SOC 2 Compliance Checklist

7 Steps To Prepare for an Upcoming Audit

1 Determine if a Type 1 or Type 2 Report Is Necessary

When it comes to SOC 2 compliance, determining the appropriate report type is crucial. Let's dive into the key factors that can help you make an informed decision:

1. **Have you completed a SOC 2 audit before?**
   If this is your first SOC 2 audit journey, starting with a Type 1 report may be ideal. A Type 1 report provides a snapshot of your organization's control environment at a specific point in time, offering a solid foundation to build upon for future compliance efforts.
2. **Do you need the report urgently?**
   If time is of the essence and you require a faster turnaround, a Type 1 report might be the way to go. It is generally less comprehensive than a Type 2 report, allowing for a quicker acquisition and delivery of the report.
3. **Do you have the resources to develop and implement security policies?**
   Developing and implementing robust security policies can be a resource-intensive process. If your organization has the necessary resources and infrastructure to establish and maintain these policies, opting for a Type 2 report is recommended. A Type 2 report covers a more extended period and assesses the effectiveness of controls over time, providing a more comprehensive evaluation of your organization's compliance posture.

By carefully considering these factors and answering the questions above, you can determine whether to start with a Type 1 or Type 2 report. Remember, both options offer benefits and serve different purposes in meeting your organization's compliance objectives.

2 Determine Your Scope

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

The five TSCs 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.

While security is mandatory, other categories, such as availability, confidentiality, processing integrity, and privacy, may or may not apply to your company. Consider these categories carefully to understand what is necessary to protect your information and demonstrate compliance.

3 Communicate Processes Internally

Effective internal communication is critical throughout the SOC 2 audit planning process. Engage with executive management and department leaders to ensure they understand their responsibilities in implementing SOC 2 controls and providing evidence to the auditor.

Communicating the audit's purpose, timeline, and expectations will best prepare employees for their obligations before, during and after the audit and ensure ongoing compliance with the framework.

4 Perform A Gap Assessment

Conducting a gap assessment, also known as a readiness assessment, is an essential initial step in your SOC 2 journey.

Evaluate your existing procedures, policies, and controls to assess your current security posture and identify any gaps that need to be addressed to meet the applicable requirements of the Trust Services Criteria.

A SOC 2 readiness assessment provides answers to questions such as:

- Is my business adequately prepared for a SOC 2 audit?
- Does my organization have effective controls and policies in place?
- Are there any security weaknesses or vulnerabilities present?
- If any, how can those vulnerabilities be remediated before the audit?

5 Remediate Control Gaps

Once the gap assessment is complete, prioritize remediation efforts to address control gaps and ensure compliance with SOC 2 requirements.

Collaborate with your team to review:

- policies
- formalize procedures
- make necessary software alterations
- integrate new tools and workflows

Closing these gaps before the audit takes place enhances your readiness.

6 Monitor and Maintain Controls

After remediating control gaps and implementing the necessary controls to achieve SOC 2 compliance, organizations must establish processes to monitor and maintain the implemented controls continuously.

Continuous monitoring is a crucial requirement of SOC 2. Consider implementing a tool that automates control monitoring and evidence collection, streamlining your ongoing compliance efforts.

7 Select An Auditor

Choosing the right auditor is paramount to a successful SOC 2 audit. The right auditor can do much more than conduct your audit—they can help you:

- Understand and improve your compliance programs
- Streamline your security and privacy processes
- Achieve a clean SOC 2 report

ALL IN ONE COMPLIANCE

Achieve SOC 2 Compliance with ISMS.online

Our powerful platform covers over 50 standards and regulations so it can grow as your business does.

Get started →

SOC 2

Completed	Awaiting Approval	Open	Overdue
198	23	76	0

Control Environment

Communication and Information

Risk Assessment

Monitoring Activities

Control Activities

Logical and Physical Access Controls