rewind

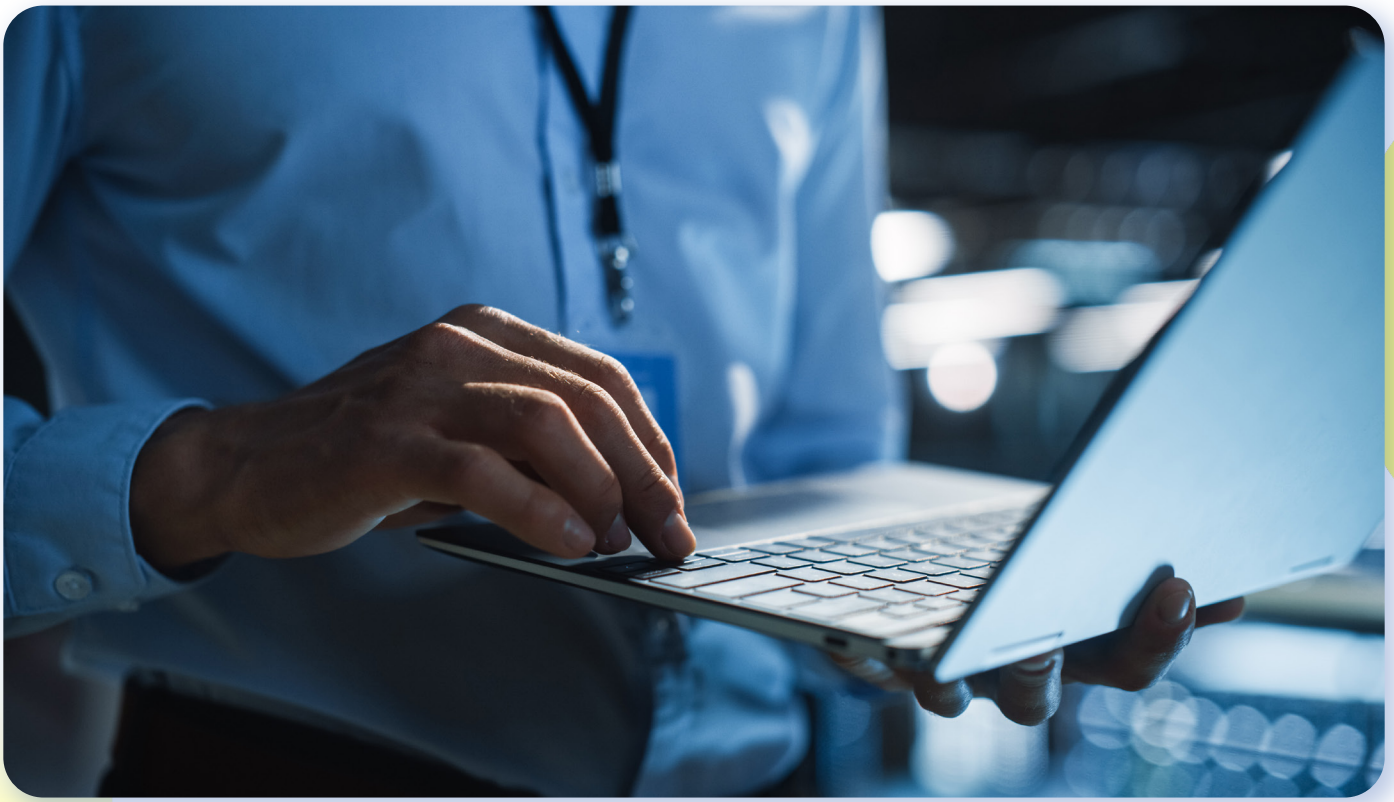
How SaaS Companies Can Achieve SOC 2 Compliance

SOC 2 is a standard developed by the American Institute of Certified Public Accountants (AICPA), and is designed to provide assurance about a company's information security policies, particularly those around the safeguarding and security of client data.

The assessment takes the form of an auditor's attestation report, and provides detailed information about a company's adherence to one or more of five trust service principles: security, availability, processing integrity, confidentiality, and privacy. In other words, you have to show, via documentation and demonstrations, that you're acting in good faith with other people's information.

