THE ULTIMATE GUIDE TO SOC 2

BEMO

LAST UPDATED: MAY 2024

A comprehensive guide for SMBs to understand and prepare for the SOC 2 Audit and Attestation.

Introduction

Have you found yourself at a crossroads in your compliance journey where questions seem to multiply faster than answers? The pressure mounts as your SMB urgently requires compliance to secure vital deals, but the question lingers: where does one even start?

This daunting process seems to be tailored for larger enterprises. It's a predicament that many small and medium-sized businesses face.

The question here is clear:

How do SMBs attain SOC 2 compliance?

We've heard your concerns and witnessed your determination to safeguard your operations. That's why we've crafted this eBook with a clear goal in mind- to simplify, demystify, and empower.

Our eBook is your SOC 2 tour guide, designed to break down the SOC 2 compliance process into comprehensible parts. We'll show you what to expect, highlight tips to reduce timelines and flatten learning curves, and explain the SOC 2 process *without* the compliance jargon.

With our expert insights and practical tips, you'll transform SOC 2 from an intimidating hurdle into an achievable milestone.

With BEMO, SOC 2 compliance is not a distant dream but an achievable reality.

Ready to dig in? »

Table of Contents

5 What is SOC 2?

14 What to Expect From the SOC 2 Audit

25 The Costs of SOC 2 Compliance

29 Preparing for an SOC 2 Audit

34 Post Compliance: Now What?

Section One:
What is SOC 2?

What is SOC 2?

Before we dig into the “how,” “when,” and “how much,” we need to be on the same page about what SOC 2 is and why it is important. If you want to stand out from the crowd of competitors and attract more customers, you need to prove that you care about data security and privacy. SOC 2 is the best way to do that.

SOC 2, or Service Organization Control 2, is a comprehensive set of standards established by the American Institute of Certified Public Accountants (AICPA).

AICPA Service Organization Control Reports

AICPA

SOC 2

Formerly SAS 70 Reports

These standards are designed to assess and evaluate how effectively a service provider manages critical aspects of data security, availability, processing integrity, confidentiality, and privacy for its customers' data.

In the context of an SOC 2 audit, businesses must demonstrate the effectiveness of their policies, procedures, and systems in safeguarding information across these five crucial categories.

An independent auditor reviews the evidence provided for controls in each category, and when completed, you receive your official SOC 2 attestation report. This report serves as a testament to the organization’s commitment to data protection and can be shared with customers and partners, instilling trust and confidence in your organization’s brand.

Why is SOC 2 Important?

By successfully attaining SOC 2 compliance, an organization signals its commitment to robust risk management practices. This entails the ability to systematically identify and promptly address vulnerabilities, ensuring the safeguarding of sensitive data from potential threats.

However, the significance of SOC 2 extends far beyond internal security measures. It serves as a powerful badge of trust and reliability in the competitive market. SOC 2 compliance reassures customers, stakeholders, and partners that your business is not only well-established but also exceptionally reliable in its operations.

Competitive Advantage

Data Breach Protection

Long-term Savings

Enhance Brand Reputation

Boost Employee Morale

Improve Efficiency

IA SOC 2 Attestation signifies that you have undergone a rigorous evaluation of your security controls, attesting to your proactive stance in protecting vital information.

Visit BEMO's Article on Why Should SMBs Care About SOC 2 Compliance

LONG-TERM SAVINGS OF TIME AND MONEY

Completing SOC 2 certification will make it easier to attain other security certifications. You will save time filling out different security questionnaires for every large customer. These questionnaires can be incredibly detailed and difficult to fill out if you do not already have processes and documents in place.

REDUCE THE RISK OF DATA BREACHES

You will have a robust system of controls and policies that will protect your data and assets from threats. You will also have less downtime and more productivity, as you will be able to handle any issues quickly and efficiently.

ENHANCE YOUR BRAND REPUTATION AND CREDIBILITY

Customers, partners and investors will see you as a reliable and secure provider of services, and they will want to do more business with you. You will also avoid any nasty lawsuits or fines that could ruin your reputation. And yes, you get to display the SOC 2 seal logo on your website!

GAIN COMPETITIVE ADVANTAGE

Demonstrate your commitment to quality and excellence, and beat out competitors who might not have an SOC 2 report.

BOOST EMPLOYEE MORALE

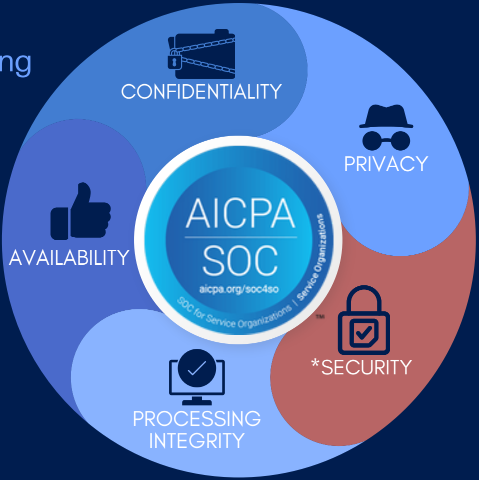
Your employees can feel proud of working for a reputable and responsible organization that values their data and privacy.

IMPROVE YOUR OPERATIONAL EFFICIENCY AND PERFORMANCE

You will improve your performance and efficiency by streamlining your processes and operations. You will have clear goals and objectives, and you will be able to continuously measure and monitor your progress and results, ultimately leading to reduced operational risks and costs.

