No. 2020-10
21 May 2020

Technical Line

How SOC reporting may be affected by the COVID-19 pandemic

In this issue:

What you need to know

- Service organizations that provide System and Organization Controls (SOC) reports to the companies they do business with need to consider how the COVID-19 pandemic will affect this reporting.
- Many service organizations have made significant changes to their systems and controls due to stay-at-home orders and other restrictions instituted worldwide.
- Management of a service organization should update the organization's risk assessment and consider modifying management's description and management's assertion in any SOC reports.
- Management needs to understand the concerns of user entities that rely on the service organization's SOC reports and communicate with them about any significant deficiencies that relate to the suitability of the design of controls or the operating effectiveness of controls and changes to the timing of a report.

Overview

Management of service organizations that provide SOC 1® or SOC 2® reports to the companies they do business with needs to consider the implications of the COVID-19 pandemic on this reporting.

That is, management needs to consider whether the service organization's system and controls changed due to stay-at-home orders and other restrictions instituted worldwide. Management also needs to consider whether it needs to update its risk assessment and/or make changes to its description of the system and its assertion about the design of the organization's controls and their operating effectiveness.

Effect on a system and controls

The following types of changes to a service organization's operations, processes and workforce should be considered to determine the effect on the organization's system and controls:

- Implementing a work-from-home policy
- Restricting access to facilities
- Reassigning responsibilities between employees and locations
- Reducing the size of the workforce
- Increasing the load on internet infrastructure such as virtual private network systems and firewalls
- Delaying the implementation of additional processing capacity
- Delaying the implementation of system changes
- Delaying subservice organization and vendor risk and controls assessments

These changes, along with any changes in the availability of key employees, should be considered in evaluating whether controls that operated before the pandemic continue to operate at an appropriate level. If a control cannot be performed as previously designed, management needs to make sure any changes in design address the both original risks and any new or modified risks.

Changes to controls may include:

- Changes in the precision of a control (e.g., using higher tolerances)
- Changes in the evidence that supports the performance of a control (e.g., managers who formerly documented the performance of a review control on paper may now be documenting it electronically)
- Suspension of a control (e.g., canceling planned penetration testing or disaster recovery testing)
- Implementation of new controls and software

If these changes are material, management should revise its description of its system or identify and implement new controls necessary to achieve the service organization's control objectives.

If processes or controls are modified, it is critical that the service organization's evaluation of the suitability of the design of controls and their operating effectiveness appropriately address:

- Changes to the system during the pandemic
- Changes to controls during the pandemic, including additions or deletions of controls
- Nature (e.g., scope) of the evaluation of the controls
- Timing of the evaluation

Effect on the risk assessment

Updating a service organization's risk assessment is critical to assessing the effectiveness of existing controls and identifying the need for new controls in response to changing threats or vulnerabilities. To update a risk assessment, management should start with the risks and controls the service organization identified before the COVID-19 pandemic and consider whether:

- Controls as designed are less effective due to:
  - New threats to the functioning of the system or an increase in the likelihood of an existing threat occurring before normal operations resume (e.g., attackers will increasingly target online payments)
  - Vulnerabilities in the system as a result of changes in how the system is used (e.g., the capacity limits in the design of the two-factor authentication system do not support the greater use of remote access, resulting in security failures in authentication)
  - Elevated risk of fraud or noncompliance with laws or regulations
- Controls are suspended or are temporarily replaced with substitute controls that are less effective during the response period.
- Controls fail to operate effectively during the period before normal operations resume due to:
  - Insufficient facilities and infrastructure (e.g., limits on the number of permitted participants in a secure web meeting tool results in not all members of a change advisory board being able to participate in meetings.)
  - Execution of controls in an environment that is not conducive to the performance of the control
  - Inability to document that controls operate effectively (e.g., a manager may be able to review a reconciliation package from a remote location, but the manager may not be able to sign the top sheet of the package to evidence the review)
- The unique circumstances caused by the pandemic reveal deficiencies in the design of controls, particularly those related to availability in a SOC 2 report. For example, management may discover that a second data center that is designed to take over when a failover occurs does not have remote access capabilities sufficient to meet the service organization's commitments.
- The planned implementation of new controls is delayed, resulting in the failure of controls to be suitably designed.

Updating a service organization's risk assessment is critical to assessing the effectiveness of existing controls and identifying the need for new controls.

Effect on management's description of the system

As a service organization makes changes to its system and controls, management needs to consider the effect of these changes on management's description in the report and how these changes will be disclosed.

The report may need to reflect changes to services provided, locations, applications, and how processes and controls are performed. The overview of the service organization may need to be updated to reflect changes to services, organizational structure, customers, headcount and locations. Management will also need to address the effect on the service organization's internal control, including relevant aspects of the control environment, the risk assessment process and monitoring activities, and any significant changes to the design and operation of controls.

Management may also want to consider additional disclosures related to the COVID-19 pandemic, including significant incidents in which control objectives were not achieved for a SOC 1 report, or service commitments and system requirements were not achieved for a SOC 2 report.

Effect on management's evaluation of the operating effectiveness of controls

In a SOC engagement, management is responsible for having a basis for its assertion that controls are suitably designed and operating effectively. If processes or controls are modified as a result of the pandemic, management of a service organization needs to consider whether it should perform additional procedures to have a basis for its assertion as a result of:

- Changes to the system during the period
- Changes to controls during the period, including additions or deletions of controls
- Procedures management planned to perform as part of its basis could not be performed
- Procedures that management performed as part of its basis were performed before the pandemic

Effect on management's assertion

Management may need to extend or modify the reporting period to provide users of the report with the information they need about changes to a service organization's system and controls. A service organization also may delay issuing a report if it is still making changes to its systems or controls.

Management also may need to modify its assertion to address changes to controls and control deficiencies. For example, it may be impossible for some controls to be performed due to access restrictions. In these situations, it would be beneficial to disclose the circumstances that prevented the control from being performed.

It is imperative that management understand the concerns of user entities that rely on SOC reports and communicate with them about any significant deficiencies that relate to the design of controls, the operating effectiveness of controls and any changes to the timing of a report.