

conducted by a qualified, independent party at least once every five years. The CAE should discuss the form and frequency of the external assessment, as well as the qualifications and independence of the external assessor, with the audit committee.

## Oversight of internal audit



There are several ways the audit committee can oversee the internal audit function. The IIA provides the following checklist of considerations for audit committees in overseeing the internal auditors:

- The audit committee engages in an open, transparent relationship with the CAE.
- The audit committee reviews and approves the internal audit charter and internal audit plan annually.
- As a result of discussions with the CAE, the audit committee has a clear understanding of the strengths and weaknesses of the organization's internal control and risk management systems.
- Internal audit is sufficiently resourced with competent, objective professionals to carry out the internal audit plan, which has been reviewed and approved by the audit committee.
- Internal audit is empowered to be independent by its appropriate reporting relationships to executive management and the audit committee.
- The audit committee addresses with the CAE all issues related to internal audit independence, objectivity, and resources.
- Internal audit is quality-oriented and has a quality assurance and improvement program in place.
- The audit committee regularly communicates with the CAE about the performance and improvement of the CAE and internal audit.
- Internal audit reports are actionable, and audit recommendations and other improvements are implemented by management satisfactorily.
- The audit committee meets periodically with the CAE without the presence of management.



## Questions for audit committees to consider

### Interactions with internal audit

- Does internal audit have a clearly articulated strategy that is reviewed and approved by the audit committee periodically?
- Does internal audit have a clear set of performance expectations that are aligned with the success measures of the audit committee and measured and reported to the audit committee?
- Does internal audit have a charter that is reviewed and approved by the audit committee periodically? Does internal audit operate in accordance with its charter?
- Is the internal audit plan aligned to the primary risks of the organization and other assurance activities? Is internal audit's risk assessment process linked to the company's enterprise risk management activities appropriately?
- Is internal audit flexible and dynamic in addressing new risks promptly and meeting the needs of the audit committee?
- Is internal audit effective in using advanced technologies, such as data analytics, to improve audit quality?
- Does internal audit organize or perform peer reviews or self-assessments of its performance and report the results to the audit committee?
- Does the CAE have the right mix of experience and capabilities, including industry knowledge and business acumen, to understand the company's risks?
- Does the CAE have a professional certification, such as certified internal auditor, and participate in relevant continuing education programs?
- Is internal audit funded and adequately and staffed with the appropriate mix of professionals needed to achieve its objectives?
- Does internal audit's reporting structure within the organization ensure sufficient independence and respect from management and other employees?
- Is the level of assurance provided by internal audit and its interaction with other assurance sources clear and appropriate for the audit committee?
- Does the internal audit function have and demonstrate the level of independence needed to execute its responsibilities properly?
- Does internal audit meet with the independent auditor regularly to discuss risk assessments, the scope of procedures, or opportunities to achieve greater efficiencies and effectiveness in the company's audit services?
- Does internal audit report issues in a timely manner and address them with management?
- Are issues identified and reported by internal audit highlighted to the audit committee appropriately, and is the progress of remediation tracked and reported?
- Are reports and other communications from internal audit to the audit committee of an appropriate standard and do they provide value?

## Other interactions with management and the board

In executing their governance responsibilities, audit committees frequently interact with other stakeholders, in addition to the internal and independent auditors.

### Interactions with the finance organization

The finance function's leaders and professionals can have a direct impact on a company's risk profile, value creation, and return on investment for investors and other stakeholders. The audit committee relies significantly on the finance function and needs to maintain an open and effective relationship with them. Their oversight can contribute to the finance organization's interest in having the right resources available to support the quality and reliability of financial accounting, reporting, and related controls. Audit committees may also provide input on the assessment and compensation of finance professionals who they interact with regularly.

The audit committee can help monitor and strengthen finance talent initiatives, in particular the succession plans for leaders and finance professionals in roles of critical importance, through regular discussions with the CEO, CFO, and other finance executives, as well as regular oversight of issues related to finance talent.

**Common practices and considerations.** Interactions with the finance organization vary, but may include the following practices:

- To foster open communication, meet periodically with management, the director of the internal audit function, and the independent auditor in separate executive sessions ([NYSE Corporate Governance Rule 303A.07\(b\)\(iii\)\(E\)](#)).
- Provide input on the performance of key finance executives, including the CFO and CAO.
- Provide input into management's goal-setting process.
- Hold annual discussions of succession planning for the finance organization with the CEO and CFO and regular discussions of the finance organization's bench strength.
- Invite succession candidates to present during audit committee meetings to develop a firsthand view of their potential.
- Understand management's process for early identification and resolution of accounting and other issues.
- Understand plans to address new accounting and reporting requirements and related risks.
- Visit company locations and meet with members of management periodically.

