

letsbloom 

SOC 2

COMPLIANCE CHECKLIST

The Ultimate Guide to Prepare for SOC 2 Audit



Data security and privacy are need of the hour in today's world.

With the global average cost of a **data breach reaching USD 4.88 Million in 2024** – the highest total ever, businesses must safeguard their data, people, infrastructure, and their organization's bottom line. Implementing data security frameworks and standards like **SOC 2 (System and Organization Controls)** can help strengthen your data security programs, protecting critical assets and data spread across multiple environments.

This guide offers a comprehensive checklist to help you fast-forward your journey to SOC 2 compliance and build trust with your customers and stakeholders.

What is SOC 2?

SOC 2 is a security compliance standard designed for service providers that handle customer data. It evaluates the effectiveness of the organization's security controls, processes, and policies to ensure that they meet industry standards and best practices. SOC 2 compliance demonstrates how well a company has implemented adequate security controls with regards to the five Trust Services Criteria (TSC): Security, Availability, Processing Integrity, Confidentiality, and Privacy.









Types of SOC 2 Compliance Audits

There are two types of SOC 2 audit reports: Type 1 and Type 2.

A SOC 2 Type 1 report evaluates the design of security processes and controls at a specific point in time, while SOC 2 Type 2 report assesses the design as well as the operative effectiveness of these controls over a longer period of time, typically 6 months to a year.

The type of report an organization pursues depends on their specific needs and requirements. Type 1 is often a preliminary step, with Type 2 providing more comprehensive and ongoing assurance.

Difference between SOC 2 Type 1 and Type 2

	SOC 2 Type 1	SOC 2 Type 2
 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 may 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.*

Why is SOC 2 Compliance Important for Your Business?

Achieving SOC 2 compliance offers several benefits that enhance an organization's reputation and market standing:



Building Customer Trust

SOC 2 certification demonstrates to customers that their data is secure and handled with integrity. This can be a significant competitive advantage, especially when dealing with sensitive information.



Competitive Advantage

With increasing data privacy regulations & security concerns, SOC 2 compliance sets your business apart. It shows prospective clients and partners that you take data security seriously, potentially winning you more business.



Expanding Market Opportunities

Many industries, particularly those heavily regulated, require SOC 2 compliance as a prerequisite for doing business. By achieving this certification, you open doors to new markets and opportunities.



What is SOC 2 Compliance Checklist?

A SOC 2 compliance checklist is essential for any organization preparing for a SOC 2 audit. It outlines the necessary steps and requirements needed for achieving and demonstrating compliance with the TSC.

This checklist enables businesses to simplify, streamline, and speed up their journey to SOC 2 compliance, saving time and resources. It also helps ensure that no crucial aspect of SOC 2 compliance is overlooked, providing a structured framework for achieving certification.

SOC 2 Checklist: 7 Key Steps to Get You Audit-ready

Preparing for a SOC 2 audit involves a structured approach.

Here are 7 key steps to guide your organization through the process:

1. Identify Which SOC 2 Type is Applicable

Determine which SOC 2 Type audit is required based on your business needs and objectives.

- **SOC 2 Type 1** assess whether your controls are designed effectively and is a good starting point
- **SOC 2 Type 2** provides more extensive assurance that the controls are not only designed properly but are functioning as intended over an extended period.

Here's how you can choose the right report:

- Have you conducted a SOC 2 audit before?
- Is there an urgent need for the report?
- Do you have the resources to implement the necessary security policies and procedures?

If you answered 'no' to most of these questions, it might be best to start with a Type 1 audit. SOC 2 Type 1 is less comprehensive and can typically be obtained more quickly than a SOC 2 Type 2 report. However, if you answered 'yes' to all the questions, consider opting for a Type 2 audit.

2. Define Your Scope

Decide which of the Trust Services Criteria you want to include in your audit.

- Security is the mandatory category for every SOC 2 audit
- You can also choose to include Availability, Processing Integrity, Confidentiality, and Privacy, depending on your services and data handling practices

3. Perform Risk/Gap Assessment

Conduct a thorough review of your current policies, procedures, and controls to identify any gaps, risks, or weaknesses. This assessment will provide valuable insight into your current security posture and the necessary controls needed to meet the TSC requirements.