There are two types of SOC 2 compliance, type 1 and type 2. The two types are complementary, and type 1 is often used as a stepping stone to type 2. Type 1 compliance is a point-in-time audit, and demonstrates that privacy and security controls are in place and well designed. Type 2 is a longer-term process (usually six to twelve months) that demonstrates the effectiveness of those controls in a real-world environment.

SOC 2 compliance is a voluntary standard. You don't have to have it—unless you're hoping to break into highly regulated industries, or want to build trust with customers, or improve your organizational security. Compliance shows that you take security seriously, and that you're willing to stand behind the controls that you've put in place.



While SOC 2 compliance can be hugely beneficial, it's also a major commitment, and requires buy-in from your whole team. There's not a checklist where you can simply follow the steps and, when you reach the end, you're compliant. One of the lightbulb moments for Rewind as we pursued compliance was when we realized that the controls weren't a set of strictly defined rules we had to follow, but rather a flexible framework that allowed us to develop our own controls and implementations.

The SOC 2 standard is unique in that it's entirely customizable. It allows you to choose what you want to pursue—from just security, the only mandatory principle, to all five—as well as how you'll pursue that specific outcome. In addition to the time required to create and implement security procedures, it also requires a significant amount of time up front spent thinking about what you want to achieve, and what your desired outcomes look like.

As of October 2021, Rewind is proudly SOC 2, type 1 compliant. The process reaching SOC 2 compliance was lengthy, and required the entire team's buy-in. In this book, we'll share what we've learned along the way.

SOC 2 compliance isn't a destination, but an ongoing journey through the security landscape. While there isn't a map, we hope that our experience can serve as a guide.

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. As a whole, both private and public sector groups are becoming more conscious about how their proprietary data is handled by other parties. For highly regulated industries such as finance, healthcare, or publicly traded companies, SOC 2 compliance has essentially become a cost of doing business. For SaaS companies that want to "grow up" and sell to big brands, the question "Do you have your SOC 2?" will be one of the first things your sales team gets asked.

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

Today's cybersecurity landscape is rough, and SOC 2 reports can provide assurance to customers and stakeholders. The volume of cyberattacks is increasing every year. A security breach can trigger fines, damage a company's reputation, cause an exodus of customers, or even drive a company out of business. SOC 2 compliance mitigates losses from these scenarios by ensuring that you have key protection processes in place. A compliant business is more likely to respond to a breach quickly, thus limiting its impact.

What is SOC 2?

SOC stands for Service Organization Control; businesses can receive a SOC 1, a SOC 2, or a SOC 3 report. SOC 1 reports deal with financial data, and SOC 3 reports are public, non-confidential versions of SOC 2 reports. A SOC 2 report is the most commonly used, so that's what we'll be covering in depth in this book.

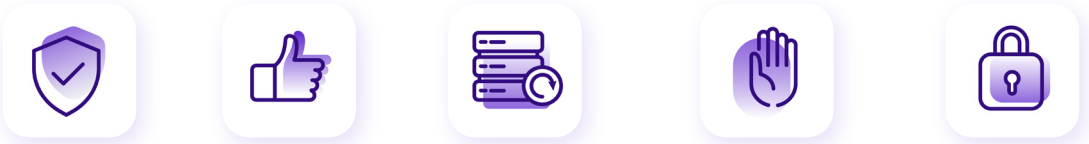
A SOC 2 report is a way to tell the world that you care about keeping your customer's information safe and secure. After a SOC 2 audit has been performed by an accredited auditor, an organization can share its results with stakeholders such as potential customers, other auditors, or investors.

A SOC 2 report is basically a report card where an auditor grades the company's performance of appropriate data protection procedures. The five different trust service 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 criterion.

You can choose to be audited on one or a combination of the trust service principles. For example, Rewind was audited on the security and confidentiality controls. Security is the only principle that you must be audited on.

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 red flags will start to show up in your SOC 2 report. That's why a strong security posture around all five trust service principles is essential.

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



Security | Availability | Processing Integrity | Confidentiality | Privacy

Security

According to the AICPA, *"security"* refers to the protection of *"information during its collection or creation, use, processing, transmission, and storage"*. It also includes all systems that use electronic information to *"enable [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 you use also needs to comply with SOC 2 security requirements. This is a confident demonstration that your customer data is handled securely throughout your supply chain.

Availability

The availability trust service principle means that your systems must be ready and able to run as described in 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?*

The availability criterion often involves 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. This criterion also requires periodic backups and recovery tests of business-critical applications.

