www.pwc.com

Service Organization Controls (SOC) Reports

SOC 2 Basics:

A comprehensive look at the SOC 2 reporting standard

pwc

Agenda

Section One: Background of Service Organization Controls (SOC) Reports

Section Two: The Details of SOC 2 Reporting and Other Key Considerations

Section Three: The Trust Service Principles

Section Four: Is SOC 2 Applicable To Your Organization?

Section Five: How it Works: What to Expect From Your Accounting Firm

Section Six: The Next Frontier: SOC 2+ (When SOC 2 Isn't Enough)

Section One:
Background of Service Organization Controls (SOC) Reports

Background on Service Organization's Controls (SOC) Reports

Today, it is more and more common for businesses to outsource certain services or even entire functions to service organizations. In outsourcing these services, however, many of the risks of the service organization also become the risks of the companies using the service organizations. While management can delegate services or functions to a service organization, the responsibility for the controls cannot be delegated.

User entities and organizations want reporting that provides assurance on controls over operations and compliance, rather than just on controls over financial reporting. The AICPA responded by creating a framework to enable a broader type of third party attestation reporting on controls at service organizations beyond merely financial reporting. This framework is the Service Organization Control (SOC) reporting framework.

The SOC framework has 3 different reporting options: SOC1, SOC2, and SOC3.

SOC 1 Reports

- An engagement performed under the AT801 (SSAE No. 16) standard is known as a **SOC 1** engagement. SOC1 reports replaced the former SAS70 reports.
- SOC 1 reports focus solely on systems and controls at the service organization that may be relevant to user entities' internal controls over financial reporting.
- These reports are frequently requested from service organizations as they are needed for the audit of a user entities' financial statements. Examples of service organizations that may provide a SOC1 report include:
  - Payroll processing companies
  - Healthcare benefit processing companies
  - Trust departments of banks and insurance companies
  - Custodians for investment companies
  - Mortgage servicers or depository institutions that service loans for others
  - Application Service Providers

SOC 2 Reports

SOC 2 reports are appropriate for engagements to report on controls at a service organization related to the Trust Service Principles, defined by the AICPA in TSP Section 100. The Trust Service Principles are:

- Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy

**** SOC 2 engagements are performed in accordance with AT section 101,** *Attestation Engagements,* using guidance in the AICPA Guide*, Reporting on Controls at the Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*.

SOC 3 Reports

SOC 3 reports address a similar subject matter and use the same criteria (Trust Service Principles) as a SOC 2 report, but do not include the following reporting components.

- A description of the service organization's system prepared by management of the service organization.
- A description of the service auditor’s tests of controls or results

SOC 3 reports are general use reports, which allows the service organization to provide the report to anyone. On the other hand, SOC 2 reports are restricted use reports and are typically intended for a specific party with prior business knowledge or understanding of the services provided by the service organization.

Combination of SOC reports

Combining SOC1 and SOC2 reports is not permitted, as SOC2 reports are not specifically designed to focus on systems and controls that may be relevant to user entities' internal controls over financial reporting. Further, SOC1 and SOC2 reports are issued under different standards.

SOC 2 and SOC 3 reports can be combined, the work performed in a SOC2 engagement may enable a service auditor to report on a SOC3 engagement as well. However, you will need to consider the following key factors:

- No subservice organizations can be carved out from a SOC 3 report. All subservice organizations must be included in the scope of the engagement.
- All significant controls relevant to meet the applicable Trust Services Principles need to be encompassed in the SOC 3 report. Complementary user entity controls cannot be used to address these Trust Services Principles, in the SOC3 report.

Comparison of SOC 1, SOC 2, and SOC 3 reports

	SOC 1	SOC 2	SOC 3
Under what professional standard is engagement performed?	AT section 801, (AICPA, **Professional Standards**). Statement on Standards for Attestation Engagements No. 16, **Reporting on Controls at a Service Organization** (SSAE 16)	AT section 101**, Attest Engagements** (AICPA, **Professional Standards**). TSP section 100, **Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy**	AT section 101. **Attest Engagements** (AICPA, **Professional Standards**). TSP section 100, **Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy**
What is the subject matter of the engagement?	Controls at a service organization relevant to user entities' internal control over financial reporting.	Controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy. If the report addresses the privacy principle, the service organization's compliance with the commitments in its statement of privacy practices.	Controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy. If the report addresses the privacy principle, the service organization's compliance with the commitments in its privacy notice

Comparison of SOC 1, SOC 2, and SOC 3 reports (continued)

