A CAQ COVID-19 RESOURCE

Understanding Cybersecurity and the External Audit in the COVID–19 Environment

Published July 2020

CAQ

THECAQ.ORG

WE WELCOME YOUR FEEDBACK

Please send comments or questions to info@thecaq.org

The COVID-19 pandemic and the related market conditions create many new uncertainties for auditors, audit committees, investors and management of public companies. As SEC Chair Jay Clayton recently recognized, the continuing operation of the US capital markets is an essential component of our national response to, and recovery from, COVID-19. COVID-19 continues to impact public company financial statements in different ways and at differing levels of severity depending on an entity's capitalization, geographic location and the industry in which the entity operates, among other factors. This resource is intended to provide a high-level overview of the impact of COVID – 19 on cybersecurity with respect to financial reporting, including the financial statement and internal control over financial reporting (ICFR) audits.

This resource is intended as general information and should not be relied upon as being definitive or all-inclusive, or a substitute for PCAOB and SEC rules, standards, guidance, or other resources.

CYBERSECURITY AND AUDITS OF FINANCIAL STATEMENTS AND ICFR

Auditing standards require the financial statement auditor to obtain an understanding of how the company uses information technology (IT) and the impact of IT on the financial statements. This includes 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 produced by the company and used in the financial reporting process.

In assessing the risks of material misstatement to the financial statements—including IT risks resulting from unauthorized access—financial statement auditors are required to take into account their understanding of the company's IT systems and controls.

In a company's IT environment, the systems and data in scope for most financial statement 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.

It is important to remember that 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. The financial statement 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 of the financial statements and when applicable of ICFR—that is, systems and applications that house financial statement-related data. Audit procedures are then developed to address each company's unique IT environment. Many cyber incidents 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.

In addition, if information about a material cybersecurity breach is identified, the auditor would need to consider the impact on financial reporting, including required disclosures, and the impact on ICFR.

CYBERSECURITY AND DISCLOSURE

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 audited 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 also would 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 audited financial statements. The auditor should follow guidance in paragraphs 4 and 5 of the PCAOB's Auditing Standard 2710, Other Information in Documents Containing Audited Financial Statements.

COVID – 19 CONSIDERATIONS

As companies have shifted to remote working to protect their workers while continuing to serve their customers, they have moved the majority of their activity to a virtual environment. This new way of working could expose companies to new or different cyber vulnerabilities, and many have been focused on maintaining security and business continuity.

As a result, companies may be instituting new or making changes to existing cybersecurity related processes and controls. From a remote access perspective, the changes could include additional servers, new or incremental virtual private network controls and instituting multi factor authentication. In addition, companies may need new controls related to new technology tools, applications or devices employees may be using in the work from home environment.

Companies also may be responding to the impact of circumstances such as restructurings, furloughed employees and contractor changes by assessing whether access administration controls are appropriately designed and operating effectively to respond to the risks of these new or different scenarios.

The SEC's Office of Compliance, Inspections and Examinations recently issued an Alert in response to an apparent increase in the sophistication of ransomware attacks on SEC registrants and also ransomware attacks impacting service providers to registrants. These attacks may use COVID-19 as "bait" to impersonate brands and mislead customers or employees. With the threat and volume of attacks increasing, companies may be considering what additional network perimeter security might be necessary to improve their defense. Given the new threat level, companies also may be evaluating their incident response plan to determine whether it appropriately accounts for these changing circumstances, and that resources are appropriately positioned to detect and respond to threats.

As companies evolve to respond to these new or increasing cyber-related risks, auditors will need to update their understanding of the IT environment accordingly, and revise risk assessments and audit procedures to be responsive to any new or different risks of material misstatement that could impact the financial statements and/or ICFR.