KirkpatrickPrice
Innovation. Integrity. Delivered.

The SOC 2 Compliance Handbook:

Your guide to SOC 2 Audit Success

16057 W. Tampa Palms Blvd. | #134 | Tampa, FL 33647 | kirkpatrickprice.com | 800.770.2701

Table of Contents

Abstract

Organizations don't want to do business with at-risk vendors. That's why many service organizations are being asked for a SOC 2 audit report. SOC 2 compliance helps to address any and all third-party risk concerns by evaluating internal controls, policies, and procedures that directly relate to the security at a service organization.

This white paper will help familiarize you with an overview of SOC 2 compliance and reporting. We will discuss reasons why you may have been asked by a client to receive a SOC 2 audit, the history of SOC 2 reports, understanding the different Trust Services Principles and how they may apply to your organization, and reasons why your organization will benefit from SOC 2 compliance.

Why am I being asked about SOC Compliance?

It's another busy day in the office. Your time is consumed by overseeing a multitude of responsibilities, conference calls, and customer service. On top of your regular duties, you've just been asked by a client to get a SOC audit. "A what?!", you think. As you scramble to research what a SOC audit is, you may be wondering why you're being asked about SOC compliance in the first place.

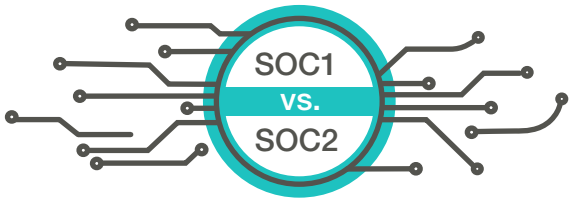
Service organizations are often required to produce, for their clients and prospects, independent third-party reviews. For companies to be certain their vendors are protecting the confidentiality, integrity, and availability of their sensitive information, they must validate that the internal controls and processes they have in place are protecting key systems and data.

Service Organization Control reports are reports based on the assessment of the internal controls of the services provided by a service organization, and thusly are a common method for demonstrating a commitment to privacy and security.

"demonstrate a commitment to privacy & security"

What's the difference between a SOC 1 and SOC 2?

SOC compliance comes in a few different shapes and sizes. Do you need SOC 1 or SOC 2 compliance? What's the difference? Do you need both?



SOC 1 Audits

A Service Organization Control 1 report, or SOC 1, is based on an audit of the internal controls at a service organization that are relevant to internal control over financial reporting (ICFR). If you handle information that could potentially affect your client's financial reporting, you will most likely be asked for a SOC 1.

SOC 2 Audits

A Service Organization Control 2 report, or SOC 2, is similar to a SOC 1 in that it evaluates internal controls, policies, and procedures. However, the difference is that a SOC 2 reports on controls that are directly related to the security, availability, processing integrity, confidentiality, and privacy. These five criteria are also referred to as the Trust Services Principles, or TSP's.

History of the SOC 2

The SOC 2 came into existence as a way for service organizations to manage the risks that are associated with outsourcing business operations. The original standard, SAS 70, was a new way for organizations to demonstrate the effectiveness of the internal controls at their organization. When the SOC 1 replaced SAS 70 as a way to report on controls that may affect a client's financial statements, the SOC 2 was introduced as an assessment that specifically addressed security.

The SOC 2 is intended to give a broader range of organizations the information security assurance they need to demonstrate that their internal controls related to security, availability, processing integrity, confidentiality, and/or privacy are appropriate and operating effectively.

Understanding the Trust Services Principles

The SOC 2 audit is based on a predefined set of criteria known as the Trust Services Principles (TSPs). Understanding the Trust Services Principles is a critical part of determining the scope of your SOC 2 audit, deciding how the principles apply to the services you provide, and selecting which Trust Services Principles you want to include in your SOC 2 audit report. SOC 2 reports can address one or more of the following principles: Security, Confidentiality, Availability, Processing Integrity, and/or Privacy.

The AICPA has defined the Trust Services Principles to address the following:

Security

In a non-privacy SOC 2 engagement, the Security principle must be included. Security is the common criteria that applies to all engagements, and is what the remaining Trust Services Principles are based on. The Security principle addresses whether a system is protected (both physically and logically) against unauthorized access.

Availability

The Availability principle typically applies to companies providing colocation, data center, or hosting services to their clients. It ensures that the system you provide to your clients is available for operation and use as agreed upon. It also addresses whether the services you provide are operating with the type of availability your clients expect.

Processing Integrity

If the services you provide are financial services or e-commerce services and you are concerned with transactional integrity, include Processing Integrity in your SOC 2 report. The Processing Integrity principle attests that the services you provide to our clients are provided in a complete, accurate, authorized, and timely manner.

Confidentiality

If your organization is responsible for handling sensitive data, such as Personally Identifiable Information (PII) or Protected Health Information (PHI), the Confidentiality principle should be present in your SOC 2 audit report. The Confidentiality principle addresses the agreements that you have in place with your clients in regards to how you use their information, who has access to it, and how you protect that information. It verifies whether you are following your contractual obligations by properly protecting client information.

Privacy

The Privacy principle stands on its own and specifically addresses how you collect and use consumers' personal information. It ensures that your organization is handling client data in accordance with any commitments in the entity's privacy notice as committed or agreed, and with criteria defined in the generally accepted privacy principles issued by the AICPA.

Type I vs. Type II

There are similarities and differences between a SOC 2 Type I and a SOC 2 Type II. Most organizations eventually undergo a SOC 2 Type II audit, however, it is often recommended that service organizations begin with a SOC 2 Type I as a good starting point and then move to a SOC 2 Type II.

A SOC 1 Type I and Type II are both service organization control reports, reporting on the controls and processes at a service organization. A SOC 2 Type I report is an attestation of controls at a service organization at a specific point in time. A SOC 2 Type II report is an attestation of controls at a service organization over a minimum six-month period and reports on the "suitability of the design and operating effectiveness of controls" whereas with a SOC 2 Type I, there is no testing.

Contents	Type I	Type II
Independent Service Auditor's Report	*	*
Service Organization's description of controls	*	*
Offers opinion on management's presentation of the Service Organization's current controls	*	*
Evaluates the suitability of design of management's description of the Service Organization's systems	*	*
Evaluates the Services Organization's control systems		*
Offers a description of the Service Auditor's tests of the operating effectiveness of controls and the results of each test		*

Who can issue a SOC 2 audit report?

A SOC audit can only be performed by an independent Certified Public Accountant (CPA). CPAs must adhere to the specific standards that have been established by the American Institute of Public Accountants (AICPA) and have the technical expertise to perform such engagements. This third-party opinion verifies the suitability of the design and operating effectiveness of the service organization's controls to meet the criteria for the selected principles.

Why should I get a SOC 2 audit?

Many organizations are required to undergo a third-party audit. If this is the case, you should have a SOC 2 audit performed. By being able to produce a SOC report, you may be a better contender for RFP's. Having a SOC 2 audit report can give you a competitive advantage by demonstrating to your clients, and prospective clients, that you are dedication to security and delivering high-quality services. Lastly, knowing that your internal controls are validated and operating effectively can give you the peace of mind you need to be confident in your security posture.