	SOC 1	SOC 2	SOC 3
What is the purpose of the report?	To provide the auditor of a user entity's financial statements information about controls at the service organization that may be relevant to a user entity's internal control over financial reporting. A type 2 report can be used as audit evidence that controls at the service organization are operating effectively.	To provide management of a service organization, user entities, and other specified parties with information and an independent accountant's opinion on controls at the service organization relevant to security, availability, processing integrity, confidentiality, or privacy. If the report addresses the privacy principle, the service organization's compliance with its privacy commitments.	To provide interested parties with an independent accountant's opinion on controls at the service organization relevant to security, availability, processing integrity, confidentiality, or privacy. If the report addresses the privacy principle, the service organization's compliance with the commitments in its privacy notice.
Who are the intended users of the report?	Management of the service organization; user entities during some or all of the period covered by the report (for type 2 reports) and user entities as of a specified date (for type 1 reports); and auditors of the user entities' financial statements. This does not include prospective users.	Management of the service organization and other specified parties who have sufficient knowledge and understanding of the business, including prospective users.	General distribution

Section Two:
The Details of SOC 2 Reporting and Other Key Considerations

Types of SOC 2 reports

There are two types of SOC 2 reports:

- **Type 1 reports** – The service auditor expresses an opinion on whether the description of the service organization's systems is fairly presented and whether the controls included in the description are suitably designed to meet the applicable Trust Service criteria as of a point in time.
- **Type 2 reports** – The service auditor's report contains the same opinions expressed in a type 1 report, but also includes an opinion on the operating effectiveness of the service organization's controls for a period of time. A type 2 report also includes:

  - A description of the service auditors tests of operating effectiveness and the results of those tests.

Circumstances where a Type 1 report might be useful:

- The service organization's system has not been in operation for a significant length of time
- The service organization has recently made significant changes to the system and related controls and does not have a sufficient history with a stable system
- New service/new report, thus first year reporting considerations

Components of a SOC 2 report

Type 1 report	Type 2 report
A description of the service organization's system.	A description of the service organization's system.
A written assertion by management of the service organization regarding the description of the service organization's system and suitability of design.	Same as type 1 + an assertion by management on the operating effectiveness of the controls in meeting the applicable Trust Services criteria.
A service auditor's report that contains an opinion on the fairness of the presentation of the description of the service organization's system and the suitability of the design of the controls to meet the applicable Trust Services criteria as of a point in time.	Same as type 1+ a service auditor’s report on the operating effectiveness of those controls. A description of the service auditor's tests of controls and the results of the tests.

Responsibilities of Management

In a SOC 2 engagement, management of a service organization is responsible for preparing the description, providing a written assertion and providing a written representation:

- Preparing a description of the service organization's system:
  - Note: The description need not address every aspect of the service organization's system as certain aspects may not be relevant to user entities or beyond the scope of the engagement.
- Providing a written assertion:
  - In the assertion management confirms, to the best of its knowledge that,
    - ◦ Description of system is fairly presented as implemented throughout period
    - ◦ Controls were suitably designed throughout the specified period to meet applicable trust services criteria.
    - ◦ Controls operated effectively throughout period (Type 2 report only)
- Providing written representations to the independent accounting firm

Section Three:
The Trust Service Principles

Defining the system components

Key components of the System

Footnote 1 of TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Technical Practice Aids),* contains the following definition of a system:

***A System* consists of five key components** organized to achieve a specified objective. The five components are categorized as follows:

- *Infrastructure*. The physical and hardware components of a system (facilities, equipment, and networks)
- *Software*. The programs and operating software of a system (systems, applications, and utilities)
- *People*. The personnel involved in the operation and use of a system (developers, operators, users, and managers)
- *Procedures*. The programmed and manual procedures involved in the operation of a system (automated and manual)
- *Data*. The information used and supported by a system (transaction streams, files, databases, and tables)

The Five Trust Services Principles

TSP section 100 provides criteria for evaluating and reporting on controls related to security, availability, processing integrity, confidentiality, and privacy. In TSP section 100, these five attributes of a system are known as *principles*, and they are defined as follows:

a. *Security*. The system is protected against unauthorized access (both physical and logical).

b. *Availability*. The system is available for operation and use as committed or agreed.

c. *Processing integrity*. System processing is complete, accurate, timely, and authorized.

d. *Confidentiality*. Information designated as confidential is protected as committed or agreed.

e. *Privacy*. Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy notice and with criteria set forth in generally accepted privacy principles (GAPP) issued by the AICPA and CICA.

Trust Principles Criteria Components

The following four components are represented in the respective principles and criteria.

- **Policies** – The entity defines and documents its policies for the *'Trust Services Principle'* of its system.
- **Communications** – The entity communicates its defined *'Trust Services Principle'*
  policies to responsible parties and authorized users.
- **Procedures** – The entity placed in operation procedures to achieve its documented *'Trust Services Principle'* objectives in accordance with its defined policies.
- **Monitoring** – The entity monitors the system and takes action to maintain compliance with its defined system *Trust Services Principle*' policies.

Security Principle

The system is protected against unauthorized access (both physical and logical).

