8-Step SOC 2 Checklist

1. Determine which SOC 2 report best suits your business' needs.

There are actually two types of SOC 2 reports that you can attain.

- ☐ **A SOC 2 Type 1 report confirms that, at a specific moment in time, your internal controls have been established to align with the SOC 2 checklist requirements.**

  A Type 1 report proves that your company has suitable controls in place to meet SOC 2 security standards, meaning it implies your company has the ability to keep data secure.

- ☐ **A SOC2 Type 2 report confirms that the controls you have in place are actually being implemented and maintained over a period of time.**

  A Type 2 report comes with a mandatory monitoring period of 3-6 months and proves that your company has effective controls in place to maintain SOC 2 security standards, meaning it confirms your company has the ability to keep data secure.

---

2. Define the scope of your audit by determining which of the 5 Trust Services Principles (TSPs) are relevant to your business.

The only TSP that is required for certification is Security; beyond that, the audit should be customized to your business' needs. Below are reasons to include the other TSPs, Availability, Confidentiality, Processing Integrity, and Privacy, in your audit.

Reasons You Would Include Each TSP in Your Audit

- ☐ Security - Mandatory for certification.
- ☐ Availability - Your customers, vendors, or partners have concerns about downtime. Only include if applicable to your business.

- [ ] Confidentiality - Your company retains confidential data under the protection of non-disclosure agreements (NDAs) or your clients have particular confidentiality requirements. Only include if applicable to your business.
- [ ] Processing Integrity - Your company performs essential customer functions like payroll management, financial processing, or tax processing. Only include if applicable to your business.
- [ ] Privacy - Your customers store PII. Only include if applicable to your business.

---

3. Conduct an internal risk assessment.

Effective risk management and evaluation play a vital role in your SOC 2 compliance process. It's essential to recognize and document potential risks tied to factors such as expansion, geographic location, and information security best practices.

Subsequently, you should assess the scope of these risks stemming from identified threats and vulnerabilities. Each identified risk should be evaluated in terms of its likelihood and impact, followed by the implementation of appropriate measures (controls) to minimize them in accordance with the SOC 2 checklist.

---

4. Perform gap analysis and remediation based on the results of your risk assessment.

Use the results of your internal risk assessment to determine how your company's existing policies, procedures, and controls measure up against SOC2 requirements and identify any gaps that need to be remediated through improved or new policies, procedures, and controls.

---

5. Implement stage-appropriate controls.

Each TSP has its own set of criteria that you will need to deploy internal controls for, but make sure the controls you are implementing are stage-appropriate for the size and maturity of your business. The controls required for large enterprises are very different from the controls required for startups. There are 61 controls in total, but remember, you only

need to implement the controls required to meet the TSP standards within the scope of your audit.

---

6. Take a readiness assessment.

Conduct a readiness assessment with an independent auditor to determine if you satisfy the minimum requirements listed in the SOC compliance checklist before proceeding with a comprehensive audit. Determining if you meet the requirements of the audit before the actual audit may seem redundant but it will save you time in the long run by capturing any gaps in your company's processes and policies, and allowing you time to make any necessary changes, before the official audit.

---

7. Conduct the audit.

Commission a certified independent auditor to complete your SOC 2 audit and generate a report. A Type 2 audit process can take anywhere from 2 weeks to 6 months, depending on how many corrections your auditor identifies. Since a Type 1 audit does not require any monitoring period, the process tends to be a less intrusive and less time consuming, assuming you enter the audit properly prepared to provide snapshot evidence that you have the proper systems and checks in place to meet the SOC 2 control requirements.

---

8. Implement continuous monitoring practices.

To maintain your SOC2 compliance you must perform audits annually. Ensuring the security of your business' data is a never ending process as attackers are continuously finding new ways to exploit any vulnerabilities in your environment and make it past your defenses. Be sure to stay on top of any new policies and procedures that were implemented to achieve your SOC 2 certification and continue to update your policies and procedures as needed to keep up with an ever evolving threat landscape.