Processing Integrity

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. The processing integrity criterion asks the question: *How do you ensure that the information you are processing is complete, valid, accurate, timely, and authorized?*

Confidentiality

This one is pretty basic: information designated as confidential needs to be 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.

Privacy

Privacy is another seemingly obvious criterion that is 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 to the personal information you have collected about or on behalf of customers and/or clients.

In a nutshell, those are the trust service criteria, each covering a set of internal controls that SOC 2 auditors assess. Of course, there's a lot more detail to know about each, which you should investigate fully before beginning the SOC 2 audit process.

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.

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 to operate. 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 back up and restore customers' data (over two petabytes worth!) is definitely business-critical. Our auditors checked a variety of our controls to ensure our systems are 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 Megan Dean, Rewind's Information Security and Risk Compliance Manager.

If a type 1 report is a point-in-time report, a type 2 report is more like an annual performance review—an assessment of how well you've maintained compliance through the entire observation period.

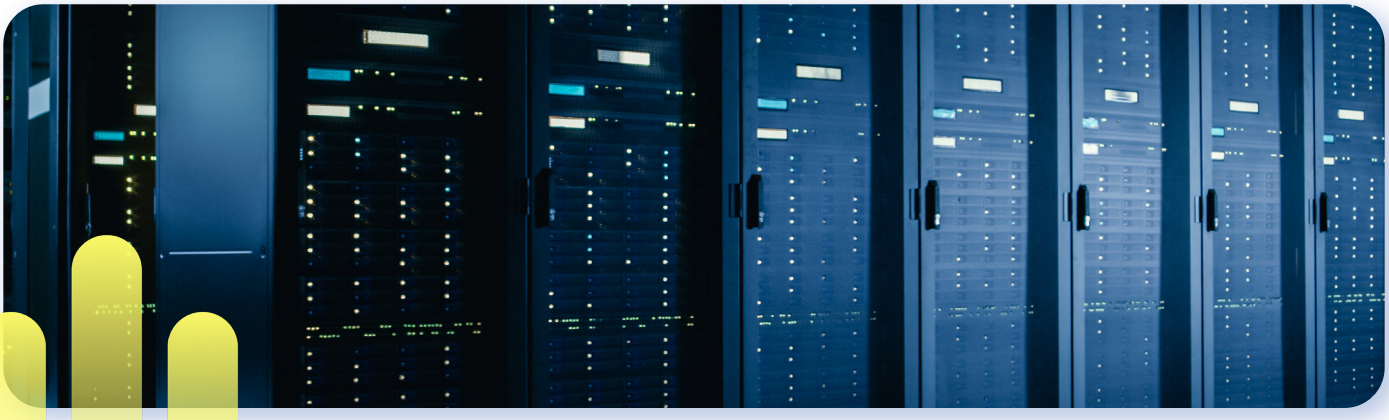
Getting SOC 2 the Swift and Smart Way

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

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. 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're completely "safe" and never have to think about them again. Wearing a seatbelt makes for a safer car ride—but it doesn't mean you don't also have to obey the speed limit and pay attention to your surroundings. Similarly, in cybersecurity, you must always remain vigilant against emerging threats.

Before Rewind began pursuing SOC 2 compliance, we had some processes in place, such as change management procedures for when emergency fixes need to be released to production quickly. But after beginning our SOC 2 journey, we realized that to be SOC 2 compliant and audit ready, they needed to be formalized.

Achieving SOC 2 can be an intimidating task. Once you've made the decision to pursue it, the next step is understanding your company's SOC 2 goals and priorities, and identifying what steps need to be taken to become compliant. Here's a quick framework to help you get prepared for the road ahead.



Choosing Your Scope

The first step is to decide on the scope of your audit: what service or product will be the focus, and what trust service principles you want to include in your auditing. Security is a mandatory principle, but you can also include confidentiality, availability, processing integrity, or privacy principles.

The service you provide to your customers can determine what trust service principles to focus on. For example, if your company processes financial data, "processing integrity" is an important principle to showcase.

Rewind provides SaaS backups, so the scope was our own software platform. For our first SOC 2 certification, the focus within this scope was on security and confidentiality controls. Confidentiality was an important principle, since customers are trusting us with their backup data, and we want to demonstrate how we ensure the confidentiality of the information entrusted to us.

