The Ultimate SOC 2 Guide

1. Introduction
2. SOC 2 Report Types
3. Trust Services Criteria
4. SOC 2 Audit Process
5. VGS is SOC 2 Compliance, Reimagined
6. VGS Case Study: Accord

Introduction

Enterprises often view audits as a necessary cost of doing business. Indeed, a SOC 2 report may simply be a requirement for your next contract. But there is a better way to understand a serious security audit.

In today's marketplace, it is a competitive differentiator, and a way for your organization to strengthen its credibility with customers, partners, and investors. A SOC 2 audit demonstrates how seriously your organization takes security and compliance, and proves that you are committed to protecting sensitive data.

The SOC Framework

System and Organization Controls (SOC) is a reporting framework through which your organization can describe the effectiveness of its information security and cybersecurity risk management programs.

SOC is relevant to a broad range of stakeholders, is used to assess and address the risks associated with an outsourced service, and is defined by the American Institute of Certified Public Accountants (AICPA). There's also a SOC1 (financial controls) and SOC3 (security controls for public consumption), but this paper only covers SOC2.

What is a SOC 2 Report?

A SOC 2 report provides detailed information and assurance regarding the security posture of organizations that provide services to other organizations. It evaluates the controls that handle user data, based on the following Trust Services Criteria (TSC):

- Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy

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.

Who Needs a SOC 2 Report?

SOC 2 reports are designed to meet the needs of stakeholders who need detailed information and assurance about the systems, information, and controls at businesses that process user data.

SOC 2 reports play an important role in:

- Organizational oversight
- Vendor management
- Corporate governance
- Risk management
- Regulatory oversight

Due to the impact of thousands of devastating data breaches, SOC 2 has become ubiquitous in the software as a service (SaaS) business-to-business (B2B) world, and standard for any organization that stores customer data in the cloud.

Can I Share My SOC 2 Report?

Yes, but it is a common practice to sign a non-disclosure agreement (NDA) with any and all third parties. It is natural that vendors and partners would like to review your SOC 2 report. However, because a SOC 2 report details all of your company's internal security controls, this information would give a malicious party too much technical information about your corporate architecture and its potential weaknesses. Therefore, the use of a SOC 2 report is typically restricted to business management, users with a need-to-know, and SOC 2 auditors.

However, this is where a SOC 3 report, which is a pared down and less sensitive version of an organization's SOC 2 report, comes in handy.

Refer to the next page for more information on SOC 3 reports.

Immediate Benefits

At every level of business and government, data security is increasingly the focus of regulation and legislation. And today, SOC 2 is regarded as the industry standard for B2B SaaS compliance.

SOC 2 certification provides immediate, tangible benefits:

- Validation of your strong security posture
- A certification credential that you can advertise
- A report that you can share
- Increased consumer and partner trust
- Faster business deals

In short, the rigor of the SOC 2 process demonstrates to the world that your business has a strong commitment to security, and it can be a powerful stepping stone to new opportunities in the future.

Over-the-Horizon Benefits

The SOC 2 process also offers over-the-horizon, indirect benefits that your business may enjoy long into the future. Prospective clients and partners will find your business more appealing, because they know you have policies and procedures that are defined, repeatable, scalable, and verifiable. For example, with a SOC 2 certification in hand, you may be able to skip typical hurdles such as a vendor questionnaire or a security review period, which can save weeks, if not months, as well as hundreds of back and forth emails, meetings, evidence requests, etc.

A SOC 2 certification paves the way for the achievement of further safeguards published by the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO), the Center for Internet Security (CIS), HITRUST, the Federal Risk and Authorization Management Program (FedRAMP), and more. These guidelines have many overlapping controls with SOC 2. Further, SOC 2 certification offers your business a strong foundation that can lead to more complex opportunities, such as data aliasing and tokenization.

SOC 2 Report Types

SOC 2: Type 1

A SOC 2 Type 1 audit evaluates the existence and design of a business's controls. A SOC 2 Type 1 report is often the first major milestone in achieving and maintaining SOC 2 compliance Type 2. However, if you are already confident in your control design, it is possible to skip a Type 1 altogether, and simply move straight to a Type 2.

As of a specific date, a SOC 2 Type 1 report proves to an auditor that specific organizational and technological requirements have been met. It provides your customers with a clear view of your business practices relative to the secure handling of their data.

