CENTER FOR AUDIT QUALITY

Understanding Cybersecurity and the External Audit

A Resource for Audit Committees, Investors, Management, and Others[1]

U.S. public company auditors ("auditors") can play an important role regarding cybersecurity. This resource explains that role in two important contexts: the audits of financial statements and internal control over financial reporting (where applicable),[2] and disclosures.

Cybersecurity and Audits of Financial Statements and ICFR

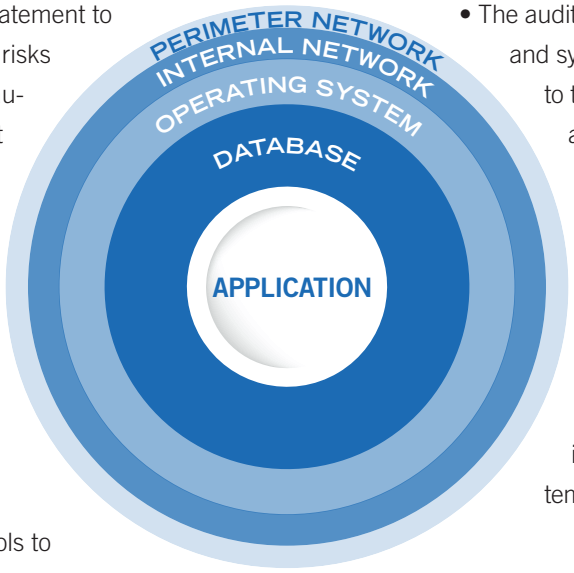
What audit procedures related to cybersecurity are performed in the audit of the financial statements and internal control over financial reporting (ICFR)?

- Auditing standards require the auditor to obtain an understanding of how the company uses information technology (IT) and the impact of IT on the financial statements.
- Auditors also are required to obtain an understanding of the extent of the company's automated controls as they relate to financial reporting, including the IT general controls that are important to the effective operation of automated controls, and the reliability of data and reports used in the audit that were produced by the company.
- In assessing the risks of material misstatement to the financial statements—including IT risks resulting from unauthorized access—auditors are required to take into account their understanding of the company's IT systems and controls.[3]
- If information about a material breach is identified, the auditor would need to consider the impact on financial reporting, including disclosures, and the impact on ICFR.
- The auditor uses a top-down approach to the audit of ICFR to select the controls to test. A top-down approach begins at the financial statement level and with the auditor's understanding of the overall risks to ICFR. The auditor then focuses on entity-level controls and works down to significant accounts and disclosures and their relevant assertions. This approach directs the auditor's attention to accounts, disclosures, and assertions that present a reasonable possibility of material misstatement to the financial statements and related disclosures.[4]

In a company's IT environment, where do public company auditors focus their attention?

- Systems and data in scope for most audits usually are a subset of the totality of systems and data used by companies to support their overall business operations, and the auditor's focus is on access and changes to systems and data that could impact the financial statements and the effectiveness of ICFR.
- A company's overall IT platform includes systems and related data that not only address financial reporting needs, but also operational and compliance needs of the entire organization.

This diagram depicts the typical access path to an IT system.



- The auditor's primary focus is on the controls and systems that are in the closest proximity to the application data of interest to the audit—that is, systems and applications that house financial statement-related data. It is important to note that cyber incidents usually first occur through the perimeter and internal network layers, which tend to be further removed from the application, database, and operating systems that are typically included in access control testing of systems that affect the financial statements.

- As audit procedures are developed to address each company's unique IT environment, the auditor should appropriately tailor the related discussion with the audit committee (in accordance with PCAOB Auditing Standard No.16) and management.

Cybersecurity and Disclosures

What procedures related to cybersecurity are performed by the auditor with respect to a company's financial statement disclosures and other information contained in the Form 10-K?

- Under current guidance, a company may determine it is necessary to disclose cybersecurity risks in various places throughout its Form 10-K (e.g., risk factors, management's discussion and analysis, legal proceedings, business description, and/or financial statements). The auditor's responsibilities depend on whether the disclosure is included in the audited financial statements or elsewhere in the Form 10-K.
- If the disclosure is in the financial statements, the auditor performs procedures to assess whether the financial statements taken as a whole, are presented fairly, in all material respects. Included in the auditor's assessment are procedures specific to the financial statement disclosures. For example, if a company had a material contingent liability for an actual cyber incident, in addition to performing audit procedures related to the reasonableness of the liability recorded, if any, the auditor would also assess whether the disclosures in the footnote related to that liability were appropriate as it relates to the financial statements taken as a whole.
- The auditor's responsibilities are different as they relate to other information, such as disclosures, presented in the company's Form 10-K outside the financial statements. The auditor should follow guidance in paragraphs 4 and 5 of the PCAOB's AU Section 550, *Other Information in Documents Containing Audited Financial Statements*.[5]

Note: This is general information related to cybersecurity and the external audit and should not be relied upon as being definitive or all inclusive. Please refer to the rules, standards, guidance, and other resources in their entirety. All entities should carefully evaluate which requirements apply to their respective organizations.

1 Please note that the content from the CAQ's *Cybersecurity and the External Audit Member Alert*, published in March 2014, has been summarized in this document for distribution to a broader audience. For additional information on the topics discussed, please see the more detailed CAQ member alert, available at http://www.thecaq.org/resources/alerts/caq-alert-2014-03---cybersecurity-and-the-external-audit.

2 According to Section 404(b) an ICFR audit "shall not apply with respect to any audit report prepared for an issuer that is neither a 'large accelerated' nor an 'accelerated' filer as defined in Rule 12b-2 of the Commission."

3 See also PCAOB Auditing Standard No. 12, *Identifying and Assessing Risks of Material Misstatement,* Appendix B, Paragraph 4 for additional IT considerations.

4 See PCAOB Auditing Standard No. 5, *An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements*.

5 To learn more about the auditor's responsibilities regarding other information for audits of fiscal years beginning on or after December 15, 2012, visit http://pcaobus.org/Standards/Auditing/Pages/AU550_04.aspx.