

SOC 2 Compliance Checklist

Preparing for a SOC 2 audit is a lot easier when you know exactly what auditors expect to see and who owns each step across your organization. Use this checklist to work through the key decisions, remediation tasks, and communication points so you can move into the audit with clear evidence, aligned stakeholders, and fewer last-minute scrambles.

01 Determine If a Type 1 Report Is Necessary

- ☐ Confirm whether you have completed a SOC 2 audit before.
- ☐ Confirm whether you need the report urgently.
- ☐ Confirm whether you have resources to develop and implement security policies.

If you answered “no” to most questions above, consider starting with a SOC 2 Type 1 report.

If you answered “yes” to all of the questions, consider starting with a SOC 2 Type 2 report.

02 Determine Your Scope

- ☐ Identify which Trust Services Categories (TSC) you want to measure against based on your industry and customer needs.
- ☐ Confirm that Security is included in scope (mandatory).

Security: Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise availability, integrity, confidentiality, and privacy of information or systems, and affect the entity's ability to meet its objectives.

- ☐ Decide whether to include Availability.

Availability: Information and systems are available for operation and used to meet the entity's objectives.

- ☐ Decide whether to include Processing Integrity.

Processing Integrity: System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.

- ☐ Decide whether to include Confidentiality.

Confidentiality: Information designated as confidential is protected to meet the entity's objectives.

- ☐ Decide whether to include Privacy.

Privacy: Personal information is collected, used, retained, disclosed, and disposed of to meet the entity's objectives.

03 Communicate Processes Internally

- ☐ Identify executive sponsors and department leaders who need to be involved (for example, Human Resources, Engineering, DevOps, Security, IT).
- ☐ Schedule a meeting (or series of meetings) with stakeholders.
- ☐ Communicate the who, what, when, where, why, and how of the audit.
- ☐ Prepare employees for their obligations during the audit.
- ☐ Share a high-level timeline and expectations with all relevant teams.

04 Perform a Gap Assessment

- ☐ Review existing procedures, policies, and controls to understand your current security posture.
- ☐ Determine which controls you still need to implement to meet the applicable TSC criteria.
- ☐ Run a SOC 2 compliance scan using an automated compliance scanning tool
- ☐ Document all identified gaps and areas for improvement.

05 Remediate Control Gaps

- ☐ Review policies identified in the gap assessment.
- ☐ Formalize procedures that are ad hoc or undocumented.
- ☐ Make necessary alterations to software and system configurations.
- ☐ Integrate any new tools and workflows required to meet control objectives.
- ☐ Validate that all remediations are implemented and operating effectively.
- ☐ Confirm that identified gaps are closed before the audit takes place.

06 Update Customers and Prospects

- ☐ Decide whether you will publicly communicate that you are pursuing SOC 2.
- ☐ Outline how you keep customer data safe, even if you do not explicitly mention SOC 2.
- ☐ Publish a high-level overview of employee training programs (for example, security awareness).
- ☐ Publish a high-level overview of data encryption procedures.
- ☐ Publish a high-level overview of penetration testing or security testing you have conducted.
- ☐ Publish a high-level overview of any continuous security control monitoring you have in place.

07 Monitor and Maintain Controls

- ☐ Assign owners for key controls.
- ☐ Establish a cadence for periodic control reviews.
- ☐ Implement processes or tools to track control performance over time.
- ☐ Implement a tool that automates control monitoring and evidence collection
- ☐ Define how issues will be identified, escalated, and remediated.
- ☐ Document ongoing monitoring activities and results.

08 Find an Auditor

- ☐ Identify audit firms that conduct SOC 2 audits.
- ☐ Verify that potential auditors have strong references or customer testimonials.
- ☐ Confirm that potential auditors understand your industry and customer expectations.
- ☐ Assess how well each auditor collaborates with your team.
- ☐ Confirm that the auditor answers questions clearly and in terms your team understands.
- ☐ Confirm the auditor's experience with companies of your size and stage.
- ☐ Select the auditor that best fits your organization's needs.

09 Undergo the SOC 2 Audit

- ☐ Confirm scope, timeline, and deliverables with your auditor.
- ☐ Provide all requested documentation and evidence for each in-scope control.
- ☐ Coordinate and schedule walkthroughs and interviews with control owners.
- ☐ Respond promptly to follow-up questions and additional evidence requests.
- ☐ Review the draft SOC 2 report from your auditor.
- ☐ Clarify any questions or discrepancies in the draft report.
- ☐ Receive the final SOC 2 report from your auditor.
- ☐ Share the final report with internal stakeholders and, as appropriate, with customers and prospects.