No. 2022-13
2 November 2022

To the Point

AICPA revises guidance on applying its Trust Services Criteria and SOC 2 Description Criteria

Service organizations may need to make changes to their controls and their disclosures in SOC 2 reports to comply with the new guidance.

What you need to know

- The AICPA revised its Trust Services Criteria and SOC 2 Description Criteria documents to provide guidance on considering technological threats and vulnerabilities, confidentiality and privacy issues, and disclosures service organizations make in SOC 2 reports.
- The changes are intended to help service organizations better meet the information needs of their customers and business partners who use their SOC 2 reports.
- While the AICPA didn't change its Trust Services Criteria and SOC 2 Description Criteria, it updated the points of focus associated with the Trust Services Criteria and its implementation guidance on the Description Criteria.
- Service organizations are encouraged to consider whether changes are needed in their controls and their SOC 2 reports.
- The AICPA also updated the SOC 2 guide, which is used by service auditors to perform SOC 2 engagements and by service organizations to prepare their disclosures for the reports.

Overview

The Assurance Services Executive Committee of the American Institute of Certified Public Accountants (AICPA) revised its guidance relating to both the **criteria management of service organizations used to describe the system providing the services in Service Organization Control (SOC) 2 reports** and **the criteria management and service auditors used to evaluate the controls** over the system.

Building a better working world

The new guidance is aimed at enhancing the usefulness of SOC 2 reports and helping management and service auditors evaluate whether a service organization's controls are suitably designed and operating effectively. Service organizations may need to make changes in their controls and their disclosures in their SOC 2 reports as a result of the guidance.

SOC 2 reports are intended to provide customers and business partners of service organizations with information to help them evaluate whether the organization's internal control over its system for providing the service appropriately addresses the risks to the achievement of its service commitments and system requirements. The AICPA issued the Trust Service Criteria[1] (TSC) in their current form in 2017 and the Description Criteria[2] in their current form in 2018.

Key considerations

Revisions to the Trust Services Criteria guidance

While the AICPA didn't change the criteria in the TSC, it added new points of focus and clarified existing points of focus that address the evaluation of whether controls are suitably designed and operating effectively to achieve the entity's service commitments and system requirements.

The AICPA said the revised points of focus are intended "to better support application of the criteria" in an environment of ever-changing threats and vulnerabilities; new technologies; legal, regulatory and cultural expectations regarding privacy; and changing expectations regarding data management and confidentiality. The revisions also provide guidance on topics that entities have struggled with, such as which privacy points of focus apply to data controllers and which ones apply to data processors.

Service organizations should consider whether and how their controls address the clarifications and new points of focus. In evaluating the new guidance, organizations should pay particular attention to the following changes:

- Types of relevant information — New points of focus clarify that the types of information relevant to systems of internal control include information about data flow, asset inventory and location, information classification, and the completeness and accuracy of information used in the system.
- Risk assessment — The revised points of focus on risk assessment provide users with a more granular approach to evaluating risks by understanding the underlying components of risk assessment: threat and vulnerability identification and the evaluation of the likelihood and magnitude of a threat event intersecting with a vulnerability. The revised points of focus also include the consideration of residual risk after considering internal controls and management's decisions to accept, reduce or share risks.
- Monitoring activities — The revised points of focus encourage service organizations to consider activities performed by the first and second lines of defense (i.e., monitoring performed by the people who perform a function and monitoring performed by managers who oversee them, respectively) in addition to internal audit functions and other recurring information technology (IT) assessments many service organizations have historically identified in their SOC 2 reports.
- Logical access — Modified points of focus encourage consideration of logical access controls across the system architecture, including all relevant infrastructure, IT tools, and types of access, such as employee, contractor, vendor, business partner, system and service accounts. In addition, recovery of devices, such as laptops, is now considered in the points of focus.

- Change management — Two new points of focus have been added to address change management. The first relates to the identification, testing and implementation of software patches. The second addresses the consideration of resilience requirements during the change management process if a SOC 2 report addresses system availability.
- Availability — Given the increase in ransomware attacks, a new point of focus was added on management's identification of threats to data recoverability and mitigation procedures.
- Privacy — A number of points of focus were revised to better align with widely used privacy practices.

The AICPA also emphasized that the applicability of any particular point of focus depends on the facts and circumstances and that the points of focus provided are unlikely to be exhaustive for most service organizations. Consequently, use of the TSC does not require that every point of focus be met. However, a service organization should consider the applicability of the new points of focus and whether other points of focus also need to be met to achieve their service commitments and system requirements.

Revisions to the Description Criteria guidance

The new guidance emphasizes the importance of providing sufficient detail in disclosures about principal service commitments and system requirements.

The AICPA said the revised Description Criteria guidance is intended to clarify certain disclosure requirements, provide guidance on how controls meet the requirements of a process or control framework and provide guidance on disclosure of information about the risk assessment process and specific risks.

In evaluating the effect of these changes, organizations will want to pay particular attention to the following:

- The revised guidance emphasizes the importance of providing sufficient detail in disclosures about principal service commitments and system requirements. The guidance emphasizes that the disclosure is intended to give the user a reasonable understanding of key aspects of the reporting, including the scope, IT environment and related controls in place to support the achievement of the service commitments and system requirements as set forth by the service organization. The guidance indicates that the practice of referring to descriptions published elsewhere is often insufficient.
- The revised guidance addresses when disclosure of information on process and control frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, is appropriate in a SOC 2 report, given that service organizations are increasingly adopting such frameworks and making service commitments regarding their adoption.

How we see it

Service organizations should work with their service auditors to understand the implications of the new guidance and any improvements they may need to make in their controls and disclosures in SOC 2 reports.

We encourage service organizations to review their principal service commitment and system requirement disclosures and challenge the sufficiency of those disclosures. We also encourage service organizations to review the process and control frameworks they have adopted, whether those frameworks could be considered service commitments or system requirements and consider whether disclosure of those frameworks in their system description is required.

Service organizations should also regularly challenge the thoroughness and effectiveness of their risk assessment and management processes.

SOC 2 guide revisions

The AICPA also revised its SOC 2 guide that provides service auditors with guidance on the performance of a SOC 2 engagement and is often used by service organizations to help them prepare disclosures included in the reports.

Endnotes:

1 TSP Section 100 *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022)*.

2 DC Section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance – 2022)*.