During a Type 1 audit, your business must provide evidence to establish that it has an organization-wide compliance program, to include policies, properly documented technical controls, and verification procedures. For a Type 1 report, the volume of evidence required by an auditor is relatively low, as you only need to prove that the proper controls exist and are implemented correctly.

Once your first Type 1 audit and report are complete, there is no need to perform another Type 1 after the first. Thereafter, your business will perform periodic SOC 2 Type 2 audits. And it is a SOC 2 Type 2 report that most prospective customers, partners, and regulators are looking for.

SOC 2: Type 2

A SOC 2 Type 2 report evaluates the effectiveness of your organizational controls, and seeks to verify that they are functioning as intended. Whereas a Type 1 report references only a moment in time, a Type 2 audit and report evaluate evidentiary documentation that demonstrates the effectiveness of your controls over time.

The Type 2 report offers your clients a detailed, historic view of your SOC 2 compliance program for a specific, recent period of time (the audit period). The information required for a Type 2, which typically covers a period of 3-12 months, is greater than for a Type 1, because the latter only references a snapshot in time.

For the sake of efficiency, businesses often choose to undergo their first Type 2 audit shortly after completion of their Type 1 report. This decision may be driven by contractual obligations, when customers require proof that a business is capable of operating the compliance program which they outlined in a Type 1 report.

After its first Type 2 report is complete, a business typically schedules follow-on Type 2 updates based on their preferred cadence, so that it can maintain its SOC 2 compliance in the future.

SOC 1 & SOC 3

For background, here is a short description of SOC 1 and SOC 3 reports.

SOC 1 - SOC for Service Organizations: ICFR

A SOC 1 report evaluates the effect of business controls that are relevant to users' financial statements and the CPAs who audit them. ICFR stands for "Internal Control over Financial Reporting".

SOC 3 - SOC for Service Organizations: Trust Services Criteria for General Use Report

A SOC 3 report evaluates the same business controls as a SOC 2 Report, and is just as rigorous. However, a SOC 3 report is a pared down and less sensitive version of an organization's SOC 2 report, often created by the same auditor for an extra fee. Because it has far less technical detail, a SOC 3 report is usually intended for wider distribution than a SOC 2, typically for public release.

Trust Services Criteria

The AICPA Assurance Services Executive Committee (ASEC) created a list of Trust Services Criteria to evaluate the design and effectiveness of information system controls relevant to the following Trust Principles:

- Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy

The criteria may also be used to evaluate the processing of a particular type of information that is stored within a system.

For the purposes of a SOC 2 audit, it is mandatory to evaluate Security (Common Criteria), while the other Trust Criteria are optional.

Security (Common Criteria)

Security is the only mandatory Trust Principle in a SOC 2 audit. It seeks to assure that information and systems are protected against many types of threats, including:

- Unauthorized access
- Unauthorized disclosure of information
- Damage that affects the ability to achieve organizational objectives
- Damage that negatively affects the other Trust Criteria

Security refers to the protection of information during creation, collection, use, processing, transmission, and storage.

Security refers to the protection of electronic systems that store, process, transmit, or transfer information in support of organizational objectives.

Controls in this Trust Principle prevent or detect the breakdown of security threats, including data theft, software misuse, incorrect processing, system failure, circumvention of segregation of duties, and the improper access, alteration, destruction, or disclosure of information

Availability

The Availability Trust Principle refers to the uptime, performance, capacity, and operations of information systems. Your infrastructure must be ready to meet all of your organization's objectives.

At a minimum, the Trust Principle of Availability refers to the following three elements:

- Information accessibility for all of your products or services.
- System controls for monitoring and maintenance.
- The proper handling of customer data.

For even greater fidelity, Availability may include a certain acceptable level of performance, or a subjective review of a system’s functionality (e.g. usability for specific tasks or problem sets).

Processing Integrity

The Trust Principle of Processing Integrity seeks to ensure the trustworthiness of your information systems -- and by extension, the data held within them. It seeks to verify whether your systems are performing their intended functions, and achieving their intended purposes, in an unimpaired manner, free from error, delay, or omission.

Your organization's system processing should have the following characteristics.

- Complete
- Valid
- Accurate
- Timely
- Authorized

Processing Integrity encompasses a wide range of threats: misconfiguration, inadvertent mistakes, and unauthorized manipulation.