## Questions for audit committees to consider



### Finance organization talent

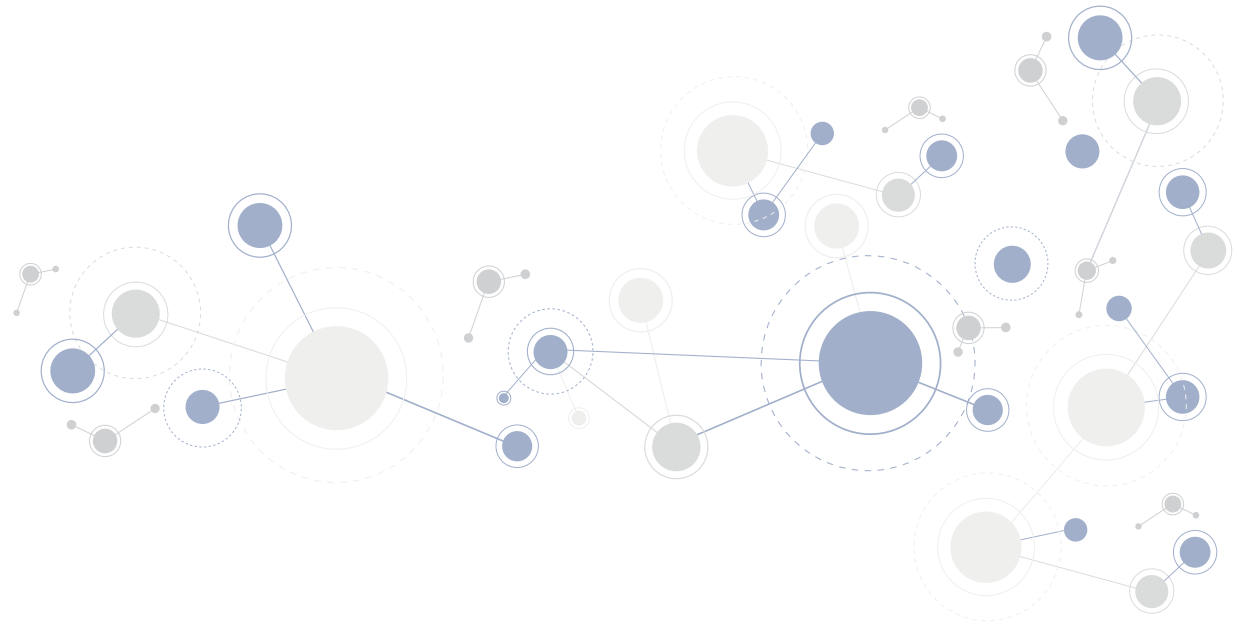
- Do you have adequate personnel, both in numbers and quality, to fulfill your responsibilities with respect to the financial statements and internal control over financial reporting?
- What is the succession plan for key finance positions?
- Are there finance professionals in the pipeline of potential leaders that the audit committee should meet? Are succession candidates given an opportunity to meet with the audit committee?
- What plans are in place to respond to unexpected turnover in finance roles? Is someone ready to begin immediately, and if not, what are the backup plans to hire temporary resources?
- What formal training and development programs are in place to keep finance professionals up to date with the latest developments and requirements? Do professionals receive training on advanced technologies that could enhance the effectiveness of the finance organization?
- How does the audit committee participate in the evaluation of the CFO? What kind of evaluation criteria are important to the audit committee?

### Interactions with the board and other committees

As the audit committee seeks to align its structure with the company's strategic priorities, it should consider the coordination required among other board committees and the full board to facilitate the optimal allocation and coverage of topics that affect more than one group and to reduce the likelihood of something falling through the cracks. The audit committee should understand the roles and responsibilities of other board committees and consider whether they could benefit from periodic joint meetings to discuss areas of common interest and significant matters.

It is particularly important for the audit committee to coordinate with the compensation committee as it considers the risk that compensation policies have on the financial statements and internal controls. The audit committee should understand management and general employee compensation plans and how related metrics may affect fraud risks. Additionally, as companies increasingly use non-GAAP metrics to determine compensation, the audit committee should understand how those metrics may impact risk and may need to be addressed in the reconciliation between non-GAAP and GAAP information.