Trust Services Criteria (TSCs)

The Trust Services Criteria (TSC) serves as the foundation for assessing and enhancing your cybersecurity posture. These criteria encompass a range of essential elements, including risk assessment, risk mitigation, risk management, organizational control, and change management. They are applicable across various dimensions of your operations, including Infrastructure, Software, People, Procedures, and Data.



*When undertaking an SOC 2 audit, Security is the sole **mandatory** TSC for all SOC 2 reports. Businesses have the flexibility to select which of the other four TSC they wish to incorporate into the evaluation. You mix and match depending on the services your organization provides.

Selecting which Trust Services Criteria to apply is crucial to defining the scope of your SOC and the system boundaries – the decision shouldn't be taken lightly. It's always a good idea to consult with a compliance expert when making these decision.

We understand that each business is unique, and your compliance needs may evolve with your services and expansion plans.

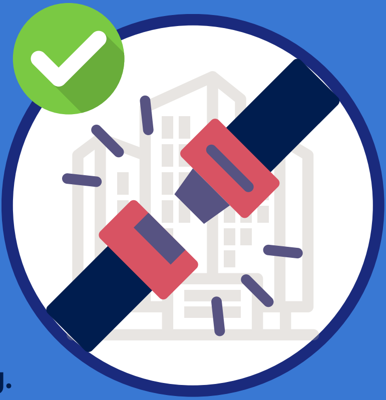
That's why our dedicated compliance experts work closely with you, conducting personalized consultations. During these collaborative sessions, we delve into the specifics of your business operations and future goals.

Through these discussions, we identify the most relevant Trust Services Criteria (TSC), review the individual requirements under each control, assess your current controls, and develop an action plan for controls that will need to be put in place to satisfy the relevant requirements.

Not familiar with "controls"? We got you. A control is a system, process, or policy that is put in place in order to mitigate something bad from happening.

Think of it like a seatbelt in a car - the policy of putting the seatbelt on or the process of pulling it over your shoulder and locking it in the buckle prevents serious harm from occurring to a person.

SOC 2 Controls do the same thing for your organization's data; they are policies or processes put in place in order to stop anything bad - like a data leak - from happening.



As your business evolves, you can further address the optional criteria to bolster your cybersecurity posture.

We understand that the SOC 2 framework is not a one size fits all approach. We work with you to tailor controls to your specific needs, risks, and objectives, ensuring that your business is effectively managing its unique information security risks.

Implementing controls within the Trust Services Criteria is key to an effective cybersecurity strategy. Security Measures can be tailored to align with the unique services you offer while maintaining a strong foundation of security through the required Security TSC.

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations

TRUST SERVICES CRITERIA

mandatory

SECURITY

This criterion requires proof that your systems are fortified against unauthorized access and other security risks. It encompasses a range of components such as security policies, security controls, risk assessment and mitigation, protection and monitoring, and configuration management.

optional

PRIVACY

Privacy within the TSC focuses on the protection of Personally Identifiable Information (PII).
It involves safeguarding sensitive data, such as social security numbers, email addresses, and physical addresses, using encryption, access control, and data retention policies.

AVAILABILITY

Availability assesses whether your employees and clients can depend on the continuous functionality of your systems. It encompasses elements like disaster recovery planning, incident response protocols, performance monitoring, and business continuity strategies.

CONFIDENTIALITY

Confidentiality evaluates how your organization safeguards sensitive and confidential information.
This includes protecting business intellectual property, financial reports, and other proprietary data through measures like access control, encryption, information protection policies, and data handling procedures.

PROCESSING INTEGRITY

Processing Integrity determines whether your systems function accurately and reliably.
It is crucial in ensuring that transaction processing remains error-free, reducing the risk of fraud and inaccuracies through methods like process monitoring and quality control.

SOC 2 Type 1 and Type 2

There is SOC 1 and then there is SOC 2 (Type 1 and Type 2) - do not mistake them. SOC 1 focuses on the financial reporting controls of the service organization.

SOC 2 focuses on the security, availability, processing integrity, confidentiality, and privacy controls of the service organization, and is relevant for users who are concerned about the protection of their data and systems. **This eBook focuses on SOC 2.**

What's The Difference?

SOC 2 **Type 1** reports evaluate a company's controls at a single point in time. It assesses if the security controls are designed properly.

SOC 2 **Type 2** reports assess how those controls function over a period of time, generally 3-12 months.

So, an SOC Type 1 report tells you what the service organization says they do, while an SOC Type 2 report tells you what they actually do.

Visit BEMO's Article on What is the Difference Between SOC 2 Type 1 and Type 2?

Which Type is Best for My Company?