Today, modern organizations employ such a large number and variety of information systems that the Trust Principle of Processing Integrity is often focussed on information systems and services that are relatively close to the core of an organization.

Confidentiality

The Trust Principle of Confidentiality addresses an organization's ability to protect information, such as customer data, that is intended to be kept secret. There are many reasons for information confidentiality, including regulatory requirements, rapidly evolving legislation, contractual obligations, tacit understanding, proprietary data, and customer trust.

To support the Trust Principle of Confidentiality, an information custodian must protect information throughout its lifecycle, from creation or collection to classification, storage, modification, and destruction.

Information confidentiality is more important than your organizational objectives, and limits data usage in the following ways.

- Access
- Use
- Retention
- Disclosure

Often, information is restricted to parties who are specifically defined by mutual agreement. Further, it is common to limit access to specific information within an information system; in other words, some personnel who have authorized system access will not have access to all of the information within that system.

Confidentiality is different from privacy in that confidentiality applies to various types of sensitive information (including personal information, but also trade secrets and intellectual property), whereas privacy applies only to personal information.

Privacy

The Trust Principle of Privacy refers to the collection, use, retention, disclosure, and disposal of personal information in the pursuit of organizational objectives.

Privacy is subdivided into the following elements.

Notice and communication of objectives

- Data subjects are informed of organizational objectives and organizational privacy practices.
- For any changes to objectives or practices, this notice is updated and communicated to data subjects in a timely manner.

Choice & consent

- The organization documents its basis for determining consent.
- Data subjects are provided with available choices regarding the collection, use, retention, disclosure, and disposal of their personal information.
- If necessary, explicit consent is obtained from data subjects or other authorized persons.

Collection

- Personal information is collected in a manner that is consistent with organizational objectives related to privacy.

Use, retention, disposal

- The use, retention, and disposal of personal information is limited by privacy-related constraints, and consistent with the purposes identified in the organization's objectives related to privacy.

Access

- The organization grants data subjects the ability to access their stored personal information.
- Upon request, the organization provides physical or electronic copies of that information.
- The organization corrects, amends, or appends personal information, based on input provided by data subjects, and communicates all changes to third parties.
- If data access is denied, or if a request for data correction is denied, data subjects are informed of the denial, to include the reason for the denial.

Disclosure and notification

- The organization discloses personal information to third parties only with the explicit, prior consent of data subjects.
- The organization retains a complete, accurate, and timely record of authorized disclosures of personal information.
- Upon request, the organization provides this information to the data subject.

Disclosure and notification (cont.)

- The organization obtains privacy commitments from third parties with access to its personal information.
- The organization assesses third-party compliance, and takes corrective action if necessary.
- In the event of actual or suspected breaches, incidents, or unauthorized disclosure, the organization notifies affected data subjects and regulators in accordance with established incident-response procedures.

Quality

- All personal information is accurate, up-to-date, complete, and relevant to organizational objectives.

Monitoring and enforcement

- The organization implements a process for receiving, addressing, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others.
- The organization makes corrections in a timely manner.

Privacy is different from Confidentiality in that Privacy applies only to personal information, whereas Confidentiality applies to various types of sensitive information.

SOC 2 Audit Process

This section highlights the main areas that auditors examine during a SOC 2 assessment, as they attempt to determine your organization's state of compliance. It also presents ways that your organization can prepare for the audit — technically, operationally, and culturally.

SOC 2 auditors want to know that your business's information security and privacy controls are in place and can protect customer data. Many businesses find that how they approach the SOC 2 audit and report process is almost as important as the end result of achieving compliance.

Service Description

One of the first things you will do during a SOC 2 audit is to tell the auditor what your service does (and what it does not do). You must share a complete picture of your service, to include the following:

- On-premises hardware
- Cloud systems
- Applications
- Data sets
- Activities
- Transactions
- Data exchanges
- Storage
- Access control
- Logging

Audit Scoping

The next step, in coordination with your auditor, is to determine the scope of your SOC 2 audit. Its parameters are defined by the AICPA Trust Services Criteria:

- Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy

For a SOC 2 audit, the only mandatory Trust Principle to evaluate is Security. The other Trust Criteria are optional. Corporate requirements and contractual obligations will determine whether you add any or all of the other four Trust Criteria. Availability is currently one of the more common add-ons, while Privacy is growing in popularity.