It's important to remember you can start with a limited scope, and expand to include other trust service principles in future audits. Your SOC 2 compliance program and internal processes can be extended to integrate new principles when you're ready.

Assessing Your Level of Controls

Requests from the sales team can help you determine what trust service principles to focus on, but that doesn't mean you can start the audit process tomorrow. Before going ahead with the SOC 2 certification process, it's best to complete a readiness assessment. This helps establish a benchmark of what controls you already have in place, and allows you to identify the areas that need to be focused on.

You can find readiness assessment documents on the web from third parties, or visit the AICPA website to read about requirements yourself. Many auditors will help you with your readiness assessment as part of your engagement.

As an added bonus, a readiness assessment can help you understand how to better budget for your SOC 2 program going forward. For example, if you need to perform a third-party penetration test on your application, or invest in an employee background check process, you'll need to budget for those costs.

Choose and Train Control Owners

Control owners are individuals in your business responsible for the implementation and ongoing compliance of your controls. They should be involved in designing the controls and processes needed to become SOC 2 compliant. These controls should be woven into the team's everyday processes, allowing them to perform their jobs normally while still meeting the control objectives.

New processes should be an improvement to a process or control related to one of the trust service principles you're seeking compliance with. Rewind took a collaborative approach that was led by our "Trust Team", but empowered control owners to be responsible for their own areas of compliance. SOC 2 needs to be a goal for your entire company, not just the security team.

Organizing Controls and Evidence Collection

There's no wrong way to organize your SOC 2 compliance program and controls. In the long run, though, there are approaches that make achieving and maintaining compliance easier. Many people default to using spreadsheets to keep track of controls, owners, record notes, and links to evidence, all of which will be needed for your audits, but this quickly gets messy and difficult to monitor.

At Rewind, the longevity of our SOC 2 compliance program was a crucial consideration in our decision-making. Control ownership and evidence collection needed to be centralized and accessible to all stakeholders. To do this effectively, we invested in a security assurance platform to help us manage our compliance program. Part of your SOC 2 budget should be allocated for a tool that can help you organize your controls and monitor them going forward.

It's easy to be sucked in by companies who advertise compliance solutions with promises like "Get SOC 2 in two months!", but a compliance program should be a machine that keeps going, not a race to the finish line. It's important to choose a tool that takes a sustainable, long-term approach to compliance.

Consider a Type 1 Report Before a Type 2

A SOC 2 type 1 audit is a good way to get your feet wet in the SOC 2 audit process. The SOC 2 type 1 report is a strong signal of your commitment to your compliance program, and the process allows you to develop a working relationship with your auditor—and to approach your type 2 audit with confidence.

Thinking about how SOC 2 controls can become an everyday part of your team's workflow will save you a world of headaches in the future. Creating a culture inclusive of security best practices such as role-based access control, backups and recovery plans for critical data, an infrastructure-as-code model, and continuous code auditing will not only strengthen your security stance, but will also bring you that much closer to achieving SOC 2 compliance.

Choose Your Auditors

There are many reputable CPAs out there to perform your audit for you, but different auditing companies offer different services. At Rewind, our choice of auditor (Moss Adams) is recommended by and trained to use our security assurance platform (Tugboat Logic), which we use to manage our SOC 2 program. This allows us to manage the compliance of our entire program, including providing evidence to our auditors, in the same tool. This reduces the workload of our control auditors and provides a centralized place to manage our controls, evidence collection, and audits.

When selecting auditors, you need to choose a reputable CPA who is open to working with you and your workflows. This should be a collaborative relationship, where you're able to ask for advice and know that they want to be a part of your success.

Continuous Code Auditing for SOC 2 Compliance

With the increased adoption of continuous deployment, many organizations have increased their deployment frequency in order to get product improvements into the hands of their customers as quickly as possible. A complement to this fast-paced deployment practice is continuous auditing. Both of these approaches constitute a leftward shift from the more traditional methodologies of software development.

This increased rate of deployment can lead to the occasional need for an emergency hotfix. Like many organizations, Rewind uses GitHub to build and deploy our software. In some cases, emergency fixes are required to avoid real-world consequences, such as downtime or the degradation of services. Having these changes documented as code, rather than manipulating resources in a web console, is preferred. In many cases, mean time to repair is a more useful metric than mean time to resolve. An emergency hotfix can solve the problem immediately, allowing for the appropriate retrospective to be spent on working towards a longer-term solution to the underlying problem.

