rewind

SOC 2 at Rewind: We Will, We Will, SOC 2!

Introduction

If your company or a third party you work with is responsible for handling and storing customer data, how do you ensure your clients' data will be kept safe? More importantly, how do you communicate your commitment to protecting your clients' data to potential new customers?

SOC 2 is a framework applicable to all technology service or SaaS companies that store customer data in the cloud to ensure that organizational controls and practices effectively safeguard the privacy and security of customer and client data.

As of June 2021, Rewind is now proudly SOC 2, Type 1 compliant. The process of obtaining and complying with SOC 2 was a lengthy process that required the entire team's buy-in. Here's what we learned along the way.

Why SOC 2?

Before we dive into the details, let's discuss why your organization might choose to pursue a SOC 2 report.

First of all, it can greatly expand your target market. SOC 2 compliance is necessary for service providers working in highly regulated fields or with clients who are publicly traded companies, to be seen as a viable vendor for hire. Attaining a SOC 2 report is an excellent way to unlock these new markets.

SOC 2 reports also help you build trust in the minds of your customers. The SOC 2 report will show prospects and current customers you're committed to protecting their clients and their own interests. The SOC2 report gives prospects confidence their data is being protected and you aren't a possibility for introducing vulnerabilities into their systems via integrations. Being SOC 2 compliant assures your customers and clients that you have the infrastructure, tools, and processes to protect their information from unauthorized access both from within and outside the firm.

SOC 2 reports also help businesses to pre-emptively mitigate risks in today's cybersecurity landscape. Being SOC compliant will give you a head start if your business should become the victim of a cyberattack. Often, data breaches trigger fines, reputational damage, loss of customers, a deflation of stock prices, and so much more. SOC compliance can go a long way in mitigating these losses. A compliant business is more likely to respond to a breach quickly, thus limiting its impact.

What is SOC 2?

Disappointingly, SOC 2 has nothing to do with socks. SOC stands for Service Organization Control; businesses can receive a SOC 1, a SOC 2, or even a SOC 3 report. SOC 1 reports deal with financial data, and SOC 3 reports are non-confidential public versions of SOC 2 reports. A SOC 2 report is the most commonly used, so that's what we'll be covering in-depth today.

A SOC 2 report is essentially a way to tell the world that you care about keeping your customer's information safe and secure. After a SOC 2 audit has been performed by an accredited auditor, an organization can share its SOC 2 report with different stakeholders such as potential customers, other auditors, or investors.

A SOC 2 report is basically a report card, where an auditor has checked that the company is actually performing appropriate data protection procedures. The five different trust services principles form the basis of the entire SOC 2 report. Note that not all five categories always apply; if your company doesn't handle customer data, you don't need to worry about the privacy criteria, for example.

Megan Dean, Information Security and Risk Compliance Manager at Rewind, agrees on the importance of a strong security program. "If you don't have a formalized security program, you'll eventually be asked by an auditor to prove something you don't have. And then those red flags will start to show up in your SOC 2 report."

The five different trust service principles are broken down into broad categories:

1. Security
2. Availability
3. Processing Integrity
4. Confidentiality
5. Privacy

You can be audited on one or a combination of the trust services principles. For example, Rewind was audited on the Security and Confidentiality controls. Security is the only mandatory principle that you must be audited on. Let's dive into the five trust service criteria in a bit more detail.

Criteria

SECURITY CRITERIA

According to the AICPA (the organization that designs the SOC 2 Trust Services Criteria and regulates SOC auditors), "security" refers to "information during its collection or creation, use, processing, transmission, and storage". It also includes all systems that use electronic information to "enable the entity (e.g. your business) to meet its objectives." That means that not only are your own internal processes under scrutiny, but every other third-party application, tool, or SaaS product should also comply with SOC 2 security requirements. This is a confident demonstration that your customer data is handled securely throughout your supply chain.

PRIVACY CRITERIA

Privacy is another seemingly obvious criterion that is nonetheless vital. Privacy ensures that "personal information is used, collected, retained and disclosed to meet the entity's objectives." While confidentiality applies to various types of sensitive information, such as financial data or health records, privacy applies only to personal information you have collected about or on behalf of customers and/or clients.

In a very nutty nutshell, those are the trust service criteria that each cover a set of internal controls that SOC 2 auditors assess. Of course, there's a lot more detail to know about each, so be sure to investigate fully before beginning the SOC 2 audit process.

