



1

SOC Reports





SOC

SOC Stands for '**System and Organization Controls**'. It is an attestation standard put forth by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA). SOC reports are intended to examine services provided by a service organization so that end users can assess and address the risk associated with an outsourced service. Before understanding SOC reports, it is an important to understand '**Types of Auditing**'. Basically, security audits are of 3 types: Internal, External and 3rd Party.





Types of Audit Reports

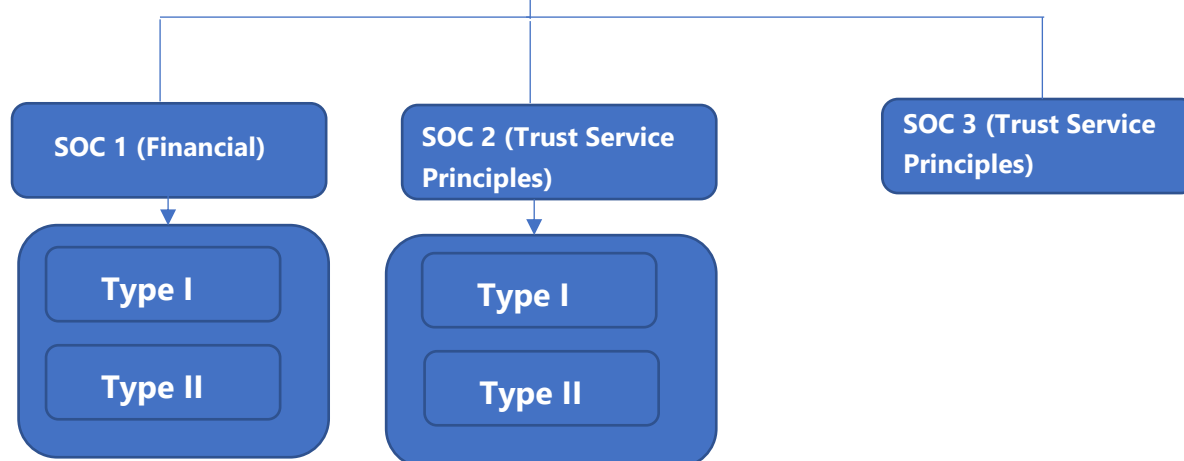
Type I

- Type I audits cover **single point in time**.
- Provide description of the controls provided by the audited organization as well as the auditor's opinion based upon description.
- Does not include actual testing of controls by the auditor.
- Type I reports simply take the service organization at their word that the controls are implemented as described.

Type II

- Type II covers a **minimum six-month time period** and include opinion from the auditor on the effectiveness of controls.
- Actual control testing performed by the auditor.
- Type II reports are considered more reliable than Type I as include independent testing of controls.