The audit committee chairman should also coordinate with the nominating and governance committee as it considers board candidates. The chairman should communicate the skills and experiences needed from members to effectively carry out the audit committee's responsibilities.



## Audit committee external communications

Investors, policymakers, and regulators are continuing to show interest in more detailed disclosure about audit committees, their activities, and their oversight of the relationship with independent auditors. As these external parties request additional clarification about the roles and responsibilities, audit committees should consider whether they should enhance disclosures in the proxy statement.

Various SEC rules and exchange listing requirements address audit- and audit committee-related information that must be disclosed in the proxy statement, including the audit committee report, and on company websites.

SEC rules require companies to disclose the name of each audit committee member and include an audit committee report in their proxy statements. In the report, the audit committee must state whether it has:

- Reviewed and discussed the audited financial statements with management
- Discussed with the independent auditor all matters required under applicable auditing standards
- Received required independence disclosures from the independent auditor.

Based on this review and discussion, the report must also include a statement of whether the audit committee recommended to the board that the audited financial statements be included in the annual report to be filed with the SEC.

Proxy statements must disclose whether the board has adopted a written charter for the audit committee, and if so, include a copy of the charter as an appendix to the proxy statements at least once every three years.

## Audit committee reporting



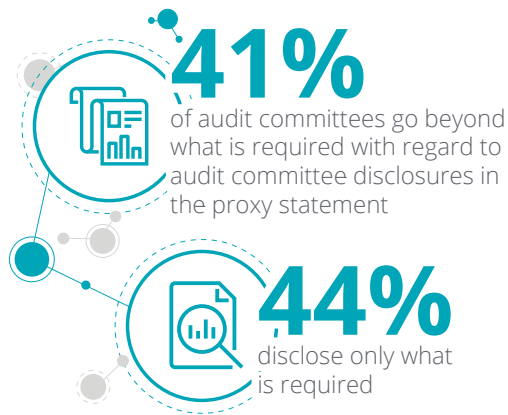
Over the past several years, investors and other governance groups and investors have sought expanded disclosures on how audit committees execute their duties. As recently as November 2016, the United Brotherhood of Carpenters' Pension Fund announced that it would send letters to 75 companies encouraging their audit committees to enhance auditor independence disclosures in 2017 proxy statements—a request they have been making since 2013. The SEC weighed in on the discussion when it issued a request for public comment in a July 2015 concept release titled [Possible Revisions to Audit Committee Disclosures](#).

Deloitte's latest proxy statement analysis, [Audit Committee Disclosure in Proxy Statements – 2017 Trends](#), indicates that companies have generally increased voluntary disclosures about the role and activities of audit committees over the past several years. While it is not necessary, or possible, to disclose everything an audit committee does each year in fulfilling its duties, additional insight into the structure and activities of the audit committee can help increase investor confidence in both the committee and the company as a whole.

The Center for Audit Quality (CAQ) and Audit Analytics published the [Audit Committee Transparency Barometer](#) in November 2016, which presents findings from an analysis of audit committee disclosures in proxy statements and measures the robustness of these disclosures among S&P Composite 1500 companies. The report measures the content of proxy statement disclosures in areas that include auditor oversight and scope of duties. The CAQ joined with several governance organizations in 2013 to form the Audit Committee Collaboration,<sup>1</sup> which released a report titled [Enhancing the Audit Committee Report: A Call to Action](#) in November 2013 to encourage enhanced audit committee disclosures.

The calls for increased transparency into audit committee duties, including the oversight of the independent auditor, are expected to continue to grow. Audit committees can respond by providing more meaningful disclosures that increase awareness of their responsibilities and how individual committees carry them out. For more information, read the [July 2015 Audit Committee Brief: SEC Issues Concept Release Concerning Audit Committee Reporting Requirements](#).

<sup>1</sup> The following groups are members of the Audit Committee Collaboration: Association of Audit Committee Members, Inc.; Center for Audit Quality; Corporate Board Member/NYSE Euronext; The Directors' Council; Independent Directors Council; Mutual Fund Directors Forum; National Association of Corporate Directors; and Tapestry Networks.



Source: Deloitte 2016 Board Practices Report

Companies whose securities are quoted on NASDAQ or listed on the NYSE must disclose whether the audit committee members are independent as defined in the applicable listing standards, as well as certain information regarding any director on the audit committee who is not independent.

Regulators continue to solicit views of audit committees with respect to industry- and company-specific knowledge and experience. Taking the time to engage in formal or informal communication with regulators, industry groups, or the independent auditor on these topics can have a substantive impact on the development of standards and rules.

