SOC 2: System and Organization Controls Reporting

Technology and processes can be outsourced; risks and accountability cannot

Entities often leverage business relationships with other companies to achieve their organization's goals. Modern cloud computing and telecommunications systems have significantly enhanced the economic benefits derived from outsourcing tasks or entire functions to another organization (service organization). **While these relationships can boost revenues, expand market opportunities, and reduce costs for organizations (user entities), they also introduce additional risks from interactions with the service organization and its system.**

These risks specifically relate to the security, availability, confidentiality, processing integrity and privacy of customer data. Therefore, the management of these user entities must identify, evaluate, and address these risks as part of their risk assessment. Even though management can delegate specific tasks or functions to a service organization, they remain accountable for these tasks to boards of directors, shareholders, regulators, customers, and other stakeholders. Consequently, management is responsible for establishing effective internal controls over interactions with the service organizations and their systems.

To manage risks associated with a service organization, user entities often need information about the system's controls. They may request a report, which examines if: (a) the system's description is accurate, (b) the controls are designed to meet service commitments and system requirements, and (c) in a type 2 examination, the controls operated effectively to help ensure service commitments and system requirements associated with security, availability, processing integrity, confidentiality, or privacy of the system are met. This is known as a SOC 2® examination.

SOC 1 and SOC 2 reports are similar yet distinct:

- SOC 1® reports are designed to report on controls that address risks associated with internal controls over financial reporting.
- SOC 2® reports are designed to report on controls that address risks associated with security, availability, processing integrity, confidentiality, and privacy.

This whitepaper focuses on SOC 2 reports.

A SOC 2® report details the controls management has implemented to meet trust services criteria based on its service commitments and system requirements. The examination identifies where these control processes are in place, highlights any deviations from their intended design and implementation, and assesses their consistent operation over time. SOC 2® reports provide comprehensive information about the controls and their effectiveness in managing risks.

[Source: AICPA SOC 2® - SOC for Service Organizations: Trust Services Criteria Guide]

According to Zain Shabbir, a SOC Assurance Leader at KPMG LLP, service organizations are rapidly looking to get to market with their service offerings. This urgency often leads to challenges in aligning their risk assessments with the commitments they are providing to their customers. As a result, many service organizations struggle to adequately implement controls to address these risks.

In the rush to deliver innovative solutions and gain a competitive edge, service organizations may overlook critical aspects of risk management. This can lead to gaps in their control environments, making them vulnerable to potential security breaches and compliance issues. Effective risk assessments are essential to identify and mitigate these risks, ensuring that the service organization's commitments to security, availability, processing integrity, confidentiality, and privacy, as applicable are met.

Moreover, the dynamic nature of the technology landscape means that new risks are constantly emerging. Service organizations must continuously update their risk assessments and control frameworks to address these evolving threats. This requires a proactive approach to risk management, involving regular reviews and updates to their control processes.

By aligning their risk assessments with their service commitments, service organizations can build trust with their customers and stakeholders. This not only helps in meeting regulatory requirements but also enhances the overall security posture of the organization. Implementing robust controls and maintaining transparency through SOC 2® reports can provide assurance to customers that their data is being handled securely and responsibly.

Management Responsibilities in a SOC 2® Examination

Before engaging a service auditor for a SOC 2® examination, service organization management must make several key decisions that impact the examination's scope, timing, and procedures, including:

- Identifying the services provided to user entities, the system used, and the risks from business partners
- Selecting the trust services categories
- Determining the type of SOC 2® examination (type 1 or type 2).
- Establishing the examination period
- Evaluating the impact of services provided by other entities and deciding whether to include them as subservice organizations

Management is responsible for:

- Specifying the principal service commitments and system requirements
- Identifying and analyzing risks
- Designing, implementing, and monitoring controls that are suitably designed and, in a type 2 examination, operate effectively to ensure the service organization's commitments and system requirements are met.

To enhance the usefulness of the SOC 2® report, management may discuss these matters with intended users before engaging the service auditor.

When planning for a SOC 2® report, service organizations should:

- Establish a list of primary services or systems to be evaluated and define specific trust services criteria (TSCs) based on client commitments.
- Gather documents demonstrating their ability to provide security, availability, processing integrity, confidentiality, and privacy
- Schedule in-depth risk assessments and summarize findings
- Survey senior executives about risks to be addressed in the SOC 2® report
- Establish an incident response plan detailing how security incidents and breaches will be handled and reported
- Create a system for data classification and management, ensuring data confidentiality and integrity
- Document processes for controlling and monitoring access to systems and data, including monitoring and logging activities
- Deploy training programs to enhance staff awareness of security policies
- Communicate security policies and updates to stakeholders through a documented plan
- Perform a readiness assessment and consider a type 1 report for the first instance of the report

[Source: AICPA & CIMA - Information for Management of a Service Organization in a SOC 2® Engagement]

Timing and Phases of a SOC2® Report

Understanding the timeline and phases involved in completing a SOC 2® report is crucial for effective planning and execution. According to Samantha Brady, a SOC Assurance Leader at KPMG LLP, companies often underestimate the amount of time it takes to prepare for and execute an effective SOC 2 program. It is important for management to define the scope of the report, their commitments and requirements and engage with an external audit firm early in the process. Organizations with starting their SOC 2® journey often begin with a readiness assessment or a Type 1 report before moving to a Type 2 report, which evaluates the effectiveness of controls over a period of time. While some engagements may be completed in as little as twelve (12) weeks with strong coordination and preparation, timelines can vary significantly depending on the complexity of the environment, scope, and readiness of the organization. Reports are typically targeted to be issued 30–45 days after the period end date.

Next Steps to Strengthen Your Security Posture

In today's dynamic landscape, ensuring data security and privacy is paramount. Working with a professional services firm for your SOC 2® examination can help provide a thorough assessment of your control environment. Their assurance services can help verify the effectiveness of your controls and identify areas for improvement.

Strengthen your security posture and demonstrate your commitment to excellence. Connect with us to see how our SOC 2® examinations and readiness services can support your organization's objectives and build trust with your stakeholders.

For more information on SOC reporting

The value of SOC reports in monitoring third-party risks

Click here to read ▸

Authors

Zain Shabbir
Managing Director,
Technology Assurance Audit
T: 415-963-8686
E: zshabbir@kpmg.com

Samantha Brady
Managing Director,
Technology Assurance Audit
T: 314-444-1541
E: smorr@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**