SOC Reporting and COVID 19

Brief Overview

COVID-19, the most buzzed word these days, a virus that has not only impacted health of the humans but has also affected almost each and every industry in the world including organizations (*user organization*) relying on other companies (*service organization*) to provide their services. Companies have either shifted their staff to remote environments or laid off their workers. Organizations looking for a SOC (System and Organization Controls) report from their service organizations are in a dilemma whether they will be able to get a renewed report or not for the COVID year.

SOC examinations are designed to test the information technology and business process control systems that a company has implemented to protect the security of its customer's data (SOC 2), or ensure the accuracy and completeness of financial transaction processing and reporting (SOC 1). If your customers and the related stakeholders do not perform SOC reports on a timely basis, it could influence their business objectives.

Further, the entities who issue SOC reports (i.e. independent third party audit firms) , are anxious on how to support the remote attestation of controls during this time where companies have a reduced headcount, decreased revenues, ceased operations due to government / mandatory requirements to continue operations. Remote assessment of risks and attestation either of internal controls over financial reporting (SOC 1) or AICPA's trust service criteria (SOC2) without being physically present at the client location has become a big challenge. However, the business must go on so should the SOC reporting.

In this article, we will be touching upon the considerations that should be taken care by service & user organizations as well the third party auditors during the pandemic scenario.

Service Organizations

Service organizations should evaluate their Operations and IT environments to determine if any controls have been impacted.

- The company should examine any impact on functioning of controls caused by reduced number of employees and any SoD (segregation of duties) conflicts should be addressed using additional monitoring controls
- The company employees accessing the regulated data should receive appropriate trainings on handling that data in a remote work environment.
- The new user provisioning / user termination processes should operate effectively with sufficient authentication of remote users.
- Supplementary guidance on remote work cyber security practices should be communicated to staff working from a remote location.
- Security of applications enabled for remote work should be taken care along with the implementation of multi-factor authentication (MFA) which should be required for all critical systems.
- Service organizations should discuss the procedures around video conferencing to perform virtual walkthroughs with their service auditors. Most common procedures include physical security walkthroughs of buildings and data centers that ensure security measures and environmental protections are in place.

User Organizations

They as a receiver of the SOC 1 and/or SOC 2 reports, should have frequent communications with their vendors to discuss whether COVID-19 has impacted their operations and their SOC report. Following things should be considered as one reviews the SOC reports where evaluation period includes the timing of the pandemic.

- The SOC report should be reviewed for any disclosures on changes to the system, operations or controls due to the impact of COVID-19. An assessment should be done to identify if any change impacts you and your reliance on the SOC report.
- The SOC report should also be reviewed for any exceptions and you can expect to have increased number of exceptions within your service organizations due to the pandemic. These exceptions and their corresponding impacts should also be evaluated.
- The complementary user entity considerations should be reviewed. Analysis should be done if the service provider has included any additional items due to any changes in the controls or system description.

Assessors / Auditors

Following key aspects should be considered by the auditor while performing a third party assessment remotely.

- Risk associated with key personnel should be evaluated and the organization should have adequate personnel available to support critical business and IT functions.
- Changes related to the organizational structure should be assessed and their possible impact on segregation of duties should be analyzed.
- Organization's Disaster Recovery and Business Continuity Plans should be evaluated and appropriate changes should be suggested as required in a pandemic situation.
- Keeping in consideration the travel restrictions, Distance Audit methods such as video conferencing should be used to perform virtual walkthroughs like physical security walkthroughs of buildings and data centers to ensure security measures and environmental protection methods are adopted.
- Video conferencing can also be used to communicate with client personnel and gain an understanding of client's systems for a new engagement, or test the effectiveness of controls for on-going engagements.
- For the controls not operating during the testing period due to pandemic situation, auditors should simply add an additional rationale in the report explaining the reason. However, the overall report opinion is not modified.
- The critical functions such as review of risk assessments, reviewing policies, periodic user access reviews, or ticketing for timely removal of terminated user access should continue to operate uninterruptedly and should be tested as usual. For exceptional cases, an annual control can be rescheduled to occur in future months, as long as it is still within your SOC examination period. In other instances, those activities may can be performed virtually.

You can also visit below link to read AICPA articles related impact of COVID 19 on audit and assurance.

https://future.aicpa.org/topic/audit-assurance/covid-19-audit-assurance

Please reach out to us in case you would like to discuss more on this topic or if you have any queries related to SOC reporting.