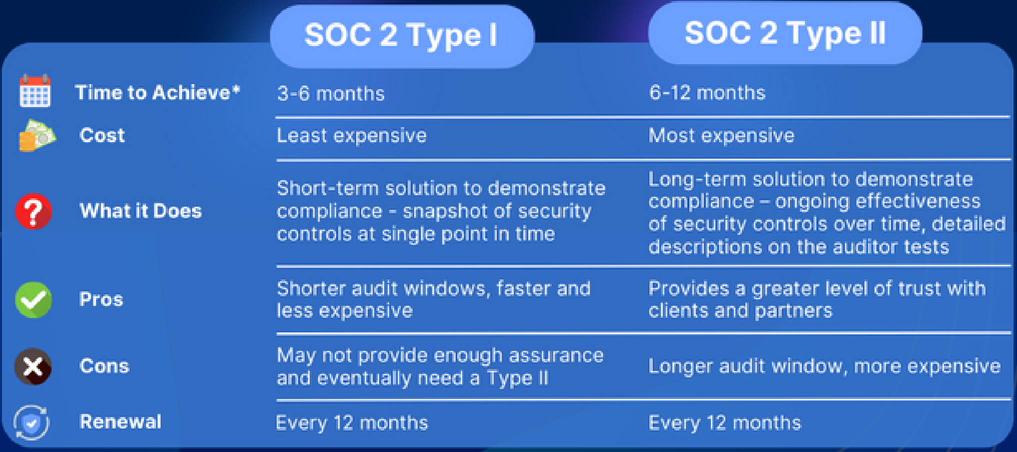
When choosing between a Type 1 and Type 2 SOC 2 audit, several key factors come into play. Each audit type offers its own set of advantages and challenges, making it crucial to align your choice with your specific goals, client requests, budget considerations, and timeline constraints.

For instance, a Type 1 audit demands less investment in terms of both time and finances. *Why?* Because it provides a snapshot assessment of your controls at a given point in time, without the need to demonstrate their ongoing effectiveness.

This simplicity in scope makes it a more cost-effective and time-efficient option for organizations.

On the other hand, a Type 2 audit signifies a higher level of compliance commitment. It offers a more comprehensive and in-depth view of your security controls by evaluating their effectiveness over an extended period.

While this type of audit demands a greater investment of resources, it provides a broader and more detailed picture of your commitment to security and compliance, which can be advantageous in building trust with customers and partners.



	SOC 2 Type I	SOC 2 Type II
Time to Achieve*	3-6 months	6-12 months
Cost	Least expensive	Most expensive
What it Does	Short-term solution to demonstrate compliance - snapshot of security controls at single point in time	Long-term solution to demonstrate compliance – ongoing effectiveness of security controls over time, detailed descriptions on the auditor tests
Pros	Shorter audit windows, faster and less expensive	Provides a greater level of trust with clients and partners
Cons	May not provide enough assurance and eventually need a Type II	Longer audit window, more expensive
Renewal	Every 12 months	Every 12 months

*Dependent on size of the organization and the organization's readiness level

Section Two:

What to Expect From the SOC 2 Audit

The SOC 2 Process

Odds are, you've never gone through the SOC 2 compliance process before. And if that's the case, it can be pretty ambiguous.

What do you need to do?

Who do you need to find?

How long does this take?

Where do you start?

Honestly, these answers are pretty hard to find, but we've laid out the general process for you below.

1 STEP 1: UNDERSTANDING SOC 2 COMPLIANCE

While this might seem like a no-brainer, it's important to understand what SOC 2 Compliance is, the general steps, and how your company will achieve compliance before you begin the actual process.

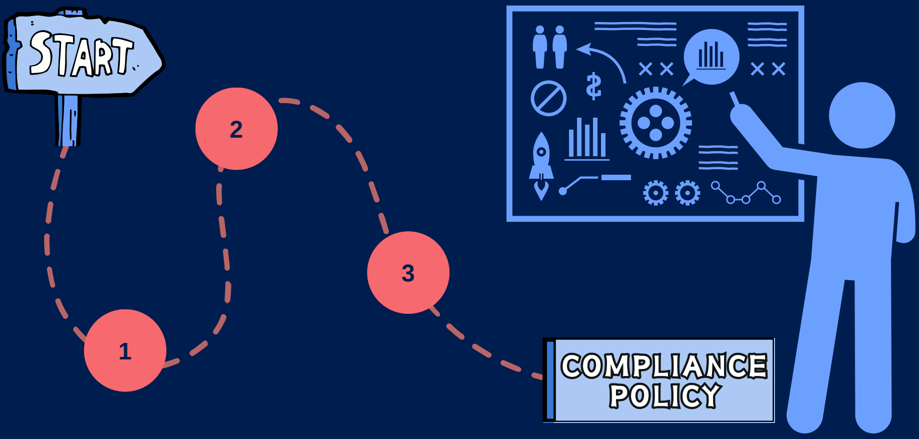
Will you be doing it yourself or going with a compliance provider? Familiarize yourself with the basics and then begin formulating your plan of attack. Reading this guide is a great start!

STEP 2: PRELIMINARY PREPARATION 2

Creating policies and procedures and tracking evidence that policies are understood and followed are key to proving your company's readiness. A compliance policy *answers questions* about what employees do and why they do it.

For example, a data security policy may state that employees must use strong passwords and encrypt sensitive data to protect the organization from cyberattacks.

A compliance procedure is the *instructions* on how to follow a compliance policy. A compliance procedure provides the step-by-step details for how policies are to be implemented and enforced.



For example, a data security procedure may specify how to create and change passwords, how to encrypt and decrypt data, and how to report any security incidents.

Organizations, especially those without internal security teams, may need to engage with an information security consultant to establish policies and processes aligned with SOC 2 requirements.

In the previous section, you learned about Type 1 vs Type 2 and the Trust Service Criteria. As part of your preliminary preparation, you should decide on the following:

A. Select SOC Type I or Type II.

B. Communicate the SOC 2 initiative internally to stakeholders. Explaining the who, what, when, where, why, and how of the audit will be critical in preparing employees for their roles in the process.

