SOC 2 Compliance Checklist

9 Steps To Prepare for an Upcoming Audit

Step 1. Determine if a Type 1 Is Necessary

First, decide which SOC 2 report type is right for your organization. Here's how to decide:

- [ ] Have you completed a SOC 2 audit before?
- [ ] Do you need the report urgently?
- [ ] Do you have resources to develop and implement security policies?

If you answered no to most of the questions above, you may want to start with a Type 1 report, which is less robust and can often be acquired faster than a SOC 2 Type 2 report. If you answered yes to all of the above questions, consider starting with a Type 2 report.

Step 2. Determine Your Scope

Define your scope by determining which of the Trust Services Categories (TSC) you want to measure against. The TSC you choose will depend on your industry and customer needs.

The five TSC are:

- [ ] **Security:** Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.
- [ ] **Availability:** Information and systems are available for operation and used to meet the entity's objectives.
- [ ] **Processing integrity:** System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.
- [ ] **Confidentiality:** Information designated as confidential is protected to meet the entity's objectives.
- [ ] **Privacy:** Personal information is collected, used, retained, disclosed, and disposed of to meet the entity's objectives.

You don't have to include all five Trust Services Categories. Security is the only mandatory category, however, Availability and Confidentiality are frequently included.

SOC 2 Compliance Checklist

9 Steps To Prepare for an Upcoming Audit

Step 3. Communicate Processes Internally

To ensure you have buy-in from all necessary parties, you should communicate early and often with key players. Those roles include your organization's executive management and department leaders (Human Resources, Engineering, DevOps, Security, IT, etc.).

To do this:

- [ ] Organize a meeting (or separate meetings) with stakeholders to communicate the who, what, when, where, why, and how of the audit to prepare employees for their obligations.

Step 4. Perform a Gap Assessment

A gap assessment involves looking at your existing procedures, policies, and controls to help better understand your current security posture and which controls you still need to implement to meet the applicable criteria of the TSC.

You can do this by either:

- [ ] Running a SOC 2 compliance scan using an automated compliance scanning tool
- [ ] Manually performing a gap analysis to see which SOC 2 criteria meet requirements or are missing

Step 5. Remediate Control Gaps

Once your gap assessment has been completed, it can take time to remediate and ensure SOC 2 control mandates are being achieved.

You will need to work with your team to:

- [ ] Review policies
- [ ] Formalize procedures
- [ ] Make necessary alterations to software
- [ ] Address any additional steps like integrating new tools and workflows

This will allow you to close gaps before the audit takes place.

SOC 2 Compliance Checklist

9 Steps To Prepare for an Upcoming Audit

Step 6. Update Your Customers and Prospects

Although you don't have to announce to customers and prospects that you're pursuing SOC 2, you can still outline the processes you have in place to keep their data safe in an effort to be a transparent partner.

On your website or social media, consider outlining a high-level overview of:

- [ ] Employee training
- [ ] Penetration testing you've conducted
- [ ] Data encryption procedures
- [ ] Any continuous security control monitoring you have in place

Step 7. Monitor and Maintain Controls

Now that you've made remediations and added controls to reach SOC 2 compliance, establish processes that help you and your team continuously monitor and maintain those controls.

- [ ] If you haven't already, implement a tool that can automate control monitoring and evidence collection.

Step 8. Find an Auditor

Before you begin looking for an audit firm, you must find an auditor. The right auditor can do much more than conduct your audit—they can help you understand and improve your compliance programs, streamline the process, and ultimately achieve a clean SOC 2 report.

Look for someone who:

- [ ] Has good references
- [ ] Collaborates well with you and your team
- [ ] Understands your industry
- [ ] Answers your questions intelligently and in a way your team understands

Step 9. Undergo the SOC 2 Audit

At this stage, you're ready to begin the audit process. Once you provide all the necessary information to your auditor, they will review evidence for each in-scope control, verify information, schedule walkthroughs, and provide you with the final report.