SOC 2 Opinions

Unqualified Opinion - No issues were noted in the description, controls, testing, etc. that would cause a modification of the opinion, and management's assertion is deemed reasonable. This is the type of opinion you should be striving for. When you hear people refer to "passing" a SOC 2 examination, they are more than likely referring to an unqualified opinion.

Qualified Opinion - A common but undesired opinion that means the service auditor identified at least one issue or exception in the report. An example exception is one of the sampled new hires did not complete security awareness training.

Disclaimer of Opinion - If there was a severe inability for the service organization to produce evidence for the examination (the scope limitation was material and pervasive). The service auditor would not have enough information to make a suitable opinion in this case.

Adverse Opinion - If there were material misstatements that were both material and pervasive to the point that the control environment is failing to meet either SOC 2 criteria or the service organization's commitments, system requirements, or objectives.

SOC 2 Report Types

In a SOC 2 examination, organizations can undergo a SOC 2 Type 1 or SOC 2 Type 2 examination. A Type 1 examination is a report on the controls at a service organization at a specific point in time, whereas, a Type 2 examination is a report on the controls at a service organization over a period of time. The period of time evaluated in a SOC 2 Type 2 examination is typically between 3-12 months.

Type 1:

- As of a single point in time
- Shows the suitability of the design of the controls and environment
- Used as a stepping stone for service organizations doing their first SOC 2
- Demonstrates maturity to customers and publish the AICPA SOC Logo on your website

Type 2:

- Covers a period of time (3-12 months is recommended review period)
- Shows operational effectiveness of controls in addition to suitability of the design of the controls and the environment.
- An annual assessment undertaken by a service organization to measure their controls
- Demonstrates a consistent and continuous security program to your customers

Tip: Most companies undergo a SOC 2 readiness or use a SOC 2 automated readiness platform (e.g. ByteChek) before pursuing a SOC 2 Type 1 or Type 2. The logical next step after the readiness is a SOC 2 Type 1. After the SOC 2 Type 1, the review period for the SOC 2 Type 2 begins for anywhere between 3-12 months.

SOC 2 Sections of the Report

In a SOC 2 report, there are five sections to be aware of.

Section 1:
Independent Service Auditor's Report:

Section 2:
Management's Assertion

Section 3:
System Description

Section 4:
Trust Services Categories, Criteria, Related Controls and Tests of Controls Relevant to In-Scope TSCs

Optional Section 5:
Other Information Provided by Management That Is Not Covered by the Service Auditor's Report

SOC 2 Process

Earning a SOC 2 requires a Company to undergo a third-party examination by a Certified Public Accountant (CPA). The CPA is required to follow a set of AICPA standards to perform the audit and issue the report. Most companies follow a logical process to earning their SOC 2:

Step 1: Readiness examination: An exercise where your Company finds out the current status of the organization as it relates to SOC 2 controls. Organizations use readiness examinations to prepare for their SOC 2 assessment and learn what gaps they must resolve before earning their SOC 2.

Step 2: Earn a SOC 2 Type 1 - While it is not required for an organization to earn a SOC 2 Type 1 before a SOC 2 Type 2, the logical next step on the SOC 2 journey is to complete a SOC 2 Type 1 examination. The path from readiness to SOC 2 Type 1 is all dependent on how fast the organization can remediate gaps identified in the readiness assessment.

Step 3: Earn your SOC 2 Type 2 - After a specified period of time (anywhere from 3-12 months) organizations earn their first SOC 2 Type 2. Typically the Type 2 review period begins the day after the date of the Type 1 review period.

Step 4: Renew your SOC 2 Type 2 every 12 months. A SOC 2 Type 2 looks back in time and every year you'll need to undergo a Type 2 examination to keep your SOC 2 current.