Once an auditor understands your service and the scope of the audit, they will already have a good idea of what the final report should include. After that, it is up to you to help the auditor guide you along the path to SOC 2 success, with as few roadblocks as possible.

Policy Development

After you agree on the scope, your team will develop, implement, and tune policies and procedures that are sufficient to meet the operational requirements of the Trust Services Criteria. Everything should be documented, from security awareness training, to risk assessments, penetration tests, etc.

As relevant issues arise, it is important to address them sooner rather than later. Companies can pay a huge price for allowing even simple security measures to remain unaddressed for too long. During a SOC 2 audit, there are many issues that can potentially slow down or even derail a final report, each of which could touch on overlapping areas of scope.

A key aspect of policy management is articulation and communication. You must demonstrate policy documentation and distribution to all employees (including new hires), and every employee must verifiably confirm that they have read, agreed, and signed the policies. And in the future, if and when your operating environment changes, policies must also be updated to reflect the changes, and employee review and approval are required again.

Gap Analysis

SOC 2 auditors will collect evidence that allows them to assess and determine whether your controls, processes, technology, and employees are in compliance with your policies and the Trust Services Criteria. Inevitably, they will discover gaps that need to be documented, evaluated, and addressed. Often, one of the key areas of shortcoming lies in the interaction between your technology and the people who use it.

Ideally, you should think about this aspect of the SOC 2 process beforehand, and endeavor to identify these gaps before initiating your SOC 2 audit. This will give you an opportunity to address the gaps first -- before they are discovered by an auditor. An alternative is to create a clear action plan to close your gaps as soon as possible. In the latter case, proactivity is always viewed positively.

Depending on the severity of your gaps, an auditor may be forced to delay your report's completion. However, depending on your business partner, transparency, communication, and a strong action plan may be sufficient to proceed before a SOC 2 report has been completed.

Mitigation

During your SOC 2 audit, it is likely that some potentially harmful vulnerabilities will be discovered, or unforeseen security incidents will take place. Mitigation is the process of reducing the likelihood that either can negatively affect your business (in the past, present, or future).

Mitigation is an essential element of risk management. It encompasses both information technology and the people who use it. For software, vulnerability management is the process of identifying, classifying, prioritizing, and remediating vulnerabilities. For people, it is critical that your business enforce security concepts like social engineering awareness, and also test your employees on a periodic basis.

Whenever vulnerabilities are discovered, or security incidents take place, it is crucial that you mitigate the potential for harm, thoroughly document what you have done, and communicate your findings to auditors, customers, and partners, as soon as possible.

Culture

A successful SOC 2 engagement depends on clear management buy-in and communication. It is critical that senior leaders set the tone, directly from the top, about the importance of this initiative. Auditors, clients, and partners want to see and feel a positive workplace ethos relative to security and compliance.

Even the world's best set of controls ultimately rely on human operators. Employees should respond to security issues quickly, accurately, and effectively.

Culture (cont.)

Culture refers not only to the intersection of information technology and people, but also to achievements and rewards.

This is only possible when your workplace culture is ready and willing to accept it. In other words, problem-solving skills alone are insufficient; they also require a high level of morale before they can be put into action.

If an auditor gains a negative impression of your workplace culture, a critical foundation of the SOC 2 process is placed in jeopardy, as well as the timing or completion of your report. At a minimum, an auditor will likely seek to offset any doubts by requiring the collection of more evidence.

Trust

The ultimate payoff of investing in a SOC 2 audit is trust. During the certification process, your best chance to build a positive rapport with your auditor is to provide evidence that is “complete and accurate”.

After you have successfully completed your SOC 2 certification, trust will come not only from your auditor, but also from clients, partners, and investors. A SOC 2 report provides proof that your business, technology, people, processes, and products are in compliance with SOC 2 Trust Services Criteria.

VGS is SOC 2 Compliance, **Reimagined.**

VGS Control is the fastest way to get SOC 2 compliant and secure your data.

Only VGS combines the world's most powerful SOC 2 compliance automation with a data security solution in a single, easy-to-use platform. With VGS Control, you'll implement real security on Day 1 and build trust with a complete and accurate SOC 2 compliance report.

