Scrut Automation SOC 2 Checklist

Ten steps for acing your audit and getting your report

STEP 1: Determine type of report needed

SOC 2 attestations come in two different types:

□ **Type I**: The auditor evaluates the design and sufficiency of controls to meet the American Institute of Certified Public Accountants (AICPA)'s Trust Services Criteria (TSC), at a single point in time. A Type I report does not, however, render an opinion on the operating effectiveness of the controls.

□ **Type II**: The auditor determines whether controls are operating effectively and as intended over a certain period, usually one year. Importantly, a Type II report includes an opinion on the operating effectiveness of controls and a detailed description of tests performed by the auditor.

Companies generally begin with a Type I report to become familiar with the process. If you have either an:

- urgent need to receive a Type II report; or
- existing and effective set of policies and controls

you may decide to proceed directly to a Type II report.

□ Mark complete

STEP 2: Choose trust service criteria

SOC 2 audits measure one mandatory and up to four optional TSC (determined by the organization undergoing the audit):

□ **Security(required):** the protection of

- information during its collection or creation, use, processing, transmission, and storage; and
- systems that use electronic information to process, transmit or transfer, and store information to meet company objectives.

Security-related controls prevent or detect:

- breakdown and circumvention of segregation of duties.
- system failure.
- incorrect processing.

- theft or other unauthorized removal of information or system resources.
- misuse of software.
- improper access to or use of, alteration, destruction, or disclosure of information.

□ **Availability:** The accessibility of information used by the company's systems, products and service.

□ **Processing integrity:** The completeness, validity, accuracy, timeliness, and authorization of system processing.
Evaluation of processing integrity addresses whether systems achieve their intended purpose without:

- impairment.
- error.
- delay.
- omission.
- unauthorized or inadvertent manipulation.

□ **Confidentiality:** The company's ability to protect information designated as confidential from collection/creation through final disposition/ removal. Information is confidential if the custodian is required to limit access, use, and retention and restrict its disclosure to defined parties. Confidentiality requirements may be contained in laws or regulations or in contracts.

□ **Privacy:** Although confidentiality applies to various types of sensitive information, privacy applies only to personal information. The privacy criterion includes requirements for:

- **Notice and communication of objectives:** The company provides notice to data subjects about its objectives related to privacy.
- **Choice and consent:** The company communicates available choices for the collection, use, retention, disclosure, and disposal of personal information.
- **Collection:** The company collects personal information to support its privacy objectives.
- **Use, retention, and disposal:** The company limits does these in accordance with its privacy objectives
- **Access:** The company provides data subjects with access to their personal information for review and correction.
- **Quality:** The company collects and maintains accurate, up-to-date, complete, and relevant personal information.

- **Disclosure and notification:** The company discloses personal information in accordance with its privacy objectives. It notifies affected data subjects, regulators, and other appropriate stakeholders following data breaches.

SOC 2 reports covering the privacy TSC are quite rare because business-to-business (B2B) customers rarely demand them. SOC reports with the privacy TSC also don't provide any guarantee of compliance with standards like the European Union (EU) General Data Protection Regulation (GDPR). Confidentiality and availability, however, are frequently included along with security.

□ Mark complete

STEP 3: Establish scope

SOC 2 reports do not necessarily need to cover every aspect of your company's operations. It is conceivable (and sometimes appropriate) to limit the audit to certain:

□ **Product lines:** For example, if your company provides Software-as-a-Service (SaaS) as well as customer-managed options, it generally makes sense to focus the SOC 2 report on the SaaS offering.

□ **Business units:** If you have certain business units that do not process customer or data, it might be reasonable to exclude them from the scope of the report.

□ **Geographical areas:** Similarly, if processing or storage of customer data does not take place at certain facilities or in certain regions, you do not necessarily need to include them.

Clearly establishing the scope of your audit ahead of time, rather than attempting to document exclusions in the middle of the process, will build trust with your auditor and ensure the process is smooth.

□ Mark complete

STEP 4: Assess gaps

Once you have determined which TSC you will pursue and what the scope of the audit will be, the next step is to identify gaps.

- □ **Are you just beginning your security program?**
- □ **Is there a program in place, but do you need to expand it to meet TSC requirements?**
- □ **Do you need to harmonize a program designed for another standard (e.g. ISO/IEC 27001) with SOC 2?**

Either an internal or external party can conduct this assessment. Once you have figured out where your areas for improvement are, you can move toward building (or enhancing) your security program.

□ Mark complete

STEP 5: Determine roles and responsibilities

Receiving a favorable SOC 2 report requires coordination throughout your company. Ensure stakeholders from all functional units understand their responsibilities, e.g.

- □ **Governance, risk, and compliance (GRC):** Manage the security program, SOC 2 audit process, and make recommendations about risk management.
- □ **Product management:** Make risk management decisions.
- □ **Human resources:** Administer employee background checks.
- □ **Engineering:** Patch software vulnerabilities within required timelines.
- □ **Information technology (IT):** Ensure departing employees no longer have access to company accounts and information systems.
- □ **All employees:** Conduct security awareness training, report phishing emails, and notify the GRC team about suspected incidents.

Establishing these will require senior leadership involvement to ensure appropriate prioritization.

Once you have determined roles and responsibilities, a critical next step is to memorialize them.