C. Define the audit scope by identifying the most relevant Trust Services Criteria (TSC) and review the individual requirements under each control.

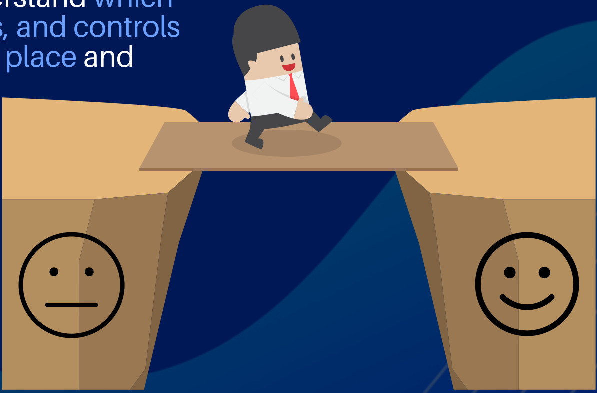
D. Plan the tool(s) to be used to manage the compliance activities. This could be manual tracking and manual evidence collection or better yet, the use of Compliance Automation Software to streamline the process.

E. Start Security Awareness Training for all employees. Security awareness training is one of the common criteria that the organization must meet to demonstrate SOC 2 compliance. By providing security awareness training to all staff, the organization can reduce the risk of human errors, breaches, and incidents that could compromise the confidentiality, availability, and integrity of the data and systems that they manage. Security awareness training also helps to model appropriate security behaviors and foster a culture of security within the organization

3 STEP 3: GAP ANALYSIS AND INTERNAL CONTROL REMEDIATION PLAN

Now that you've prepared to become SOC 2 compliant, it's time to perform a gap analysis and develop a plan to remediate the gaps.

The gap analysis helps understand which existing policies, procedures, and controls your business already has in place and operating. Measuring those against SOC 2 requirements, your team will form a remediation plan to protect your business and implement controls to fill those gaps.



Remediation might involve procedures that will monitor new processes or changes on existing ones.

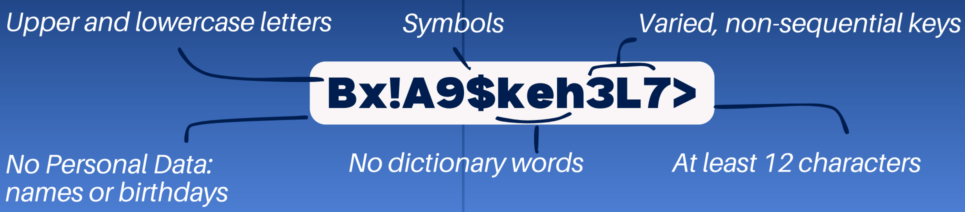
Current State

For example, you might discover a gap in password security where there has been no policy in place or maybe the policy exists but is not sufficient to meet the requirement.

Additionally, you might discover that the policy is not being enforced and employees are using weak passwords. Either way, a plan must be developed to fully correct (remediate) the issue.

Desired State

Strong Password Policy



Upper and lowercase letters

Symbols

Varied, non-sequential keys

Bx!A9$keh3L7>

No Personal Data: names or birthdays

No dictionary words

At least 12 characters

Vulnerability scanning and 3rd party penetration testing should be performed to help reveal the "not so obvious" gaps in your security. Both activities are essential to provide a list of potential security gaps to address in your remediation plan, with the ultimate goal of hardening security.

STEP 4: PERFORM A RISK ASSESSMENT

4

A. Define objectives of the entire service you provide customers as a whole, and determine what you've promised through written agreements, SLAs, etc. For example, if your SOC 2 only includes the Security category, focus on those promises that your organization has made specific to the security of your service.

B. Map out the individual, “in-scope” systems that support that service.

These are the critical systems that facilitate you providing your service.

- Procedures
- People
- Data
- Infrastructure and software
- Vendors or subservice orgs

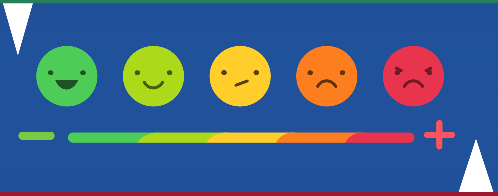
C. Perform a Risk Analysis

The goal is to to determine the risks that threaten the achievement of your objectives for the service you provide customers and determine the processes that are in place to respond to those risks.

The Risk Analysis process defines the basis for understanding how you should manage risks.

For instance, if a key performance security indicator (KPSI) for your organization is to prevent unauthorized data access, you will need to assess the risk of not achieving that benchmark.

Perhaps you assess the risk as low because you have implemented strict access controls, regular employee training, and robust monitoring systems to detect any unusual activity.

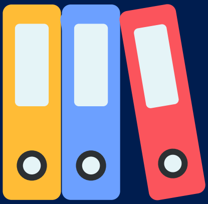


The assessed risk could be higher or much higher if you do not utilize some or any of those strategies. For example, if there are no regular audits of access logs, no clear policies about data handling, or if employees can access sensitive data from personal devices, the risk of insider threats could significantly increase.

5 STEP 5: THE SOC 2 AUDIT BEGINS

Now that you've completed all the legwork, it's time to undergo the actual audit. The audit is performed by an external 3rd party auditor – not your compliance provider, if you have one.

The auditor will gather evidence of the controls that the organization has in place. This could include policies, procedures, and other documentation. It is key to be organized with evidence to avoid extending the timeline (and cost) of the audit.