AVAILABILITY CRITERIA

The availability trust service principle means that your systems must be ready and able to run as expected based on your operating agreements with customers and/or users. Essentially, it aims to answer a single question: can I rely on this service being available to me when I need it?

Availability criteria often involve a documented business continuity and disaster recovery plans and procedures. Potential customers will want to know what your plan is in the event of an emergency. The availability criteria also require periodic backups and recovery tests of business-critical applications.

PROCESSING INTEGRITY CRITERIA

Industries where the accuracy of information processed is vital, such as services that perform financial transactions or data analytics for their customers, often consider covering processing integrity in their SOC 2 report. Basically, this criteria asks the question: how do you ensure that the information you are processing is complete, valid, accurate, timely, and authorized?"

CONFIDENTIALITY CRITERIA

This criterion is pretty basic: information designated as confidential is protected. The level of protection will depend on the type of information and industry: for example, data related to health care falls under more stringent regulations known as HIPAA.

Control your Controls

In the context of SOC 2, a control has a very specific meaning. A *control* is *a policy, process, or procedure that is created to achieve a desired event or to avoid an unwanted event*. For example, Rewind uses a number of security-related controls such as requiring employees to use multi-factor authentication.

SOC 2, Type 2 – too?

There are actually two different types of SOC 2 reports: an organization can be SOC 2 Type 1 compliant or SOC 2 Type 2 compliant.

Type 1 can be thought of as a point-in-time audit. A Type 1 report focuses on the design of a company's controls. An auditor will look at a control and check that the control is designed well alongside the trust principles, and then request evidence to show that this control is actually in place. For example, one of Rewind's controls is that user access reviews are performed quarterly. We were required to demonstrate that this process is in place and provide proof that a user access review has been performed in the last quarter.

A Type 2 Report not only covers the design of a control, but also the operational effectiveness of that control. So not only does an organization need to show that it has controls in place, but that they are followed, they get the results they need from it, and it is successfully baked into their processes. This is typically proven by providing evidence over a specified period of time called an observation period (usually 6 months to a year) rather than a one-shot piece of evidence such as in the Type 1 report. To continue with our earlier example, in our Type 2 audit, Rewind will demonstrate that user access reviews have continuously been performed on a quarterly basis over that Type 2 observation period.

If a Type 1 report is a point-in-time report, a Type 2 report is more like an ongoing performance review. Remember, Type 1 is a singular piece of evidence, like doing well on a particular test, whereas Type 2 is ongoing, like continuously good performance on all of the tests throughout a school year.

What is Business-Critical?

Business-critical is a term that SOC 2 auditors use to describe applications, equipment, processes, or even people that are required for your business. An espresso machine would be considered business-critical to a coffee shop, for example (as well as some quality beans).

A good rule of thumb is to ask yourself: "am I able to service my customers without (blank)?" If the answer is "no", then "(blank)" should be considered business-critical.

For example, Rewind's ability to backup and restore customer's data (over two petabytes worth!) is definitely business-critical. Our auditors checked a variety of our controls to ensure our systems are being built securely, regularly backed up, and protect customer data from unauthorized access.

"If you have to prove to an auditor that a particular process is taking place, and you've got one place where that process takes place, you need to make sure that's always accessible. You need to make sure that you can go back and prove that those processes did in fact happen", explains Dean.

Find Your Missing SOC

Becoming SOC 2 compliant is a great way to internally improve your organization's security while externally communicating to customers and stakeholders that you value their data's privacy and security. It's also a great way to open your business up to more heavily regulated industries such as IT, financial services, or healthcare.

But, it's important to remember that SOC 2 isn't the end of your security journey - it's the beginning.

"There's no such thing as '100% secure' in today's threat landscape", explains Dean. "While your security posture may be strong, it can always be improved. Implementing good security controls now can prevent future headaches, but just because you have controls in place doesn't mean you are completely 'safe'. Wearing a seatbelt makes for a safer car ride - but it doesn't mean you also don't have to obey the speed limit and pay attention to your surroundings. Similarly, in cybersecurity, you must always remain vigilant against emerging threats."

A secure data backup and recovery strategy is an essential security control. Rewind provides peace of mind with automated daily backups and effortless recovery.

Questions?

If you have any questions, please don't hesitate to contact us at team@rewind.com! We're here to ensure that you're successful and help you back that SaaS up.

START FREE TRIAL

rewind