Exploring SOC 2® 2023 Revisions: What's Fresh in the Latest Version

The realm of compliance is perpetually evolving, as are the regulations that govern it. SOC 2®, a well-recognized framework for assessing controls within service organizations, has recently undergone some revisions. In this article, we'll delve into the most recent iteration of SOC 2® and examine the significant alterations to what are referred to as "points of focus," (PoFs). These changes have been designed to bolster the effectiveness and pertinence of SOC 2® audits. Whether you're a service provider or an auditor, comprehending these revisions is essential to uphold compliance and trust.

In the expanding digital landscape, where data breaches and cybersecurity threats loom large, SOC 2® offers assurance to customers, partners, and stakeholders that your organization has taken requisite measures to protect their data. It has become a mandatory requirement for many service providers, encompassing data centers, cloud service providers, and SaaS companies.

The Latest SOC 2® Version: So What's Different?

The AICPA has introduced some important updates and modifications to the PoFs within the TSC, and although not major, important to take in consideration:

- Enhanced clarity on the risk assessment process.
- Explicit delineation of specific risks to consider.
- Introduction of new attestation standards.
- Greater precision regarding certain disclosure requisites.

Lawrence J. Beardsley CPA, PLLC

email info@ljbcpa.com
office 817.469.6800
web ljbcpa.com

Locations (we serve nationwide from our offices)

1301 S. Bowen Road
Suite 435
Arlington TX 76013

12222 Merit Drive
Suite 1700
Dallas, TX 75251

14800 Quorum Drive
Suite 370
Dallas TX 75254

The SOC 2® revision offers clarity on:

Novel points of focus and clarification of existing points of focus to better support the TSCs.

Guidance on how auditors should proceed when a service organization presents controls related to a framework outside the SOC 2® trust services criteria.

Distinctions between the "Confidentiality" and "Privacy" categories and when it's appropriate for a service organization to report on their respective controls.

Enhancement of controls that underpin the implementation of all five TSCs to address the evolving landscape of threat management.

Differentiation of privacy points of focus based on being a "data controller" or a "data processor."

Clarifications on disparities between the Confidentiality and Privacy TSCs and when to report on their controls.

Guidance on how management and a service auditor should account for controls that may have operated beyond the specified period and how to assess the relevance of controls that operated prior to the specified period.

Guidance on incorporating new changes to CPA attestation standards.

Clarity on objectives for service organizations and their relation to service commitments and system requirements.

Categorization of sub-service organizations versus vendors and the appropriate types of controls or disclosures related to the use of specialists by management.

Identification of software and tools used for detecting threats and vulnerabilities, such as firewalls, intrusion prevention, and detection systems.

Addressing data storage, backup, and retention concerning confidentiality.

Lawrence J. Beardsley CPA, PLLC

email info@ljbcpa.com
office 817.469.6800
web ljbcpa.com

Locations (we serve nationwide from our offices)

1301 S. Bowen Road
Suite 435
Arlington TX 76013

12222 Merit Drive
Suite 1700
Dallas, TX 75251

14800 Quorum Drive
Suite 370
Dallas TX 75254

The Net Effect

The overall impact of these revisions is minimal. If your organization has already identified and mitigated primary risks, many of the controls affected are likely in place. The new points of focus will only necessitate new or revised controls if you and your auditor determine that your existing controls do not adequately address the criteria. Organizations operating under the previous SOC 2® version are not mandated to update to this new iteration, as per the AICPA:

"The changes to the points of focus in the 2022 revisions do not, in any way, alter the criteria in the 2017 TSC. Such criteria continue to be suitable criteria for use when evaluating controls in any trust services engagement."

These updates to PoFs offer additional clarity for each TSC and align them with emerging technologies, threats, vulnerabilities, and mitigation strategies. For those curious about the specific revisions made by the AICPA, we've summarized the highlights and most notable changes below.

Information and Communication

The revisions furnish additional guidance on managing and identifying threats to data recovery, creating more effective mitigation strategies, and aligning with other privacy best practices, such as those outlined in the COSO framework. Key specifics include:

CC2.1: Management, classification, completeness, and accuracy (C&A), and asset storage.

CC2.2: Communication aspects regarding privacy knowledge, awareness, and incident reporting (*applicable when Privacy TSC is in scope).

CC2.3: Communication concerning privacy-related incidents (*applicable when Privacy TSC is in scope).

Lawrence J. Beardsley CPA, PLLC

email info@ljbcpa.com
office 817.469.6800
web ljbcpa.com

Locations (we serve nationwide from our offices)

1301 S. Bowen Road
Suite 435
Arlington TX 76013

12222 Merit Drive
Suite 1700
Dallas, TX 75251

14800 Quorum Drive
Suite 370
Dallas TX 75254

Control Environments

The revisions provide enhanced clarity on information pertinent to internal control systems, encompassing:

- Asset inventory and location.
- Information classification.
- Clarity on data flow.
- C&A of information used within a system.

The most significant change in this revision:

CC1.3 and CC1.5: These two items address newly identified privacy concerns related to reporting lines and disciplinary actions.

Risk Assessments

The revisions in the Risk Assessments PoFs outline a more detailed approach to evaluating risks, defining risk assessment components as:

Identifying threats and vulnerabilities.

