CENTER FOR AUDIT QUALITY
Serving Investors, Public Company Auditors & the Markets

CAQ Alert #2014-3 March 21, 2014

Dear Center Members

Cybersecurity and the External Audit

Please note that this document is intended as general information for public company auditors and should not be relied upon as being definitive or all inclusive. The CAQ encourages member firms to refer to the rules, standards, guidance, and other resources in their entirety. All entities should carefully evaluate which requirements apply to their respective organizations.

CAQ Member Alert: Cybersecurity and the External Audit

Background

Cybersecurity is an important business issue and, given the rise in high profile data breaches, it is receiving an increasing amount of attention by those in the business community. This issue has also attracted interest from Congress and certain regulatory agencies. When companies suffer security breaches and confidential customer information or proprietary business data is stolen or lost, they may face reputational damage, diminished investor confidence, lost business, and potential regulatory fines. Cybersecurity is no longer viewed as just an "IT" issue. Rather, it is being treated as a broader business issue.

On March 26, 2014, the Securities and Exchange Commission will hold a roundtable “to discuss cybersecurity and the issues and challenges it raises for market participants and public companies, and how they are addressing those concerns” (**SEC press release**). This Alert is being issued because we thought it would be helpful to summarize the responsibilities of the independent external auditor with respect to cybersecurity matters in advance of such discussions.

As discussed in detail below, the responsibility of the independent auditor relates to the audit of the financial statements and, when applicable, the audit of internal control over financial reporting (ICFR). The financial reporting-related information technology (IT) systems and data that may be in scope for the external audit usually are a subset of the aggregate systems and data used by companies to support their overall business operations and may be separately managed or controlled. Accordingly, the financial statement and ICFR audit responsibilities do not encompass an evaluation of cybersecurity risks across a company’s entire IT platform.

The financial statement audit and, where applicable, the audit of ICFR, include procedures with respect to a company’s financial reporting systems, including evaluating the risks of material misstatement to a company’s financial statements resulting from unauthorized access to such systems. The auditor is also responsible for evaluating a company’s accounting for cybersecurity-related losses and for assessing the impact on a company’s financial statements and disclosures, including items such as contingent liabilities or claims, as they relate to the audit of the financial statements taken as a whole and the impact on ICFR. Included within the auditor’s responsibilities would be evaluating the accounting for the impact of certain transactions or events such as a cybersecurity related incident, which may include losses or other associated costs. As it relates to ICFR, the auditor would be responsible for assessing the company’s controls related to timely recording and disclosing the necessary information in the financial statements.

What audit procedures related to cybersecurity are performed in the audit of the financial statements and, where applicable, ICFR?

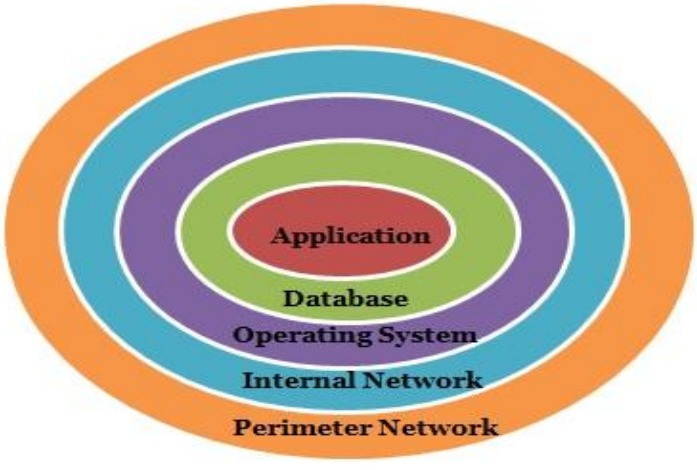
Auditing standards require the auditor to obtain an understanding of how the company uses IT and the impact of IT on the financial statements. Auditors are also required to obtain an understanding of the extent of the company's automated controls as those controls relate to financial reporting, including 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.