If you've purchased and have utilized Compliance Automation Software from the beginning of your compliance initiative, here is where you will start reaping the benefits of that decision!

The auditor will be able to log into your software's portal and review all the evidence you've collected from a single pane of glass.

The auditor will evaluate the evidence collected to determine if the controls are sufficient to meet the Trust Services Criteria you've scoped as part of the audit. If necessary, the auditor will follow up with the organization to gather more evidence.

! Remember that for a Type II audit, the auditor evaluates how the controls are operating over a period of time. This period of time can range from 3-6 months.

Finally, the auditor will perform their own independent testing and provide an opinion on whether or not they agree with the management's assertion.

6 STEP 6: FINAL SOC 2 REPORT

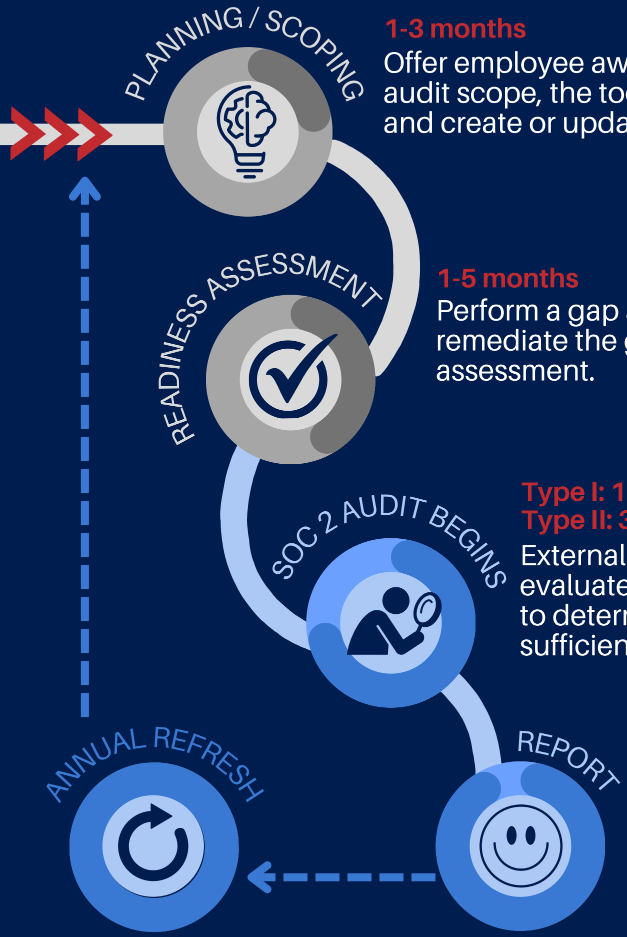
- The SOC 2 Type I report is delivered to the organization, summarizing the audit results and providing valuable insights into control effectiveness at a specific point in time.
- The SOC 2 Type II report is delivered to the organization, providing a comprehensive assessment of control effectiveness over the specified timeframe.

7 STEP 7: MAINTAINING YOUR ATTESTATION

Both SOC 2 Type I and Type II audits typically need to be renewed annually, meaning they last for a duration of 12 months. After this period, organizations are expected to undergo a new audit cycle to maintain their SOC 2 compliance status and provide up-to-date assurance to their customers and partners.

Renewal audits ensure that the controls and security practices remain effective and aligned with the trust services criteria over time.

Therefore, organizations should plan for these recurring audits to continuously demonstrate their commitment to data security and compliance.



PLANNING / SCOPING

1-3 months

Offer employee awareness training, define the audit scope, the tools to manage compliance, and create or update policies.

READINESS ASSESSMENT

1-5 months

Perform a gap analysis, develop a plan to remediate the gaps, and perform a risk assessment.

SOC 2 AUDIT BEGINS

Type I: 1-3 months
Type II: 3-12 months

External 3rd Party Auditor evaluates the evidence collected, to determine if the controls are sufficient.

REPORT

2-4 weeks

Final SOC 2 report is delivered and ready to be announced!

ANNUAL REFRESH

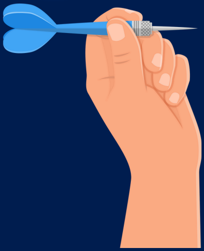
!

Please note that these timelines and steps are approximate and can vary (and overlap) based on the complexity of your organization's operations and the readiness of your controls. It's essential to work closely with your chosen audit firm to ensure a smooth and timely audit process.

How To Speed Up Your Compliance Journey

In a time crunch to reach your SOC 2 Attestation? Don’t worry, sometimes these timelines can be shortened if you work efficiently and focus on what matters. Here are five key strategies to accelerate your SOC 2 audit:

1 STRATEGY 1: DEFINE YOUR TYPE AND CRITERIA EARLY



Determine whether a SOC 2 Type 1 or Type 2 audit is most suitable for your organization. Additionally, specify the trust services criteria relevant to your business.

This early clarity helps you tailor your efforts to meet specific compliance requirements, avoiding unnecessary delays.

2 STRATEGY 2: EMBRACE A CULTURE OF CONTINUOUS COMPLIANCE

We can’t stress this enough: Don't view SOC 2 compliance as a one-and-done project. Instead, cultivate a culture of continuous compliance within your organization. Embed security and control measures into your daily operations.

This proactive approach ensures that compliance becomes a natural part of your business processes, reducing the need for last-minute adjustments during audits.