At Rewind, we follow a change management process as part of SOC 2 compliance. This process allows for emergency changes, whereby changes can be approved without the usual number of reviews for the change. There are times when an emergency fix may need to be released to production quickly, but changes made by production engineers in emergency situations should be audited.

Working in conjunction with our SOC 2 auditor, we have developed (and open sourced) tooling that leverages GitHub's search syntax to scan pull requests within a specified time window. If any pull requests are found by the search query, they're logged in AWS CloudWatch Logs, and the relevant CloudWatch Alarms are sent to SQS, then picked up by our operations team.

This notifies us of any emergency changes, so we can track the reason for the change (required for SOC 2 auditing) and triage them if necessary. It allows us to trust but verify, and also retain these records for an extended period of time, since GitHub only stores audit logs for 90 days. SOC 2 and many other security certifications require a well-documented change management process and procedure, including how to deal with emergency changes and how these changes are audited.

How to Set Up a Continuous Code Monitor

The solution uses AWS SAM and its CLI to build, package, and deploy an AWS Lambda (written in Ruby). To reduce the size of the package, we leveraged AWS Lambda layers to package up our dependencies separately.

See the following CloudFormation snippet:

```
AuditorLambdaFunction:
Type: AWS::Serverless::Function # More info
about Function Resource: https://github.com/
awslabs/serverless-application-model/blob/master/
versions/2016-10-31.md#awsserverlessfunction
Properties:
CodeUri: src/
Handler: lambda.handler
MemorySize: 384
ReservedConcurrentExecutions: 1
Role: !GetAtt LambdaRole.Arn
Runtime: ruby2.7
Timeout: 300
Layers:
- !Ref AuditorLambdaLayer
Environment:
Variables:
GITHUB_ORG_NAME: !Ref GitHubOrgName
GITHUB_TOKEN_SSM_PATH: !Ref GitHubTokenSSMPath
LAST_TIME_CHECKED_SSM_PATH: !Ref LastTimeCheckedSSMPath
Tags:
function: github-pr-auditor
service: common
platform: common
lambda: github-pr-auditor
region: !Ref AWS::Region
AuditorLambdaLayer:
Type: AWS::Serverless::LayerVersion
Properties:
LayerName: github-pr-auditor-dependencies
Description: Dependencies for github-pr-auditor
ContentUri: lambda_layer
CompatibleRuntimes:
- ruby2.7
RetentionPolicy: Retain
Metadata:
BuildMethod: makefile
```

As you can see on the left, the function is dependent upon a single layer called AuditorLambdaLayer. The layer is packaged up separately and contains all of the dependencies defined in the Gemfile.lock necessary to run the application. One caveat we ran into was that SAM does not package up Ruby gems (for Lambda layers) in a way that the Lambda runtime is expecting. Luckily, we found this issue, and were able to work around it by reorganizing the files in the layer by making use of a custom makefile.

After ensuring that the Lambda itself ran as expected, we set up an AWS Events Rule to run the Lambda on a schedule. The following CloudFormation snippet defines this:

```
LambdaSchedule:
Type: “AWS::Events::Rule”
Properties:
Description: >
A schedule for the Lambda function.
ScheduleExpression: !Ref LambdaRate
State: ENABLED
Targets:
- Arn: !Sub ${AuditorLambdaFunction.Arn}
Id: LambdaSchedule
```

Schedule Expressions for Rules can be defined as strings such as “rate(24 hours)” or “rate(5 minutes)”, depending on how frequently you want to run the code.

The last piece of the puzzle was to ensure that alarms would notify us when a certain type of log appeared.

```
EmergencyChangeAlarm:
Type: AWS::CloudWatch::Alarm
Properties:
AlarmName: !Ref AlarmEmergencyChangeName
AlarmDescription: A GitHub PR emergency change was
merged
MetricName: GitHubEmergencyChange
Namespace: GitHubAuditing
Statistic: Sum
Period: 300
EvaluationPeriods: 1
Threshold: 1
TreatMissingData: notBreaching
AlarmActions:
- !Ref AlarmSNSTopicArn
ComparisonOperator: GreaterThanOrEqualToThreshold
EmergencyChangeFilter:
Type: AWS::Logs::MetricFilter
Properties:
LogGroupName: !Ref LambdaLogGroup
FilterPattern: |-
“is non-compliant!”
MetricTransformations:
- MetricValue: “1”
MetricNamespace: GitHubAuditing
MetricName: GitHubEmergencyChange
```

We consider this type of alarm to be an “Emergency Change”. It matches the text “is non-compliant!”, which is configured as a MetricFilter. These alarms then get sent to the configured AWS SNS topic, allowing for our operations team to be notified in a timely manner.

