What is SOC 2 & Why is Everyone Talking About it?

The benchmark for validating strong IT security postures also fosters relationships with customers and business partners.

Introduction

If a customer or business partner has not already asked for your SOC 2 report, you will likely receive such a request soon. With cyberattacks on the rise and growing ever-more prevalent and impactful, businesses of all sizes are not only concerned with protecting their own information systems, but they are also focusing on the security postures of their partners and any integrated ecosystems they share.

Service Organization Control 2 (SOC 2) attestation reports play a key role in helping organizations take on this challenge by evaluating the security postures of customers and their supply chains. The report provides objective standards created by the American Institute of Certified Public Accountants (AICPA). And passing a SOC 2 audit by an independent assessor from a CPA firm and receiving a validated report enables organizations to demonstrate they have implemented a strong IT security posture for protecting sensitive data.

SOC 2 is well-regarded as a benchmark by software and services industries and provides a consistent method to assess and share the security controls and compliance postures of many entities. Additionally, organizations also benefit from a repeatable framework they can use to establish a strong security posture to demonstrate internally how well they protect their own sensitive data.

Why Get a SOC 2?

As noted earlier, many businesses decide to pursue a SOC 2 report as the result of a formal request from a customer or a business partner, often included as part of a request for price or quote (RFP/RFQ).

For this reason, you may discover competitive pressure where other businesses have proactively pursued a SOC 2 attestation report—some post the achievement on their website to attract customers—thereby highlighting that they take protecting sensitive data seriously. All things being equal, a customer will often choose to do business with a company that has a SOC 2 report over one that doesn't. They prefer to avoid taking the chance of sensitive data not being secured.

SOC 2 reports may also be required when attempting to obtain cyber insurance. And by following the assessment guidelines, businesses can further streamline their effort to achieve compliance with regulations and other standards like HIPAA, ISO, and PCI DSS.

Lastly, and perhaps more importantly, SOC 2 is simply a great place to start for any business looking to measure and improve its IT security posture—regardless of whether an external entity is requesting it. With detailed guidance on the controls that must be in place, given the scope of sensitive data in a particular IT environment, internal IT teams can make sure they meet the security requirements of the business in keeping sensitive data safe that belongs to the business as well as customers and partners.

4 Key Questions to Determine the Need for a SOC 2 Assessment:

Do you share sensitive data or integrate your sensitive data with those of other companies, (customers or partners)?	Yes	No
Can you demonstrate your ability to ensure the availability of sensitive data to authorized customers and partners?	Yes	No
Can you ensure the integrity of the sensitive data you process—proving it has not been tampered with or altered accidentally?	Yes	No
Can you prove you have deployed the necessary privacy controls to protect sensitive data?	Yes	No

If the answer to #1 is **yes**, and the answer to any one of the other questions is **no**, then you likely need to pass a SOC 2 assessment. Only then can you be sure you protect sensitive data and stay competitive in winning customer proposals and forming business partnerships.

To get started on the process, **schedule a personalized SOC 2 demo** from VGS.

What's In It For You? How Passing a SOC 2 Audit Helps Your Business.

While your initial efforts to pass a SOC 2 audit may be driven by a request from a single customer or business partner, going through the process will generate a wide range of benefits:

- **Builds a security-first culture** across the entire organization by establishing the importance of protecting sensitive data and increasing the awareness of how to prevent cyber attacks.
- **Creates a streamlined, scalable**, and repeatable foundation for the future to maintain a strong IT security posture while removing the need to complete time-consuming due diligence questionnaires.
- **Establishes trust with customers**, prospects, and partners that your organization secures sensitive data.
- **Facilitates the process of closing** on new business and generating revenue faster by eliminating security concerns upfront.

All of these benefits serve to make your company more appealing to customers and partners—and easier to do business with.

SOC 2 Report Types and Areas of Focus

Your organization can obtain either a SOC 2 Type I or a Type II attestation report. Type I audits evaluate your security controls and whether those controls operate correctly at a specific point in time. Type II audits do the same as Type I over a period of time, such as 3, 6 or 12 months.

As you explore what it will take for your organization to pass a SOC 2 audit, it helps to understand the high-level Trust Services Criteria principles that an independent auditor will examine. While the Security criteria component is part of every SOC 2 audit, the other four criteria are optional.

Security
All SOC 2 reports start with the baseline of security, also called common criteria. Are your information and IT systems protected against unauthorized access and disclosure of data (digital and physical)? This principle checks to make sure firewalls, security controls, and device configurations won't compromise the availability, integrity, confidentiality, and privacy of sensitive data.

When your organization undergoes a SOC 2 audit, Security is the default TSC, and the only one that is required.

Security is also referred to as the "Common Criteria" and covers some basic overlap with the other TSCs. The other TSCs may be added to your audit, typically for an additional cost.