3 STRATEGY 3: COLLABORATE EFFECTIVELY WITH YOUR AUDITOR

Forge a strong partnership with your chosen audit firm from the beginning. Work closely with them to understand the audit process, expectations, and documentation requirements.

A collaborative approach allows you to address any questions or concerns promptly, preventing bottlenecks and ensuring a smoother audit journey.

4 STRATEGY 4: TRANSPARENCY OVER CONCEALMENT

Resist the temptation to hide potential vulnerabilities or gaps in your security controls. Concealing issues may seem like a shortcut to compliance, but it can backfire, leading to delays and undermining the purpose of the audit.

Instead, work openly with your auditor to identify and address any shortcomings, allowing for timely remediation.

5 STRATEGY 5: CREATE A WELL-DEFINED TIMELINE & MILESTONES

Establish a clear timeline for your SOC 2 audit project. Define checkpoints and milestones to assess progress. Effective project management ensures that tasks are completed in a logical sequence and that team efforts are coordinated efficiently. Regular communication within your compliance team is crucial to staying on track.

Bonus Tip: Seek Expert Assistance When Needed. Don't hesitate to seek assistance, especially from experts like BEMO who specialize in SOC 2 compliance.

Experienced professionals can provide valuable guidance, assess your readiness accurately, and offer solutions to bridge any gaps.

Book a Meeting with a SOC 2 Expert

Our expertise can significantly accelerate the audit process, ensuring that you're well-prepared and confident in your compliance journey.

Section Three:
The Costs of SOC 2 Compliance

SOC 2 Costs

Now onto the costs of attaining SOC 2 compliance. There are a lot of different factors that go into how much your compliance will cost such as company size, current security set up, if you go through a compliance provider or not, and many more.

When attaining SOC 2, there are four main annual costs and three main monthly costs. Below are BEMO's costs for an SMB to attain SOC 2 Type 1 Compliance.

	Organization Size	
One-Time Fees	**1 to 99**	**100 to 499**
Compliance Automation Solution	$25,000	$50,000
3rd Party Auditor	$10,000	$10,000
Penetration Testing	$4,700	$4,700
Total One-Time Fees	$39,700	$64,700
Monthly Fees		
BEMO Managed Compliance	$4,800	$9,600
BEMO Platinum Security	$99/user	$99/user
Microsoft 365 E5 Licensing	$57/user	$57/user
All Migrations	Free	Free

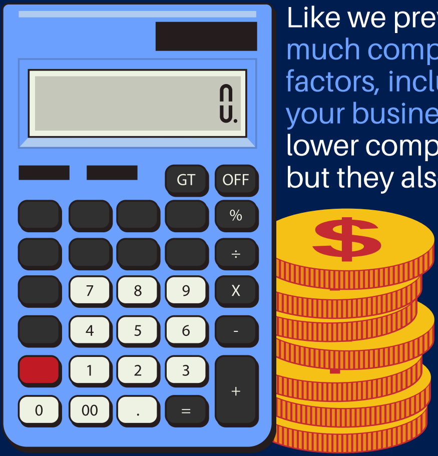
Below are BEMO's costs for an SMB to attain SOC 2 Type 2 Compliance.

	Organization Size	
One-Time Fees	**1 to 99**	**100 to 499**
Compliance Automation Solution	$25,000	$50,000
3rd Party Auditor	$14,000	$14,000
Penetration Testing	$4,700	$4,700
Total One-Time Fees	$43,700	$68,700
Monthly Fees		
BEMO Managed Compliance	$4,800	$9,600
BEMO Platinum Security	$99/user	$99/user
Microsoft 365 E5 Licensing	$57/user	$57/user
All Migrations	Free	Free

Get Your Quote Now!
Go to our SOC 2 Type II Cost Calculator

The great thing about BEMO's pricing is that you ***only*** pay for the services we offer. All third-party costs – licensing, auditors, pen testing, compliance automation software – are charged as MSRP. We don't overcharge for those services; you only pay for BEMO's in-house costs: your Security package and the managed compliance service. Oh, and did we mention all migrations are completely *free*?

Other Costs to Consider



Like we previously mentioned, precisely how much compliance costs you depends on various factors, including the size, nature, and location of your business. Small businesses typically have lower compliance costs than large corporations, but they also may have fewer resources to handle them.

Additionally, businesses operating across multiple jurisdictions often incur higher compliance costs compared to those operating in a single market. Industries subject to heavy regulations, like healthcare, finance, or energy, tend to have higher compliance costs than those in less-regulated sectors such as retail, media, or entertainment.

BUSINESS SIZE

The bigger the business, the greater the costs but also, the more resources at disposal.

INDUSTRY

Industries with heavy regulations:
*Healthcare *Finance *Energy

LOCATION

Working across different states or countries means adhering to several jurisdictions, which is more costly than operating in one single market.

Section Four:
Preparing for an SOC 2 Audit

So, you’ve familiarized yourself with the SOC 2 Audit process... now what? Let's delve into some actionable tips that will help you prepare for your audit and maintain a culture of security compliance readiness all the time.

Build a Compliance Team

You need to have an expert for every task throughout the process, this team will work together to coordinate all the aspects of your audit, so that it is manageable and not as overwhelming.

Chief Compliance Officer (CCO):
This individual takes overall responsibility for managing the audit process, coordinating team efforts, and liaising with external auditors.