SOC 2 ready in weeks

Speed up your SOC 2 audit readiness by as much as 70% with a prescriptive program, automated evidence collection, and more.

Close more business

Turn your security posture into an asset, to build trust and win more business.

Reduce costs and increase accuracy

Replace manual checklists and spreadsheets with VGS scalable compliance automation.

VGS Control for SOC 2

Very Good Security is your true compliance partner — not a checklist. Only VGS provides a simple one-stop solution for centralized governance and automated enforcement of SOC 2 security controls. We integrate your entire technology stack and automatically enable a single source of truth for all of your compliance evidence.

- ✓ Most Automated Evidence Collection
- ✓ Best-in-Class Active Monitoring
- ✓ Automated Vendor Management
- ✓ Prescriptive Tasks
- ✓ Dynamic Policy Builder & Library
- ✓ Real-time Auditor Collaboration

A One-stop Solution for Compliance Automation

Best-in-Class Active Security Monitoring

VGS Control monitors your environment and compliance status in real-time.

- Track change in compliance status
- Manage your teams' audit progress
- Monitor specific controls and integrations

Automated Evidence Collection

Automate and enforce via one simple API.

- Integration with AWS, Github, Slack, Google Workspace, Jamf, and Rippling
- Secure sensitive data with VGS Vault integration
- Evidence automatically attached to SOC 2 controls

Real-time Auditor Collaboration

Say goodbye to checklists, mass exports and email strings. Work with auditors in real-time, directly on the Control platform.

- One-click evidence acceptance/rejection
- Convenient in-app messaging
- Real-time evidence generation

Automated Vendor Management

Easily audit and assess the security posture of your partners. Save countless hours compiling responses and manually calculating risk scores.

- Automatically send security questionnaires
- Centralize responses and management
- Quickly & easily assess vendor risk

VGS' compliance and security strategies are simple and transparent. We offer unparalleled automation and performance, in a plan that's right for you, and scales as you grow.

All VGS Control plans come with:

- ➔ Access to security configuration best practices
- ➔ Chat support for questions and troubleshooting
- ➔ Readiness Questionnaire & Remediation Plan
- ➔ VGS Docs advanced documentation library

Ready to Get Started?

Connect with a VGS compliance expert for a personalized compliance needs assessment. For more information, **click here.**

Sources

2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (TSP Section 100, Includes March 2020 updates), AICPA,
https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf.

SOC 1 - SOC for Service Organizations: ICFR, AICPA,
https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc1report.html.

SOC 2 - SOC for Service Organizations: Trust Services Criteria, AICPA,
https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html.

SOC 2 Audits: What Do Auditors Look For? Stefan Slattery, Very Good Security, June 24, 2021,
https://www.verygoodsecurity.com/blog/posts/soc-2-audits-what-do-auditors-look-for.

SOC 3 SOC for Service Organizations: Trust Services Criteria for General Use Report, AICPA,
https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc3report.html.

VGS Case Study: Accord https://www.verygoodsecurity.com/case-study/accord.

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.

SOC 2 Case Study

ACCORD

Accord Builds a Foundation for World-Class SaaS Security with SOC 2 Partner VGS

We are a world-class engineering team and a world-class company. From a security standpoint, that drove a lot of our urgency.

Wayne Pan,
Co-founder & CTO

VGS has an awesome name in terms of security. We felt they'd be great partners, and they have been. What I've really enjoyed about our engagement is the guidance and education they've provided around SOC 2

Ross Rich,
Co-founder & CEO

Full Case Study >

Client

Accord helps B2B sales teams move from vendorship → partnership. Its customer collaboration platform is built for high-growth sales leaders who need to hit scaling revenue targets and build a repeatable process. Accord ensures revenue teams are reinforcing a predictable sales motion that customers actually engage with and reps love to use.

Region	Industries
United States	SaaS, Sales, Software

Goal

Build a scalable, world-class SaaS company with security as a competitive differentiator.

Challenge

Finding a partner to help them understand SOC 2 compliance requirements, achieve SOC 2 certification quickly, and scale their compliance capabilities as the company grows.

Solution

VGS Control Compliance for SOC 2

Result

With VGS, Accord was able to prioritize security controls that would help them meet SOC 2 certification. Going through SOC 2 certification has allowed Accord to go upmarket and differentiate the company from 100% of its competitors.