More Advanced Auditing

If you’re lucky enough to have a subscription to GitHub Enterprise, there are additional methods for auditing changes, such as querying GitHub’s Audit Log API. There are good examples in The GitHub Enterprise Audit log API for GraphQL beginners. This enables a far more granular approach to auditing, allowing for many other types of actions to be monitored as well.

Considerations on the Way to SOC 2 Compliance: What We Learned, So You Don't Have To

- **Preplanning**
- Spend time thinking about the course you need to take to achieve the outcomes you want.
- Clearly define what you're trying to achieve.
  - Are you seeking SOC 2 type 1, or SOC 2 type 2?
  - Establish the scope of the audit—what products or services will be included?
  - Which of the trust service principles will you be seeking compliance with?
- Choose a single person to spearhead the process. Hire someone who knows what they're doing, and let them do it.
- Set a realistic timeline, allowing plenty of time for remediation.
- Prepare yourself for the financial impact. SOC 2 compliance can be expensive.
  - Auditor costs
  - Background checks
  - Employee training
  - Remediation costs
  - Security assurance platform or services
  - Vulnerability testing
- Select an auditor.
- **Readiness Assessment**
- Readiness assessments can be done internally, or with the assistance of an external compliance specialist or auditor. Some firms will include a readiness assessment as part of their audit.
- Review existing documentation. The more well documented you are, the easier the certification process is likely to be.
  - Access control
  - Backups
  - Change management procedures
  - Contractor, vendor, and cloud provider documentation
  - Data integrity verification systems
  - Data protection policies
  - Disaster recovery procedures
  - Employee management documentation
  - Network security controls
- Identify gaps in your existing procedures.
  - Areas with no existing documentation
  - Places your security stance could be strengthened
- Develop a remediation plan. Depending on the results of your assessment, this may include creating new policies, developing or strengthening procedures, hardening infrastructure, finding replacements for insecure services, and third-party testing.
- **Remediation**
- Allow plenty of time for this step. You may need to try multiple approaches before you find one that works for your organization.
- Follow your remediation plan.
- Reassess your position regularly to ensure that the organization as a whole remains compliant.
- **Undergo the audit**
- **Going forward**
- Automate as much as possible for consistency and maintaining compliance.
- Integrate best practices into everyday work.

Wrapping Up

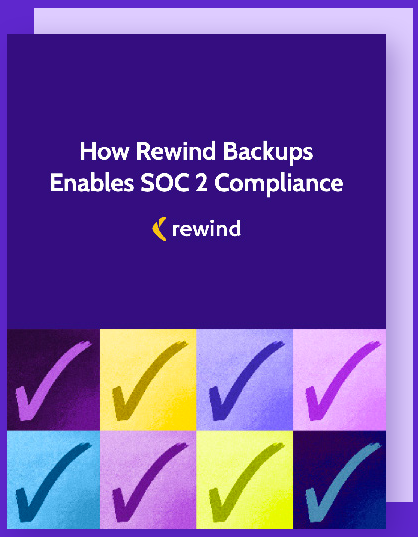
SOC 2 compliance can be difficult, but following the practices and procedures in this book will ensure that you start off on the right foot. Another thing to consider is your traveling companions—the tools you choose to bring with you on your journey towards compliance.

For SaaS companies, a crucial aspect of SOC 2 compliance is having a solid data backup strategy. Rewind offers automated data backup and restoration services, and seamlessly integrates with popular platforms like GitHub and Jira.

Free Resource

We put together this checklist to help guide you on how Rewind Backups for GitHub can help regarding each SOC 2 criteria we've addressed in this document.

Download →



Questions?

Get a quote, or schedule a demo to learn more about how Rewind can help you. Reach out to sales@rewind.com for more information.

START FREE TRIAL

rewind