### Fee disclosure

The SEC rule requires disclosure of fees paid to the independent auditor for the current and prior years, as well as a description of the services included in all categories, other than for audit fees, for both years. The audit committee's preapproval policies and procedures must be disclosed in a detailed description or by including the policy itself, along with disclosure

of any services that were initially missed and later approved under a de minimis exception in the SEC's rule. Disclosures are required in the issuer's annual report as well as the proxy statement, but companies are allowed to incorporate the information into their Form 10-K from their proxy statement.

The SEC's rule that implemented the Sarbanes-Oxley Act expanded the requirements to disclose fees paid to the auditor, and many companies have opted to provide even more information. For instance, many companies subtotal the audit and audit-related fees so shareholders can easily quantify the portion of services that are audit and audit-related in nature.

Because certain institutional investors and proxy advisers, such as Institutional Shareholder Services, have guidelines for proxy-vote recommendations related to audit fees, many companies disclose not only the nature of services in the fee categories but also the amounts associated with specific services. Issuers should consult with legal counsel to determine the content of the fee disclosure. The SEC's four fee categories are:

- **Audit fees** are fees for services that normally would be provided in connection with statutory and regulatory filings or engagements, including the audit of internal control over financial reporting. This category also may include services that only the independent auditor reasonably can provide, such as comfort letters, statutory audits, attest services, consents, and assistance with documents filed with the SEC. Audit fees may include certain services provided by specialists who assist in the audit, such as tax specialists needed to audit the tax provision or valuation specialists needed to audit a fair-value assertion; certain accounting consultations in connection with the audit; and similar items that

are not billed as audit services and that only the independent auditor reasonably can provide.

- **Audit-related fees** are for assurance and related services that are performed by the independent auditor, such as audits of employee benefit plans; due diligence related to mergers and acquisitions; accounting consultations and audits in connection with acquisitions; internal control reviews, although not the audit of internal control over financial reporting, which is part of audit fees; attest services that are not required by statute or regulation; and consultation concerning financial accounting and reporting standards to the extent that such consultation is not necessary to complete the GAAS audit.
- **Tax fees** include all tax services except those related to the audit, such as review of the tax provision, which would be included in audit fees. Typically, tax fees cover tax compliance, planning, and advice. Tax compliance generally involves preparation of original and amended tax returns, refund claims, and planning services related to tax payments. Tax planning and tax advice encompass a diverse range of services, including assistance with tax audits and appeals, tax advice related to mergers and acquisitions, employee benefit plans, and requests for rulings or technical advice from tax authorities. The provision of tax services is subject to certain restrictions, among which are that company personnel must make all management decisions and perform all management functions, and that services cannot be provided for an employee with a financial oversight role.
- **All other fees** include all fees paid to the independent auditor for services other than audit, audit-related, or tax services.

# Authors



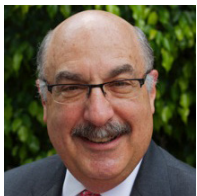
**Maureen Bujno**  
**Managing Director**  
Center for Board Effectiveness  
Deloitte LLP  
[mbunjo@deloitte.com](mailto:mbunjo@deloitte.com)



**Consuelo Hitchcock**  
**Principal**  
Audit Regulatory Affairs  
Deloitte & Touche LLP  
[chitchcock@deloitte.com](mailto:chitchcock@deloitte.com)



**Krista Parsons**  
**Managing Director**  
Center for Board Effectiveness  
Deloitte & Touche LLP  
[kparsons@deloitte.com](mailto:kparsons@deloitte.com)



**Bob Lamm**  
**Independent Senior Advisor**  
Center for Board Effectiveness  
Deloitte LLP  
[rlamm@deloitte.com](mailto:rlamm@deloitte.com)

## Acknowledgements

Deloitte would like to thank Alexia Gleeson and Amanda Piccolini for their assistance with the creation of this edition of the *Audit Committee Resource Guide*.