□ Mark complete

STEP 6: Document and communicate policies and procedures

The foundation of your security program are your documented policies. These lay down the roles and responsibilities agreed upon in the previous step while also laying out:

- □ **Risk appetite:** Policies establish how much risk a company is willing to take by identifying:
  - □ Vendor risk categorizations and compensating controls.
  - □ Bring-your-own-device (BYOD) requirements.
  - □ Timelines for fixing known vulnerabilities.
- □ **(Un)acceptable behaviors:** Your company should establish that certain activities are never appropriate using company systems, like:
  - □ Deploying malicious code.
  - □ Visiting gambling websites.
  - □ Working on for-profit personal projects.
- □ **Decision-making authorities:** Policies should not cover every single aspect of daily operations, but should rather clearly allocate duties to individual team members. These people should then establish detailed procedures laying out how to do important tasks, such as:
  - □ **Offboarding employees:** To ensure there is no residual access to company systems, a procedure for deactivating accounts, collecting hardware, and invalidating credentials is essential.
  - □ **Releasing information outside the company:** Coordinating with other companies and communicating publicly are key tasks for any business. With that said, employees should understand which types of data they can provide to whom, when, and who can authorize doing so.
  - □ **Checking for configuration errors in cloud resources:** Spinning up new virtual machines is something most DevOps teams do regularly. A standardized set of reviews prior to and immediately after doing so can prevent accidental data exposure or similar mishaps.

□ Mark complete

STEP 7: Validate controls

Once your controls are documented in the previous step, the next task is to confirm their implementation! Optimally this would be as automated as possible, via:

- □ **Evidence collection through integrations:** Tracking the security posture of your cloud assets and inventorying them is best done continuously and through machine interfaces. Having a compliance platform with these features will save tons of time throughout the SOC 2 lifecycle.
- □ **Centralized risk registers:** Staying on top of new and emerging risks as well as tracking appropriate actions to completion is difficult to do with spreadsheets and emails.
- □ **Employee awareness tracking and training:** Training and regularly updating your workforce is a key security task. A central portal with full visibility on everyone's status will make sure no one falls through the gaps.

Additional measures to consider are;

- □ **Penetration testing:** While not required by SOC 2 explicitly, having an expert manually check your network defenses can go a long way to confirming their security.
- □ **Continuous vendor monitoring:** Automated scanning tools can help track vulnerabilities and other issues present on the exterior of other company's networks.
- □ **Phishing simulations:** Testing the ability of your users to identify simulated fraudulent requests for information or funds can help them avoid falling victim to real world ones.

□ **Mark complete**

STEP 8: Find an auditor

Once you have confidence your controls are working as designed, it's time to find an auditor to confirm their effectiveness. Some key things to look for when considering an auditor are:

- □ **Knowledge of your technology stack.**
- □ **Experience with your industry.**
- □ **Communication style.**

- □ AICPA peer-reviewed.
- □ Reputation.
- □ Cost.

Businesses need to balance a wide array of considerations when determining how to have their security and compliance program audited. Picking the right partner is an important step in receiving a SOC 2 attestation.

STEP 9: Provide evidence

With the engagement letter signed and the audit underway, it's time to provide evidence of your control appropriateness and effectiveness!

A Type I audit will focus on the design of your controls (mainly policies and procedures) at a certain point in time. The evidentiary and testing burden will be relatively less than a Type II audit. For these examinations, expect to provide evidence that you are meeting your requirements through things like:

- □ Emails.
- □ IT service tickets.
- □ Meeting invitations, minutes, and recordings.

Producing this documentation can itself be a huge burden, which is why a compliance automation platform can be so helpful here. The right tool can let you collaborate directly with auditors using it. Rather than manually capturing screenshots and uploading them to shared drives, a solid GRC platform can cut through this toil and give auditors what they need, on demand.

□ Mark complete

STEP 10: Receive attestation

Once your examination is done, it's time to get your attestation. Unlike ISO/IEC 27001 and other standards, however, you won't receive a "certificate." You'll get a detailed report from auditors with one of the following four types of opinions:

- □ **Unqualified:** This is the best outcome as it means your controls were designed properly and operating effectively (if Type II). It's possible that not every control worked perfectly, however. Be prepared to answer customer questions about these issues if documented in the report and develop a corrective action plan to address them.
- □ **Qualified:** This means one or more controls were not appropriately designed or implemented and it has a material impact. How severe this opinion is will depend on exactly which controls failed the audit. If a customer is only hosting publicly-available data on your service and one of your controls for confidentiality didn't pass muster, it might not be a huge problem for them. If you are storing personally identifiable information, however, this could be a big issue.
- □ **Disclaimer**: This outcome means the auditor didn't get enough information from you during the process to make an informed decision. This would be a major red flag for customers because it means your company didn't take the audit seriously enough or, even worse, was actively withholding data.
- □ **Adverse:** The worst (and rarest) outcome, this opinion means there were pervasive and material weaknesses in your controls or the auditor encountered consistent misstatements about them.

□ **Mark complete**

Need to get SOC 2 ready?

Scrut Automation is the leading compliance automation platform for mid-market businesses. We have helped dozens of companies get ready for - and through - SOC 2 audits without wasting time or money.

Partner with us for audit readiness and a robust cybersecurity foundation

Book a demo today