- The ***Security Principle*** refers to the protection of the system from unauthorized logical and physical access.
- Limiting access to the system helps prevent potential abuse of the system, theft of resources, misuse of software, and improper access to, or the use, alteration, destruction, or disclosure of information.
- Key elements for the protection of the system include permitting authorized access based on relevant needs and preventing unauthorized access to the system in all other instances.

Availability Principle

The system is available for operation and use as committed or agreed.

- The ***Availability Principle*** refers to the accessibility to the system, products, or services as advertised or committed by contract, service–level, or other agreements. More specifically, it relates to whether the system is accessible for processing, monitoring, and maintenance.
- The ***Availability Principle*** does not, in itself, set a minimum acceptable performance level for system availability. The minimum performance level is established through commitments made by mutual agreement (contract) between the service organization and the user entity(ies).
- The ***Availability Principle*** does not address system functionality (the specific functions a system performs) and system usability (the ability of users to apply system functions to specific tasks or problems).
- Key elements for the protection of the system include identifying and preventing potential threats to the system's availability. Protective measures include: using virus prevention, performing regular system back–ups, and maintaining a disaster recovery center.

Processing Integrity Principle

System processing is complete, accurate, timely and authorized.

- The ***Processing Integrity Principle*** refers to the completeness, accuracy, validity, timeliness, and authorization of system processing.
- Processing integrity exists if a system performs its intended function in an unimpaired manner, free from unauthorized or inadvertent manipulation.
  - Completeness generally indicates that all transactions are processed or all services are performed without exception.
  - Validity means that transactions and services are not processed more than once and that they are in accordance with business values and expectations.
  - Accuracy means that key information associated with the submitted transaction remains accurate throughout the processing of the transaction and that the transaction or service is processed or performed as intended.
  - The timeliness of the provision of services or the delivery of goods is addressed in the context of commitments made for such delivery.
  - Authorization means that processing is performed in accordance with the required approvals and privileges defined by policies governing system processing.

Processing integrity *(continued)*

- **Processing integrity differs from data integrity**. Processing integrity does not automatically imply that the information stored by the system is complete, accurate, current, and authorized.
- If a system processes information inputs from sources outside of the system's boundaries, an entity can establish only limited controls over the completeness, accuracy, authorization, and timeliness of the information submitted for processing.
  - Errors that may have been introduced into the information and the control procedures at external sites are typically beyond the entity's control.
  - Even in a case when the information stored by the system is explicitly included in the description of the system that defines the engagement, it is still possible that the system exhibits high processing integrity without exhibiting high data integrity.
  - For example, an address stored in the system may have passed all appropriate edit checks and other processing controls when it was added to the system, but it may no longer be current (if a person or company relocated) or it may be incomplete (if an apartment number or mailing location is omitted from the address).

Confidentiality Principle

Information designated as confidential is protected as committed or agreed.

- In the course of communicating and transacting business, partners often exchange information they require to be maintained on a confidential basis.
- The confidentiality principle refers to the system's ability to protect the information designated as confidential, as committed or agreed.
- Examples of the kinds of information that may be subject to confidentiality includes: intellectual property and client and customer lists
- What is considered to be confidential information can vary significantly from business to business and is determined by contractual arrangements or regulations.
- Confidential information that is provided to another party is susceptible to unauthorized access during transmission and while it is stored on the other party's computer systems.

Privacy Principle

Personal information is collected, used, retained, disclosed and disposed of in conformity with the commitments in the entity's privacy notice, and with criteria set forth in Generally Accepted Privacy Principles (GAPP) issued by the AICPA and Canadian Institute of Chartered Accountants.

Privacy is defined by GAPP as "the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and disposal of personal information".

Some individuals may consider effective privacy practices to be the same as effective information security; however, privacy encompasses a broader set of activity beyond security that contribute to the effectiveness of a privacy program.

The privacy principle has extended focus areas (criteria) that differ from the other traditional components for the other principles. These additional criteria are described on the following slides.

Privacy *(continued)*

Reporting on a company's compliance with GAPP requires an evaluation of the following:

Notice – The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.

Choice and Consent – The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.

Collection – The entity collects personal information only for the purposes identified in
the notice.

Use, Retention and Disposal – The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.

Privacy *(continued)*

Access – The entity provides individuals with access to their personal information for review and update.