The auditor's understanding of the IT systems and controls should be taken into account in assessing the risks of material misstatement to the financial statements, including IT risks resulting from unauthorized access.[1]

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 audit's focus is on access and changes to systems and data that could impact the financial statements and the effectiveness of ICFR. In contrast, a company's overall IT platform includes systems (and related data) that address the operational, compliance and financial reporting needs of the entire organization.

From an operational risk or privacy perspective, companies implement processes and controls to restrict access to their systems, applications and data, including third party records and other sensitive information. Accordingly, given the focus on a narrower slice of a company's overall IT platform, the execution of an audit of the financial statements and ICFR in accordance with professional standards likely would not include areas that would address such a cybersecurity breach. However, 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 following 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, Enterprise Resource Planning (ERP) systems, single purpose applications like a fixed asset system or any set of connected systems that house financial statement related data.

On the other hand, cyber incidents usually first occur through the perimeter and internal network layers, which tend to be somewhat removed from the application, database and operating systems that are typically included in access control testing of systems that affect the financial statements. Audit procedures might include testing access controls at the application layer, and at the database and operating system layers, in that order of focus and priority. Other broader elements of security around the perimeter and network layers generally tend not to be within the scope of the financial statement and ICFR audits.

The likely sources of potential financial statement misstatement are more normally associated with transaction level access through the application. Depending on the company's business and environment, other elements of security around the internal and perimeter network layers may not pose risks to financial data, and are therefore of less importance to the achievement of audit objectives. Consequently, audit procedures performed around the internal network and perimeter network layers could vary significantly. As audit procedures are developed to address each company's IT environment, the auditor should appropriately tailor the discussion with Audit Committees (in accordance with PCAOB Auditing Standard No.16) and management.

What procedures 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, MD&A, legal proceedings, business description, and financial statements). The auditor's responsibilities depend on where the disclosure is included in the 10-K.

With regard to the auditor's responsibilities:

- 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 presented in the company's Form 10-K outside the financial statements. The auditor should follow guidance in the paragraphs 4 and 5 of the PCAOB's AU Section 550, *Other Information in Documents Containing Financial Statements* which state:

  ".**04** *[The following paragraph is effective for audits of fiscal years beginning on or after December 15, 2012. See PCAOB Release No. 2012-004. For audits of fiscal years beginning before December 15, 2012, click here.]*.

  Other information in a document may be relevant to an audit performed by an independent auditor or to the continuing propriety of his report. The auditor's responsibility with respect to information in a document does not extend beyond the financial information identified in his report, and the auditor has no obligation to perform any procedures to corroborate other information contained in a document. However, he should read the other information and consider whether such information, or the manner of its presentation, is materially inconsistent with information, or the manner of its presentation, appearing in the financial statements. If the auditor concludes that there is a material inconsistency, he should determine whether the financial statements, his report, or both require revision. If he

concludes that they do not require revision, he should request the client to revise the other information. If the other information is not revised to eliminate the material inconsistency, he should communicate the material inconsistency to the audit committee and consider other actions, such as revising his report to include an explanatory paragraph describing the material inconsistency, withholding the use of his report in the document, and withdrawing from the engagement. The action he takes will depend on the particular circumstances and the significance of the inconsistency in the other information.

.05

If, while reading the other information for the reasons set forth in paragraph .04, the auditor becomes aware of information that he believes is a material misstatement of fact that is not a material inconsistency as described in paragraph .04, he should discuss the matter with the client. In connection with this discussion, the auditor should consider that he may not have the expertise to assess the validity of the statement, that there may be no standards by which to assess its presentation, and that there may be valid differences of judgment or opinion. If the auditor concludes he has a valid basis for concern he should propose that the client consult with some other party whose advice might be useful to the client, such as the client's legal counsel."

Beyond these requirements, auditors may provide other feedback to management based on the auditor's reading of the other information, such as highlighting areas subject to recent SEC comment letters.

Other Resources

The National Institute of Standards and Technology released the first version of a ***Framework for Improving Critical Infrastructure Cybersecurity*** on February 12, 2014. The Framework, created through collaboration between industry and government, consists of standards, guidelines, and practices to promote the protection of critical infrastructure and help owners and operators of critical infrastructure to manage cybersecurity-related risk.

---

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