SOC 2 EXAMINATION CHEATSHEET

By AJ Yawn, Founder & CEO at ByteChek

Cheat Sheet v1.0

sans.org/cybersecurityleadership

System and Organization Controls or SOC 2 is a reporting framework developed by the American Institute of Certified Professional Accountants (AICPA). You should consult the AICPA website for all authoritative documents on SOC 2.

sans.org/cybersecurityleadership

SOC 2 Trust Services Categories

There are five Trust Services Categories (formerly known as Trust Services Principles) that a service organization can choose to be evaluated against in a SOC 2 examination. The five Trust Services Categories and their definitions as defined by the AICPA are:

Security:
Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.

Availability:
Information and systems are available for operation and use to meet the entity's objectives.

Processing Integrity:
System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.

Confidentiality:
Information designated as confidential is protected to meet the entity's objectives.

Privacy:
Personal information is collected, used, retained, disclosed, and disposed of to meet the entity's objectives.

Tip: Security, Availability and Confidentiality are the most common.

SOC 2 System Description

The system description must be presented in accordance with the AICPA's description criteria (DC 200). Each of the description criteria (DC) are described below:

DC1: Types of services provided
Describe what services the service organization provides as it relates to the system in scope.

DC2: Principal service commitments and system requirements
This section lets the reader know what commitments and system requirements the service organization is making, and which documents the reader can find these commitments in (e.g. MSA, SLAs, Privacy Policy, etc.). This helps give the reader context as to what trust services categories are in-scope and why.

DC3: Components of the system
The components described here include the infrastructure, software, people, procedures, and data that support and make up the system. For many Cloud Service Providers (CSP), the infrastructure section will include their hosting provider (such as Amazon Web Services). The software section should list the software and applications that support delivering the service in scope. The people section should include an overview of the departments or key personnel that support the system and what they do. Procedures should state what procedures are and their purpose. Data should discuss what the data is that the system processes (what is your customer data), as well as any other data that directly supports the system.

DC4: System incidents
Describe any security incidents that rose to the level where your company failed to either meet criteria, your commitments to customers, or your system requirements.

DC5: Applicable trust services criteria and related controls
Describe the criteria that are in-scope so that the reader understands the criteria the service organization is being measured against. The service organization will also discuss in detail the control environment and describe the controls that support it. This is a narrative section that is essentially a lighter version of the information security policy.

DC6: Complementary user entity controls (CUECs)
CUECs are the controls that the service organization's customers need to have in place in order for the system and control environment to be complete and achieve its objectives. For example, maybe the customers need to have their own logical access controls in place so that only authorized users access the service, otherwise, unauthorized access may cause you to fail to meet your security commitments.

DC7: Complementary subservice organization controls (CSOCs)
The service organization will discuss the subservice organizations that support the system and control environment. Subservice organizations are vendors that you cannot meet your criteria, commitments, or system requirements without. For most CSPs, that is going to be the cloud hosting provider (AWS, GCP, Azure, etc.)

SOC 2 Key Terms

Complementary Sub-Service Organization Controls: Controls that service organization management assumed, in the design of the service organization's system, would be implemented by the sub-service organization that is necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved.

Complementary User Entity Controls: Controls that service organization management assumed, in the design of the service organization's system, would be implemented by user entities and are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved.

Control Activity: An action established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out.

Management's Assertion: A written assertion by the management of a service organization or management of a sub-service organization, if applicable, about whether (a) the description of the system is in accordance with the description criteria, (b) the controls are suitably designed, and (c) ina type 2 report, the controls operated effectively to achieve the service organization's service commitments and system requirements based on the applicable trust services criteria.

Operating Effectiveness (or Controls That Are Operating Effectively): Controls that operated effectively provide reasonable assurance of achieving the service organization's service commitments and system requirements based on the applicable trust services criteria. personal information. Information that is about, or can be related to, an identifiable individual.

Service Organization: An organization, or segment of an organization, that provides services to user entities.

Sub-service Organization: A vendor used by a service organization that performs controls that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved.

Suitability of Design (or Suitably Designed Controls): Controls are suitably designed if they have the potential to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved. Suitably designed controls are operated as designed by persons who have the necessary authority and competence to perform the control.

Trust Services Criteria: A set of professional attestation and advisory services based on a core set of criteria (trust services criteria) related to security, availability, processing integrity, confidentiality, or privacy.