

SOC 2 CHECKLIST: PREPARE FASTER FOR YOUR SOC 2 AUDIT

Step 1: Choose your objectives for SOC 2 compliance

It helps to know why you need SOC2 attestation and whether it aligns with your business objectives. Check the ones that apply to you.

- ☐ Requested by customers
- ☐ Building a security-first culture
- ☐ Competitors are SOC 2 compliant

Step 2: Identify the type of SOC2 report you need: SOC 2 Type I or SOC 2 Type II

Here's how you can identify which SOC2 report better fits your requirement.

- ☐ We have undergone a SOC 2 audit before
- ☐ Our SOC2 report requirement isn't urgent (within three months)
- ☐ We have dedicated resources to develop and implement security policies
- ☐ Our workforce understands their roles and responsibilities when implementing controls
- ☐ We have a system in place to communicate system changes

If most of your answers are a no, it perhaps make better sense to start with a SOC2 Type I audit. You can get to the SOC2 Type II audit once you have the security controls and processes in place.

Step 3: Define the scope of compliance based on the Trust Service Criteria (TSC)

You should define the scope of your audit by identifying the TSC for which you want to establish and test controls. The scope will depend on type of your business and your customer requirements.

Select the TSC that applies to you

- ☒ **Security**
 - Do you review and document your security procedures?
 - Do you have backup and recovery procedures in place?
 - Do you have specific procedures to handle cyber safety incidents?
- ☐ **Availability**
 - What is your service uptime?
 - Do you have processes to address service issues that affect your availability?
 - Do you have access controls in place for your Who all can access your service?
 - Are there any restrictions?
- ☐ **Confidentiality**
 - How do you handle and process confidential data?
 - Do you have access management incorporated in your organization?
 - How do you avoid unauthorized access? Do you have proceses in place?

SOC 2 CHECKLIST: PREPARE FASTER FOR YOUR SOC 2 AUDIT

- ☐ **Processing Integrity**
Are your processing systems providing timely and accurate data to users?
How do you ensure integrity of data?
Do you have specific procedures in place to correct errors quickly?
- ☐ **Privacy**
Do you have a data retention policy that's documented and communicated to customers?
Do you store personally identifiable information (PII)? If yes, where and how do you store it?
Do you protect PII on your system?

Step 4: Conduct an internal risk-assessment

An internal risk assessment requires you to identify the risks associated with “growth, location, or infosec best practices.” You must then assign probabilities to each risk identified, estimate its adverse impact on your business, and put policies and measures in place to mitigate them.

- ☐ Have you identified the potential threats and associated risks to your business?
- ☐ Have you estimated the potential impact of these threats on your business?
- ☐ Have you tagged the critical systems based on the risks identified?
- ☐ Have you developed mitigation strategies for the risks?

Step 5: Perform gap analysis and remediation

After the internal risk assessment, you must identify the control gaps based on existing and potential security threats. You must remediate these gaps based on the chosen TSCs.

Here are some common remediation practices to get your started

- ☐ Align and deploy controls based on the chosen TSCs
- ☐ Set up a clear organizational structure
- ☐ Have well-defined infosec policies & procedures
- ☐ Conduct background screening procedures for all new employees
- ☐ Ensure changes in the code repositories are peer reviewed
- ☐ Conduct periodic security training of all employees
- ☐ Collect evidence of compliance

SOC 2 CHECKLIST: PREPARE FASTER FOR YOUR SOC 2 AUDIT

Step 6: Undergo Readiness Assessment

A readiness assessment evaluates whether you meet the SOC 2 requirements to undergo a full audit. You can hire an independent auditor to perform it.

Here's what to expect from the readiness assessment

- ☐ Evaluate vulnerabilities and gaps, and make recommendations to fix them to get audit-ready
- ☐ Remediate gaps identified by remapping some controls or implementing new ones

Step 7: SOC 2 audit

- ☐ Authorize an independent certified auditor
- ☐ Address auditor queries

Step 8: Establish Continuous Monitoring Practices

Compliance Getting your SOC 2 compliance report isn't just a one-time event. The report is just a start as security is a continuous process. It, therefore, pays to establish a robust continuous monitoring practice as SOC 2 audits happen annually.

Here's what makes a your continuous monitoring system robust

- ☐ Continuous monitoring should be scalable; it should grow with your organization
- ☐ It should streamline evidence collection
- ☐ It shouldn't get in the way of your employees' productivity
- ☐ It should alert you when a control isn't deployed or deployed incorrectly
- ☐ It should give you the big picture as well as an entity-level granular overview of your infosec health at any point in time
- ☐ Implement additional measures such as MDM, Incident Management System, Pen Tests, Vulnerability Scans