Project Manager:
They play a crucial role in organizing and overseeing the audit preparations. They assign tasks, make sure that deadlines are met, and ensure documentation is in order.

IT and Security Personnel:
These experts focus on implementing and maintaining the technical controls required for SOC 2 compliance. They ensure that your systems and infrastructure are secure and meet audit standards.

Legal Team:
The legal team deals with contractual and legal aspects of compliance, ensuring that your organization's policies and practices align with legal requirements.

Human Resources (HR) and Administrative Staff:
Managing policies, training, and communication with employees is the responsibility of HR and administrative staff. They help create a culture of compliance awareness within the organization.

External Consultant: In some cases, organizations may opt to bring in an external consultant with expertise in SOC 2 audits. Consultants provide valuable insights, guidance, and an unbiased assessment of your readiness for the audit.

The involvement of leadership at the onset of the SOC 2 compliance process is crucial for a successful outcome. Leadership sets the tone and direction for the compliance efforts, communicates the expectations and responsibilities to the staff, allocates the resources and support needed, and monitors and evaluates the progress and outcomes.

By being actively involved in the SOC 2 compliance process, leadership demonstrates its commitment to maintaining high standards of trust and quality for its customers and stakeholders.

Focus on Gathering Only the Necessary Documentation

Efficiency is key when preparing for an SOC 2 audit. Avoid drowning in paperwork by focusing on gathering only the necessary and relevant documentation and evidence required for your audit.

This approach saves you time and ensures that your efforts are targeted and effective.

Remember if you say you have a policy or control in place, you need to account for it with evidence. if you are not including it in your audit because it’s not key, do not focus on it.

Build Out Your Security Tech Stack

To kickstart your SOC 2 journey, we emphasize the importance of fortifying your organization's digital defenses by assembling a robust security technology stack.

A password manager is a software tool that securely stores and manages passwords for your organization. At BEMO our go-to password Manager choice is *Keeper*. It helps ensure that employees use strong, unique passwords for their accounts.

This is crucial because weak or reused passwords are a common entry point for cyberattacks.

Vulnerability scanners automatically identify and assess vulnerabilities in your network and systems. Regular scanning helps you discover potential weaknesses before attackers can exploit them, allowing you to proactively address security issues.

Antivirus and Antimalware software are necessities and must be kept up to date on all devices, including mobile devices. But basic antivirus isn't enough. To achieve compliance, organizations need to implement advanced threat protection solutions that include endpoint detection and response (EDR) capabilities, stopping both known and unknown threats at the endpoint level.

One such solution is *Microsoft Defender for Endpoint*, which not only provides next generation antivirus protection, but also EDR capabilities that can help organizations prevent, detect, and remediate cyberattacks in real time.

Backups are an essential strategy to ensure important data is protected from loss. Loss can occur as a result of things such as hardware failure, a malicious attack, natural disasters, or even accidental deletion.

Backup processes and procedures are an integral part of your *Disaster Recovery* and Business Continuity Plans.

The company must be able to prove that backups are not only being performed regularly, but also that backup data is secured, encrypted, and separated from the production environment. Backups must be tested regularly to verify the integrity of the backups.

To ensure the integrity of your team, particularly those with access to sensitive data, consider using a reputable background check provider. This step helps mitigate insider threats and build trust with your clients and customers.

Visit BEMO's Article on How to Prepare for a SOC 2 Audit

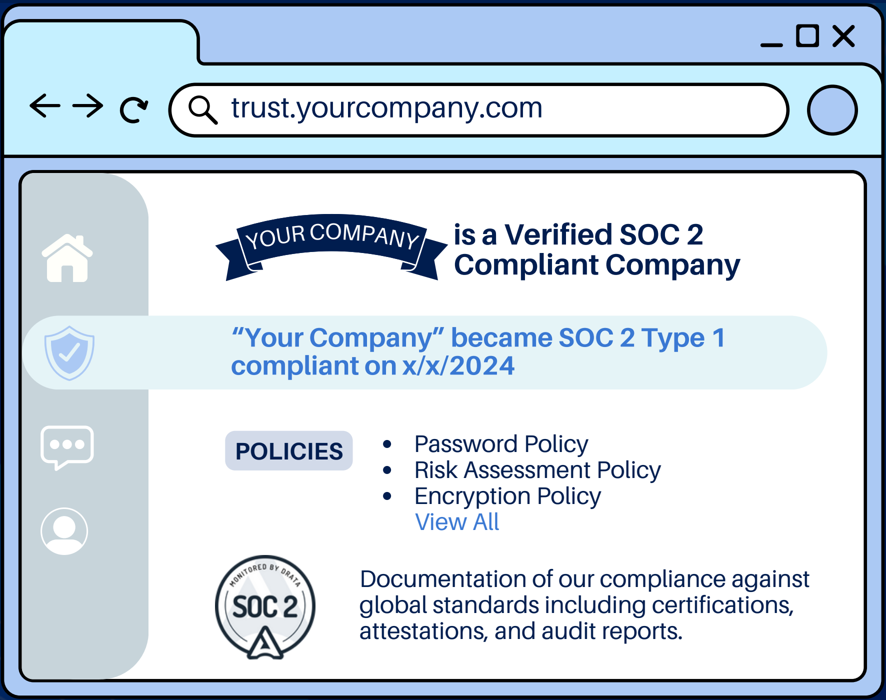
Section Five:
Post Compliance: Now What?