Availability
Are information and IT systems always available for use for your business-process workflows to operate efficiently? This principle refers to data used by your organization as well data, products and services provided to customers and partners. Assessors will verify if you have sufficiently implemented and tested your disaster recovery and business continuity plans.

SOC 2 Report Types and Areas of Focus (cont.)

Processing Integrity
Are payment transactions and data processing complete, valid, accurate, timely, and authorized to meet the requirements of business workflows? Do you correct errors promptly? In other words, can you ensure data is not tampered with or altered?

Confidentiality
Is confidential information belonging to data subjects protected by appropriate controls? The controls need to cover private and sensitive data as it goes through collection, creation and to final disposition and eventual removal from your systems.

Privacy
Is personal information properly collected, encrypted, used, retained, disclosed, and disposed of within the scope of meeting your business requirements? Whereas confidentiality applies to various types of sensitive information, privacy applies to personal information

These principles will serve as the basis for your SOC 2 program and will affect the scope of your audits. You may need to comply with only one principle, a combination, or all five; it depends on whether additional requirements are being imposed by customer or partner needs OR through added due-diligence and commitment to security on your part. After the scope is agreed upon, your team can then develop and tune policies and controls to set you up for successfully passing the audit.

How to Utilize the Results of Your SOC 2 Report

Passing a SOC 2 audit by an independent assessor from a CPA firm authorized by the AICPA demonstrates to customers and partners that an organization has implemented the appropriate controls, security configurations, and internal policies to manage their organization and their sensitive data securely. The assessor will also attest that the controls work effectively. The process begins with you asserting your controls meet the SOC 2 criteria, then the assessor provides an opinion on whether they agree with you.

Successfully completing the SOC 2 audit process and receiving a positive opinion from the assessor results in receiving a SOC 2 report. It is not considered a certification of your security controls as to how well you protect data, but rather an attestation that your controls sufficiently protect data.

Should your controls fall short during a SOC 2 assessment, you simply would not receive a report, but don't despair. Your auditor will show you where your security gaps exist, and once you close them, you can restart the process. The potential drawbacks of the failure include the cost to implement the necessary security controls. You also risk losing business because a customer or partner does not want to take the chance that your IT infrastructure might jeopardize their sensitive data.

Keep persevering. Once you pass the audit process and receive the report, you will then possess a valuable tool

What About SOC 1 and SOC 3?

A common question from businesses and organizations as they examine the SOC 2 process is whether they should also look into achieving SOC 1 and SOC 3 reports. Much will depend on what your customers and business partners request. SOC 1 focuses specifically on data that impacts financial statements while SOC 3 provides a public-facing report with confidential information removed. SOC 2 is broader in its coverage for protecting digital assets and is meant to be shared privately with customers and partners with which an entity has a business relationship.

How to Utilize the Results of Your SOC 2 Report (cont.)

to foster customer and business relationships by demonstrating just how well your organization protects sensitive data. Generally, a SOC 2 report is valid for 12 months, so you will also need to plan and budget to go through the audit review process at least annually. Keep in mind that the review period and your specific organization goals may affect this timeline. This also makes sense from a basic IT security strategy standpoint. With new cyber threats constantly emerging, your defenses can never rest. Many information security best practices suggest managing the company's security posture on a real-time basis, and there are tools available to help with this while meeting the SOC 2 requirements.

And, while receiving a SOC 2 report attests to customers and partners that you have implemented strong controls to protect sensitive data, the report does not signify compliance with regulations and other standards such as HIPAA, ISO, and PCI DSS. However, as you work towards compliance with such regulations and standards, you will discover that the security controls you validated and implemented to receive your SOC 2 report will contribute greatly in helping you achieve other compliance initiatives—or they may satisfy some requirements altogether.

Getting Started: How VGS Can Help

If you share data or integrate any of your IT systems with customers and business partners, passing the SOC 2 report is vital for your business. And that's where VGS can help.

VGS Control combines powerful SOC 2 compliance automation with a data security solution in a single, easy-to-use platform. This gives you the ability to implement strong security controls and achieve a complete and accurate SOC 2 attestation report that enables you to build trust with your customers and business partners. Visit the VGS website to learn more. If you are ready to begin your SOC 2 journey, schedule a personalized SOC 2 demo from VGS.

VERY GOOD SECURITY

207 Powell Street, Suite 200
San Francisco, CA 94102

contact@verygoodsecurity.com
verygoodsecurity.com

About Us

Very Good Security (VGS) enables organizations to focus on their core business by offloading their data security and compliance burden to VGS. VGS customers unlock the value of sensitive data without the cost and liability of securing it themselves, and accelerate compliance with PCI, SOC 2, HIPAA, GDPR, and more.