ISPECTRA
TECHNOLOGIES

Develop | Defend | Comply

SOC 2 Compliance Checklist

ISpectra Technologies

www.ispectratechnologies.com

January 2026

Step 1: Choose Your Objectives for SOC 2 Compliance

It is important to understand why your organization needs a SOC 2 certificate and how it aligns with your business goals. Having clarity on this early helps guide decisions throughout the SOC 2 compliance journey.

- Many organizations pursue SOC 2 compliance because it is required by customers.
- SOC 2 also helps build a strong security-first culture within the organization.
- In some cases, organizations seek SOC 2 compliance to stay competitive when others in the industry are already certified.

Step 2: Identify the Type of SOC 2 Report You Need

To decide which SOC 2 report best fits your organization, you should first evaluate your current level of security and process maturity. This helps determine whether you are ready for a more comprehensive audit or should start with a simpler approach.

- Consider whether you have completed a SOC 2 audit before and whether the report is needed urgently within three months.
- Evaluate if you have dedicated resources to develop and implement security policies and if employees understand their roles in applying controls.
- Review whether systems are in place to communicate and manage system changes effectively.

If most of these areas are not yet mature, starting with a SOC 2 Type I audit is recommended, with a transition to SOC 2 Type II once controls and processes are fully established.

Step 3: Define the Scope of Compliance Based on the Trust Service Criteria (TSC)

You should define the scope of your audit by identifying which Trust Service Criteria you want to establish and test. The scope of the audit depends on your business model and customer requirements, and it determines which controls will be reviewed during the SOC 2 audit.

- **Security** - review whether security procedures are documented, backup and recovery processes are in place, and clear procedures exist to handle cyber safety incidents.
- **Availability -** consider service uptime, how service issues affecting availability are addressed, and whether access controls are implemented to manage who can access the service.
- **Confidentiality** - evaluate how confidential data is handled, whether access management is enforced, and what measures are in place to prevent unauthorized access.
- **Processing Integrity** - verify that systems provide timely and accurate data, data integrity is maintained, and errors can be identified and corrected quickly.

- **Privacy** - confirm that a documented data retention policy exists, personally identifiable information is stored securely, and appropriate protections are in place to safeguard PI

Step 4: Conduct an Internal Risk Assessment

An internal risk assessment helps the organization understand risks related to business growth, location, and information security practices. Once risks are identified, their likelihood and potential impact on the business are evaluated so they can be managed effectively.

- Critical systems are identified and tagged based on the level of risk involved.
- Mitigation strategies are developed to reduce the likelihood or impact of identified risks.
- These measures help ensure risks are tracked, controlled, and addressed in a structured manner

Step 5: Perform Gap Analysis and Remediation

After completing the internal risk assessment, organizations must identify control gaps related to existing and potential security threats. These gaps should then be addressed in line with the selected Trust Service Criteria to strengthen overall compliance.

- Controls should be aligned and implemented based on the chosen Trust Service Criteria.

- Clear organizational roles, security policies, and documented procedures should be established.
- Remediation efforts typically include employee background checks, peer review of code changes, regular security training, and collecting evidence to demonstrate compliance.

Step 6: Undergo Readiness Assessment

A readiness assessment helps determine whether your organization is prepared to meet SOC 2 requirements and move forward with a full audit. It is usually performed by an independent auditor to identify gaps early and reduce audit risks.

- The assessment reviews existing controls to identify vulnerabilities and missing requirements.
- Practical recommendations are provided to help the organization become audit-ready.
- Gaps are addressed by improving current controls or implementing new ones where needed.

Step 7: SOC 2 Audit

At this stage, you must authorize an independent certified auditor to conduct the SOC 2 audit.

During the audit process, you are required to address auditor queries, submitting the required evidence, and participate in walkthroughs as needed to support audit validation.

Step 8: Establish Continuous Monitoring Practices

SOC 2 compliance is a not one-time activity. Security is basically an ongoing process, and annual SOC 2 audits require continuous monitoring and maintenance of controls.

- Monitoring should be scalable and grow with the organization.
- Evidence should be collected in a manner so as not to impede employee productivity.
- Controls need to be constantly validated for alerts, visibility, as well as security through incident management, penetration testing, and vulnerability scanning.