

COVID-19 AND YOUR SOX COMPLIANCE PROGRAM

Practical Considerations While Navigating the Crisis

Issue 4

SOC Reports: Anticipating Challenges Can Help Minimize Disruption of SOX Compliance Programs

Many organizations outsource business processes and obtain SSAE 18 Service Organization Control (SOC) 1 reports. Due to the COVID-19 pandemic, some of these SOC-1 reports may either be delayed in their issuance, as external auditors navigate the new remote working environment, or contain adverse opinions due to changes in controls at the service providers as a result of COVID-19. Additionally, access to service organizations to obtain additional support for controls execution may be more challenging than normal. In anticipation of these hiccups, we've compiled a list of practical steps that companies can take to get ahead of this brewing issue.

- 1) **Compile an inventory of third-party service providers** – It is important that each organization has a complete list of third-party providers it is relying upon from a financial reporting perspective. The information on each provider should include but not be limited to: vendor name, SOC report scope period, bridge letter requirement and subservice providers. SSAE 18 requires organizations to also evaluate subservice providers that play a role in the overall operations of the service provider (and the controls they may have an impact on or have complete ownership of), so it is critical to include them in the organization's listing. For service providers that do not have a SOC report, note that, in the listing and document management's controls for verifying, that data is complete and accurate. Cross-check the list with your external auditor. While compiling the inventory of service providers, touch base with the organization's users of these services to ascertain if there are any changes being made to the services or procedures of the service providers.
- 2) **Proactively reach out to third-party service providers to assess availability of SOC-1 reports and potential delays in their issuance** – We recommend reaching out to third-party service providers as soon as possible to understand when the SOC-1 reports will be available. This will help ascertain whether or not there are business disruptions that may impact the availability of SOC-1 reports and bridge letters and prompt your organization to assess alternatives if the SOC-1 reports will not be available prior to your SEC filing date.
- 3) **Assess control changes at service providers** – The pandemic may result in changes in the controls at service providers. Be sure to ask service providers to identify any changes in their controls as a result of user access changes or work-from-home access, any alternative controls deployed and whether or not any new control deficiencies have been identified due to the unusual circumstances.
- 4) **For delayed reports, assess the need to explore alternatives** – If a SOC-1 report will not be available on a timely basis, we highly recommend your organization start assessing alternative methods to gain reasonable assurance that the controls at service providers are operating as intended and can be relied upon by the organization.
 - a. **Ask the third-party provider if it can issue two SOC-1 reports covering a rolling period, accompanied by a bridge letter** – We are seeing that many service providers are migrating to a six-month cadence for issuing SOC-1 reports. This is increasingly viewed as a gold-standard practice because it avoids a situation where a SOC report is received after the SEC filing date. Asking service providers to consider this increased cadence will ensure your company has at least partial coverage of its 12-month reporting period.
 - b. **For new service providers, ask for the prior year's SOC report to baseline controls** – In cases where the organization has a new service provider added to the inventory for this year's Sarbanes-Oxley (SOX) assessment, leveraging the prior year's SOC report will provide insights into the typical coverage that

management can expect from this service provider's next SOC report. This analysis of last year's controls and testing can aid in assessing what alternative procedures may be required this year for this service provider.

- c. **Consider implementing additional monitoring controls to validate data provided to and received from the third-party service providers** – Look at what your organization can do with the information it sends and receives from its service providers. Sometimes management's implementation of additional controls can meet the needs of the company's SOX program.
- d. **Perform a third-party audit of the service providers' controls** – In some cases, there is no SOC report, or the time period of the SOC report is incompatible with your organization's needs. In those instances, management needs to do 'on site' reviews of internal controls at the service organization. The SSAE 18 SOC reports were meant to limit this concurrent auditing of service organizations by their multitude of clients, and many service organizations have implemented SOC audits and more frequent six-month rolling audits to meet the ongoing requests and demands from their customers. But if an organization finds itself in a situation where a SOC report is unavailable or inadequate for its needs, it will need to identify the scope of the audit that it needs to perform, including the controls, time period and how the audit will occur in a remote work environment. Check the contract for "right to audit" provisions as you navigate the path forward.

During these unprecedented and extraordinary times, early evaluations and proactive communication with third-party service providers will be key to ensuring that organizations can get adequate coverage of their service organizations to support management's attestation as part of the SOX compliance program.