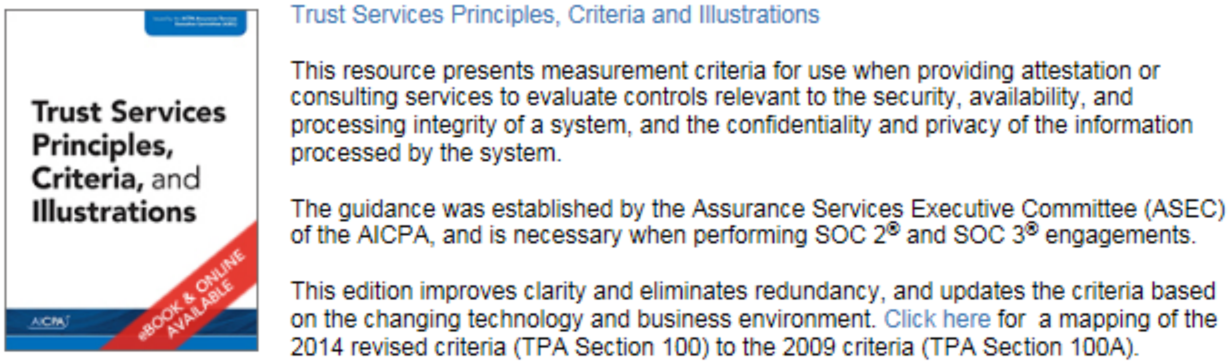
Disclosure to third parties – The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.

Security for Privacy – The entity protects personal information against unauthorized access (both physical and logical).

Quality – The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.

Monitoring and Enforcement – The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy related inquiries, complaints and disputes.

New Guidance from AICPA Available



Trust Services Principles, Criteria and Illustrations

This resource presents measurement criteria for use when providing attestation or consulting services to evaluate controls relevant to the security, availability, and processing integrity of a system, and the confidentiality and privacy of the information processed by the system.

The guidance was established by the Assurance Services Executive Committee (ASEC) of the AICPA, and is necessary when performing SOC 2® and SOC 3® engagements.

This edition improves clarity and eliminates redundancy, and updates the criteria based on the changing technology and business environment. Click here for a mapping of the 2014 revised criteria (TPA Section 100) to the 2009 criteria (TPA Section 100A).

The most significant changes include:

- **Restructuring of the trust services principles and criteria:** The principles and criteria for security, availability, processing integrity, and confidentiality are restructured into (1) common criteria that is applicable to all four principles, and (2) criteria applicable only to a single principle. The criteria related to the privacy principle contained in the generally accepted privacy principles (GAPP) are being revised separately.

- **Risk assessment:** To illustrate the linkage between criteria, risks, and controls, appendix B, "Illustrative Risks and Controls," was developed to provide examples of risks that may prevent the criteria from being met, as well as examples of controls that would address those risks.

Section Four:
Is SOC 2 Applicable To Your Organization?

Applicability

Considerations of where SOC2 reports may be applicable for your organization:
SOC 2 Reports are applicable when an entity outsources the collection, processing, transmission, storing, organizing, maintenance or disposal of the entity's information.

Here are some examples where a SOC 2 report should be obtained:

- Fintech (Financial Services Technology Providers)
- Cloud Service Providers
- Intellectual Property Protection
- Sales Force Automation
- HealthCare Providers and Payers, HIPAA
- Data Center Hosting Service Providers

Section Five:
How it Works: What to Expect From Your Accounting Firm

Evaluating Fairness of the Presentation of the Description

SOC 2 requires that management provide a written assertion and that such assertion be attached to management's description. Suitable criteria is the standard or benchmark used to measure and present the subject matter. Management will select the criteria used to measure the and present the subject matter and will state those criteria in the assertion.

Below is a subset of the criteria for determining whether the description of the service's organization's system is fairly presented:

- Types of services provided
- Components of the system used to provide the services (infrastructure, software,
  people, procedures, data)
- Boundaries/aspects of system
- Information on subservice organizations
- Other aspects of the service organization's control environment
- Any changes over the period represented.

What Does it Cost?

The cost of delivering SOC 2 reporting varies across different organizations. The following factors will impact the cost of reporting for SOC 2:

- The size and complexity of your organization (number of employees, multiple locations, etc.)
- The number of Principles selected. You can select one, several, or all of the Principles.
- The Type of report (Type 1: design only vs. Type 2: design and operating effectiveness)
- The period covered by your report (6-12 months)
- The number of controls. You can include all of your controls or minimize the scope to only high level controls or certain business areas to reduce cost and impact.

Remember this is an annual recurring report, so the upfront cost is always higher. Expect costs to lower by 10-20% in subsequent years.

How Long Does it Take?

The following are averages across multiple organizations:

Type 1 Report

Planning and Scoping: 2-4 weeks

Design Assessment: 3-4 weeks

Reporting: 2 weeks

Total Time: 7-10 weeks

Type 2 Report

Planning and Scoping: 2-4 weeks

Design Assessment: 4-6 weeks (sometimes spread over 2 periods)

Reporting: 4 weeks

Total Time: 10-14 weeks

Section Six:

The Next Frontier: SOC 2+ (When SOC 2 Isn't Enough)

Questions?

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, [PricewaterhouseCoopers LLC, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.