Now that you've got your report in hand, what's the next exciting chapter in your compliance journey? It's time to shout it from the rooftops! After all, this is the culmination of all your hard work and dedication.

Promote Your Attestation

Publish Your Trust Report

You'll want to set up a public site where customers and partners can have easy access to your report. Ideally this page will include the dates when you received and completed your reports, the policies you put in place and the tests you underwent as well as their results.



YOUR COMPANY is a Verified SOC 2 Compliant Company

"Your Company" became SOC 2 Type 1 compliant on x/x/2024

POLICIES

- Password Policy
- Risk Assessment Policy
- Encryption Policy

View All

Documentation of our compliance against global standards including certifications, attestations, and audit reports.

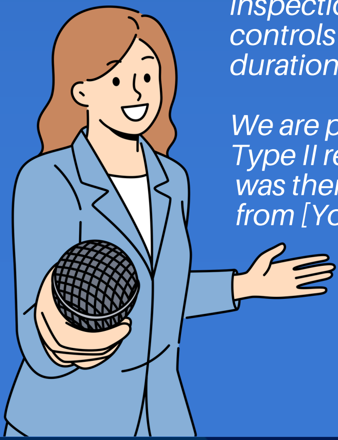
You can visit BEMO's trust page to check our SOC 2 Type I and Type 2 compliance achievements.

Press Release

Another exciting step is to a press release that broadcasts your achievement both internally and externally, all while directing everyone to your trust report. Here's a sample press release to proudly announce your successful SOC 2 audit:

"We are thrilled to announce that [Your Company] has achieved a significant milestone: successful completion of a System and Organization Controls (SOC) 2 Type II audit, expertly conducted by [Your Auditor's Company Name].

Developed by the American Institute of Certified Public Accountants (AICPA), the SOC 2 information security audit entails a meticulous examination of controls aligned with the trust services criteria, encompassing security, availability, processing integrity, confidentiality, and privacy.



A SOC 2 Type II report goes beyond surface-level inspection; it delves into the design of specific controls and their effectiveness over a specified duration.

We are proud to share that [Your Company]'s SOC 2 Type II report did not have any noted exceptions and was therefore issued with a "clean" audit opinion from [Your Auditor's Company Name]. This accomplishment reflects our unwavering commitment to ensuring the security, reliability, and trustworthiness of our services. We invite you to explore the full details in our Trust Report."

Add the SOC 2 Logo To Your Website

Once you've made it public you can put the official AICPA SOC for Service Organizations logo on your website. Simply go to the AICPA website and you'll see the appropriate logo on the page. Click on the logo to register to use it.

Continuous Compliance

Remember compliance is not a checklist matter. Yes, you may have received your report and announced it to the world (congrats!), but you can't forget about it.

Approaching SOC 2 compliance as an ongoing commitment rather than a one-time event is vital to your success.
The best companies integrate security and compliance into their everyday operations. This means that:

- ✓ Risk management practices should be ongoing, not just during audit preparation.
- ✓ Security and compliance are an integral part of daily operations.
- ✓ Policies and procedures evolve to address changing threats & technology.
- ✓ Regular training and awareness programs keep employees informed and vigilant about security.

> ! By adopting this proactive approach, compliance becomes a continuous process, reducing the need for intense, last-minute preparations before an audit and improving your organization's overall security posture.

Work with a Compliance Officer or Engineer

If you've never been through the compliance process before, or you have and don't have the luxury of a full-time Compliance Officer, you want to work with a competent Compliance Engineer. They can help you maintain compliance by continuously checking your security controls for any changes or errors and fixing them as soon as possible.

A Compliance Engineer can also provide proactive recommendations on how to improve your compliance posture and prevent future issues.

Incident Response Planning

Maintain and regularly test your incident response plan.

Being prepared to handle data breaches or security incidents promptly is crucial for continuous compliance.

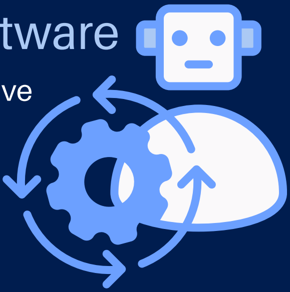
Document Everything

Maintain comprehensive documentation of your compliance processes, control activities, and incident response procedures.

This documentation not only helps with audits but also serves as a reference for employees and a record of your continuous compliance efforts.

Compliance Automation Software

This tool is designed to generate comprehensive reports, issue real-time alerts, and notify you of any compliance gaps or potential issues.
It provides real-time feedback and continuous monitoring of your security controls, reduces human error and helps you regularly identify and assess your policies and controls.



Visit BEMO's Article on
What is Compliance Automation Software?

Conclusion

We hope you found this guide helpful in learning more about SOC 2 and how you can achieve it.

As you can now see, becoming SOC 2 compliant is a complex journey. Achieving SOC 2 compliance requires an investment in time, money, and skills. But the payoff is worth the sacrifice, if planned correctly.

If you'd like to discuss how partnering with BEMO can help you overcome the challenges of achieving SOC 2, we are here to help.

Learn About SOC 2 With BEMO

Going with a compliance provider, like BEMO, can help take a lot of the pressure off you.

We handle both the achievement of your SOC 2 Compliance as well as the continual maintenance of it, giving you the peace of mind to sit back and focus on your actual work.

Plus, we have first-hand experience of what to expect from the process, since BEMO is a proudly verified SOC 2 Type II Compliant Company.