The risk assessment should include the following:

- ✓ **Identify Critical Assets:** Determine the information assets that are essential for business operations and prioritize them based on their criticality.
- ✓ **Assess Threat Impact:** Identify and evaluate the potential impact of threats to these information assets.
- ✓ **Evaluate Vulnerabilities:** Identify and assess the impact of the vulnerabilities associated with the identified threats.
- ✓ **Assess Likelihood:** Evaluate the probability of the identified threats and vulnerabilities.
- ✓ **Determine Risks:** Assess the risks associated with the information assets based on the identified threats and vulnerabilities.

4. Address the Risks

Once security risks and control gaps are identified, work on implementing the necessary controls to meet the TSC criteria.

This may involve:

- ✓ Reviewing and updating policies
- ✓ Making necessary software changes
- ✓ Establishing standard procedures
- ✓ Integrating new tools or workflows

5. Maintain Compliance through Continuous Controls Monitoring

Once you have implemented the necessary controls, it's time to establish processes to continuously monitor and maintain those controls. Automation tools can significantly assist in continuous monitoring, enabling efficient evidence collection and ensuring that controls remain effective over time.

When setting up continuous monitoring, consider the following key factors:

- ✓ **Scalability:** Ensure the monitoring processes can grow alongside your business.
- ✓ **Productivity:** The tools and processes should not impede your team's productivity.
- ✓ **Alert Mechanisms:** Monitoring platform should provide prompt alerts to notify the team when controls are not properly implemented.

6. Choose the Right SOC 2 Auditor

Look for auditors who can guide you through the entire audit journey, offering valuable insights to improve your compliance programs, streamline processes, and help you achieve a clean SOC 2 report.

When selecting an auditor, consider the following key factors:

- AICPA Affiliation:** Ensure that the auditor is affiliated with the American Institute of Certified Public Accountants (AICPA).
- Industry Expertise:** Choose an auditor who has a deep understanding of your industry.
- Effective Collaboration:** Look for someone who collaborates well with your team.

7. Undergo the SOC 2 Audit

Provide your auditor with all the necessary information and evidence. They will review all the in-scope controls, verify the information, conduct walkthroughs, and provide you with a final SOC 2 report. This report validates your compliance with the applicable TSC.

Be prepared to answer the following questions from your auditor:

- Can you provide documentation showing that all your employees have undergone background checks?
- Can you show evidence that modifications in your code repositories are peer-reviewed before being merged?
- Can you provide proof that access to emails and databases is revoked when an employee leaves your organization?
- How do you ensure that your security policies are regularly updated and communicated to all employees?
- Can you provide logs or records of security incidents and how they were resolved?
- What measures are in place to ensure the physical security of your data centers?
- How do you handle data encryption both at rest and in transit?

The Path to SOC 2 Compliance is not Without its Challenges...

Organizations must understand the obstacles specific to their business and be diligent in their efforts to achieve and maintain compliance.



Complexity and Resource Intensity

SOC 2 compliance involves a wide range of controls and criteria, requiring significant time, resources, and financial investment. Developing and implementing the necessary policies, procedures, and controls can be a daunting task, especially for businesses new to the process.



Time Commitment

The preparation and audit process for SOC 2 compliance can be lengthy, often taking several months or even years, depending on the organization's size and complexity.

C H A L L E N G E S



Internal Control Audits

Achieving SOC 2 compliance demands rigorous internal control audits. This involves extensive documentation and testing of controls, which can be a challenging, particularly for businesses without a strong internal audit function.



Continuous Monitoring

Once SOC 2 compliance is achieved, organizations must continuously monitor their controls to ensure ongoing effectiveness. Staying vigilant and responsive to any changes or emerging risks is essential.

Fast-Forward Your SOC 2 Audit Journey with letsbloom

letsbloom empowers businesses of all sizes and industries to simplify, streamline, accelerate their journey to SOC 2 compliance and be audit-ready in weeks, instead of months. Our automated compliance management platform provides:

- ✔ **Continuous controls monitoring**, ensuring you maintain compliance with all the 5 domains of SOC 2 controls.
- ✔ **Automated evidence collection** and real-time alerts on non-conformities, reducing the manual effort and time spent on audits.
- ✔ Holistic risk visibility and actionable intelligence using **MITRE ATT&CK framework**, helping you quickly address gaps.
- ✔ Seamless **SOC 2 audit reports** with built-in validations.

Why wait?

Begin your SOC 2 compliance journey now with a **30-day FREE trial**.
No credit card is required.

[Request a FREE demo! →](#)