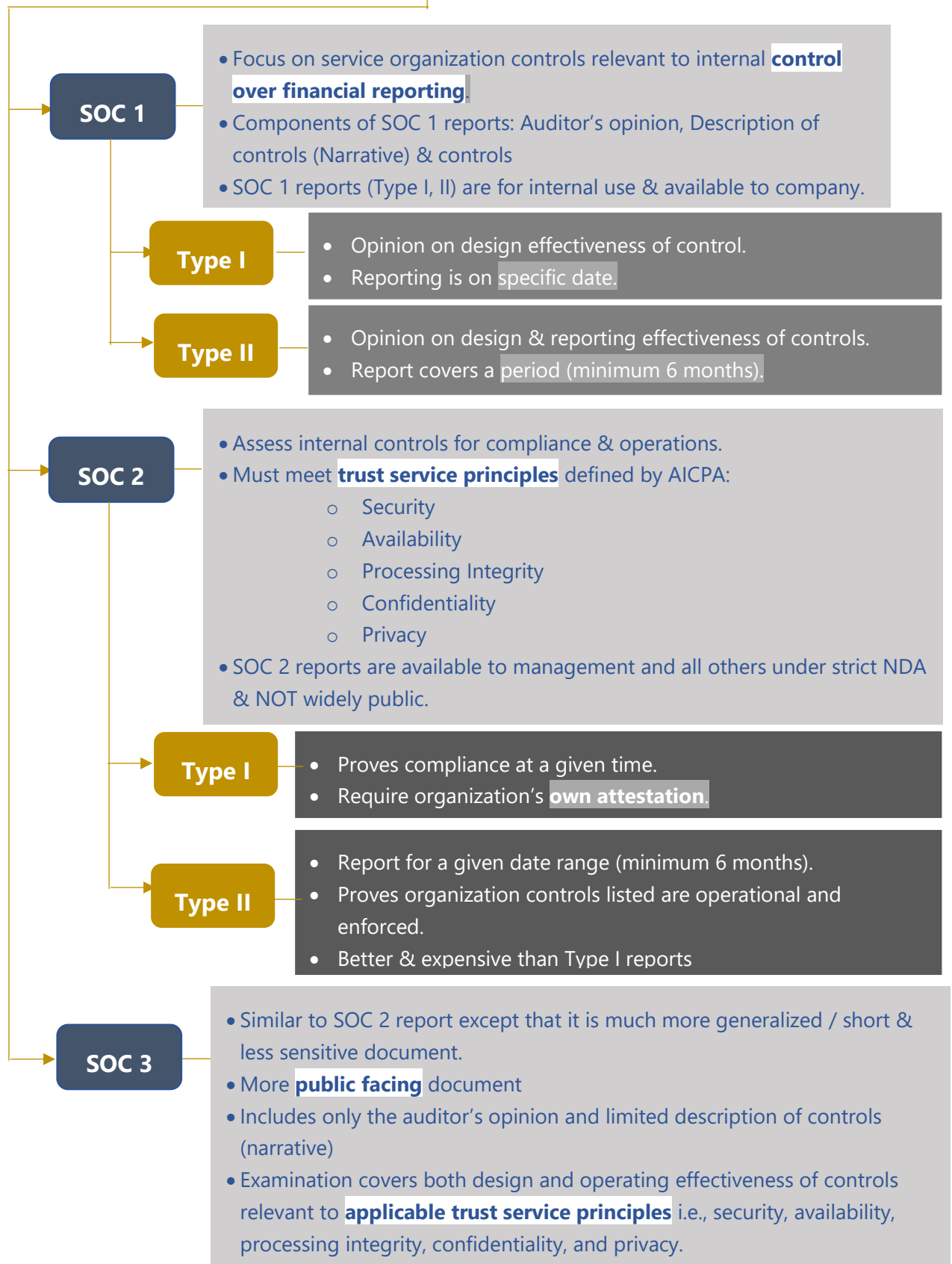
SOC Reports



	SOC 1	SOC 2	SOC 3
Internal control over financial reporting	✓		
Trusted Service Principles		✓	✓
Restricted use	✓	✓	General use



Service Organization Controls (SOC) Report





SOC 2 & SOC 3 Trust Service Principles

Principle Area	Principle Objectives
Security	The system is protected against unauthorized physical and logical access.
Availability	The system is available for operating and use as committed or agreed.
Confidentiality	Information designated as confidential is protected as committed or agreed.
Processing Integrity	System processing is complete, accurate, timely and authorized.
Privacy	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).

Evolution of SAS 70 SSAE 16 SOC Reports

Evolution of SAS 70 → SSAE 16 → SOC Reports

- In June 2010, the American Institute of certified public accounts (AICPA) issues SSAE 16, effectively eliminating SAS 70 and establishing service organization controls (SOC) reports.
- Change was made to mirror international standard on Assurance engagements (ISAE) no. 3402.



- Established SOC 1, SOC 2 & SOC 3



Purpose

1. Who gets a SOC examinations?

- Service organizations (provide services to others)

2. Why do service organization need SOC examination?

- To provide comfort to user organizations about the process & relevant to the controls at the service organization.

3. Who will be using the reports?

- User organization management
- User organization auditors



Scenarios

Below are some scenario-based questions to understand the SOC Report Types and their purpose.

Q1. Andrew is a CISO for a major hospital system and is preparing to sign a contract with a Software as a service (SaaS) email vendor and want to ensure that its business continuity planning measures are reasonable. What type of audit might Andrew request to meet his goal?

- A. SOC 1
- B. FISMA
- C. PCI DSS
- D. SOC 2

Ans. 'D': The service organization control audit program includes business continuity controls in a Type II, but not Type I, audit. Although FISMA and PCI DSS may audit business continuity, they would not apply to an email service used by a hospital.

Q2. Andrew wants to ensure that the audit report that his organization requested includes input from an external auditor, what type of report should he request?

- A. SOC 2, Type I
- B. SOC 3, Type 1
- C. SOC 2, Type II
- D. SOC 3, Type 2

Ans. 'C': SOC 2, Type II report include information about a data centre's security, availability, processing integrity, confidentiality and privacy and includes an auditor's opinion on the operational effectiveness of the controls. SOC 3 does not have types and a SOC 2, Type I only requires the organizations own attestation.

Q3. Which SOC report type is of most interest to a technical audience due to its trust services principles?

- A. SOC 1, Type I
- B. SOC 1, Type II
- C. SOC 2
- D. SOC 3

Ans. 'C': SOC 2 is available for technical audience. SOC I, Type I & SOC 1, Type II doesn't have trust services principles. SOC 3 is also ruled out.

Q4. Which statement is true about SOC 1, Type 2 report?



- A. Design of controls on a specific date
- B. Design of controls through a period for 3 months
- C. Operating effectiveness of controls on a specific date
- D. Operating effectiveness of controls over a period between six months

Ans. 'D': options A, B, C does not qualify condition of minimum time frame of six months.

Q5. As Andrew's company prepare to migrate their data center to an Infrastructure as a service (IaaS) provider, Andrew's company want to understand the effectiveness of their new service provider's security, integrity, and availability controls. What SOC report would provide them with the most detail?

- A. SOC 1
- B. SOC 2
- C. SOC 3
- D. None of the SOC reports are suited to this and they should request another form of report.

Ans. 'B': SOC 2 report are released under NDA to select partners or customers and can provide detail on the controls and any issues they may have. A SOC 1 report would only provide financial control information, and a SOC 3 report provides less information since it is publicly available.

Reference links

Below are few reference links to actual SOC reports. Links are to help understand SOC reports content and descriptions.

- [Microsoft](#)
- [Google](#)
- [AWS](#)

END