Evaluating the likelihood and impact of threats converging with vulnerabilities.

The most notable changes in this revision:

- CC3.2: Identification of vulnerabilities in system components and additional guidance on risk significance assessment for sub-service organizations.
- CC3.4: Assessment of changes in internal and external threats and vulnerabilities an organization may face.

Lawrence J. Beardsley CPA, PLLC

email info@ljbcpa.com
office 817.469.6800
web ljbcpa.com

Locations (we serve nationwide from our offices)

1301 S. Bowen Road
Suite 435
Arlington TX 76013

12222 Merit Drive
Suite 1700
Dallas, TX 75251

14800 Quorum Drive
Suite 370
Dallas TX 75254

Logical and Physical Access

Updated points of focus for logical and physical access encourage participants to assess all logical access controls throughout an organization, including:

- Infrastructure.
- Logical and Physical access (employee, contractor, vendor, or partner).
- Device recovery (laptops, work phones).
- IT tools.
- System and service accounts.
- Notable changes in this revision:

CC6.1: Addressing access and use of confidential information for specified purposes when Confidential TSC is in scope.

CC6.4: Addressing the recovery of physical devices.

System Operations and Monitoring

Revisions in system operations and monitoring encourage participants to consider activities performed by the first and second lines of defense, in addition to internal audit functions and other IT assessments traditionally identified in SOC 2® reports. Notable changes include:

CC7.3: Addressing the impact, use, or disclosure of confidential information in the event of a security incident when Confidential TSC is in scope.

CC7.4: Addressing the definition and execution of breach response procedures when the Privacy TSC is in scope.

Change Management

The revisions now include the identification, testing, and implementation of software patches and resilience requirements in the Change Management TSC, providing clarity. The most notable update:

Lawrence J. Beardsley CPA, PLLC

email info@ljbcpa.com
office 817.469.6800
web ljbcpa.com

Locations (we serve nationwide from our offices)

1301 S. Bowen Road
Suite 435
Arlington TX 76013

12222 Merit Drive
Suite 1700
Dallas, TX 75251

14800 Quorum Drive
Suite 370
Dallas TX 75254

CC8.1: Addresses the process of managing patch changes, the design, and testing phases for system resilience when the Availability TSC is in scope and privacy requirements in the design phase when the Privacy TSC is in scope.

Risk Mitigation

Updated points of focus for risk mitigation offer guidance on residual risks that persist after implementing internal controls, and when management evaluates whether to accept, reduce, or share risks. The most significant change in this revision:

CC9.2: Addresses the identification and evaluation of vendor risks and vulnerabilities stemming from business partnerships.

Regarding the changes outlined above, these updates in guidance are applicable to organizations and auditors alike. For many organizations, the impact of these changes on audit engagements is expected to be relatively minor. Some organizations may be requested to customize their existing controls to encompass these alterations or provide updated evidence. In other instances, auditors might determine the necessity for new controls to address the fresh points of focus.

It's important to note that organizations currently operating under the prior SOC 2® version are not obligated to transition to the new edition. However, for those interested in adopting the latest SOC 2® version, the new and revised points of focus have been seamlessly integrated into the existing requirements. These updated requirements can be readily accessed by those who wish to migrate to the newest SOC 2® version.

You may be wondering whether these changes affect your existing controls. The good news is that they do not. All the existing functionalities and features of SOC 2® remain intact, including Trust Service Criteria. There have been no material alterations to these functionalities, ensuring a smooth transition for those considering an update to the latest SOC 2® version.

Lawrence J. Beardsley CPA, PLLC

email info@ljbcpa.com
office 817.469.6800
web ljbcpa.com

Locations (we serve nationwide from our offices)

1301 S. Bowen Road
Suite 435
Arlington TX 76013

12222 Merit Drive
Suite 1700
Dallas, TX 75251

14800 Quorum Drive
Suite 370
Dallas TX 75254

About the firm

We proudly stand as your dedicated advocate. At LJB CPA, our unwavering commitment is driven by a profound sense of purpose and our guiding principles. We firmly reside at the crossroads of competency, purpose, value, and service, and we adhere to a set of foundational values that underpin our approach to serving all our stakeholders.

Our Values

Our firm consistently delivers exceptional service to our clients by upholding three core principles: Quality, Reliability, and Service. These principles are the bedrock of our operations and are non-negotiable.

With multiple offices at our disposal, we operate as a comprehensive accounting firm equipped to address all your accounting needs. Our structure is designed to cater to businesses seeking high-quality resources delivered in a collaborative team-oriented fashion. Our mission is to provide clients with the utmost level of service and value by prioritizing what is essential to them and their stakeholders. Whether you are a startup in need of foundational support, or an established firm looking to navigate compliance requirements and advance to the next level, we are here to assist you every step of the way.

Lawrence J. Beardsley CPA, PLLC

email info@ljbcpa.com
office 817.469.6800
web ljbcpa.com

Locations (we serve nationwide from our offices)

1301 S. Bowen Road
Suite 435
Arlington TX 76013

12222 Merit Drive
Suite 1700
Dallas, TX 75251

14800 Quorum Drive
Suite 370
Dallas TX 75254