# Contact us



**Deb DeHaas**  
**Vice Chairman and  
National Managing Partner**  
Center for Board Effectiveness  
Deloitte  
[ddehaas@deloitte.com](mailto:ddehaas@deloitte.com)



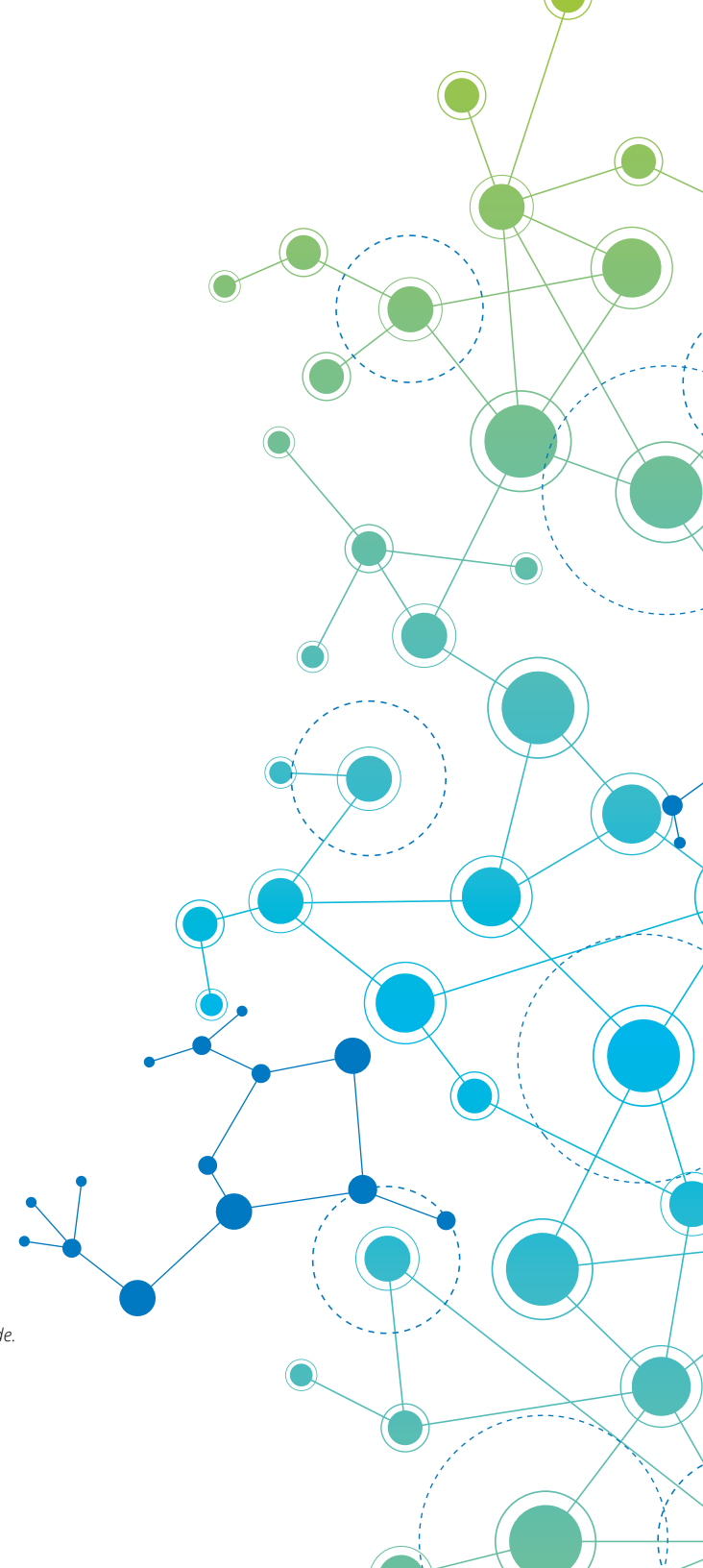
**Henry Phillips**  
**Vice Chairman and  
National Managing Partner**  
Center for Board Effectiveness  
Deloitte & Touche LLP  
[henryphillips@deloitte.com](mailto:henryphillips@deloitte.com)



**Debbie McCormack**  
**Managing Director**  
Center for Board Effectiveness  
Deloitte LLP  
[dmccormack@deloitte.com](mailto:dmccormack@deloitte.com)

For more information:

[centerforboardeffectiveness@deloitte.com](mailto:centerforboardeffectiveness@deloitte.com)







#### **About this publication**

This publication contains general information only and is not a substitute for professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser. The authors shall not be responsible for any loss sustained by any person who relies on this communication.

#### **About the Center for Board Effectiveness**

The Center for Board Effectiveness helps directors deliver value to the organizations they serve through a portfolio of high quality, innovative experiences throughout their tenure as board members. Whether an individual is aspiring to board participation or a veteran of many board experiences, the Center's programs enable them to contribute effectively and provide focus in the areas of governance and audit, strategy, risk, innovation, compensation and succession.

#### **About Deloitte**

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more about our global network of member firms.