SOC 2 Compliance Checklist

Preparing you for your upcoming audit

Step 1: To determine whether SOC 2 report is needed

□ Are you planning to sell your products and services internationally, especially in the US?

□ Have you been receiving a lot of security questionnaires from your clients and prospects?

If your answer to above is 'yes' then its necessary for you to obtain a SOC 2 report to be able to expand your business internationally without any hiccups.

Step 2: Select your report type

Do you know which SOC 2 report type is right for your organisation? Here's how you can determine:

□ Has your organisation engaged in a SOC 2 audit before?

□ Are you evaluating the design effectiveness of controls at a single point in time?

□ Are you evaluating the design and operational effectiveness of controls over a period of time?

□ Is their an urgency in obtaining the report or any contractual requirements?

If you've never obtained a SOC 2 audit before and are looking to evaluate your design and operational effectiveness, the right way to start is with a Type 1 report. This can be acquired faster than a Type 2 report.

Step 3: Establish a Compliance Team & Engage a SOC 2 Auditor

Designate a team that's responsible for this project, this includes internal team, auditors plus if you do not have the band width to do the implementation part, engage with external implementors who can guide you better through the SOC 2 journey.

□ Does the auditor and implementor fit the business culture

□ Do they understand your industry?

□ Organise meetings with stakeholders to communicate the necessary know-hows of the audit to prepare the employees of their obligation

Engage with a team that is eager to understand and improve your security and compliance, streamline the process, and ultimately achieve a clean SOC 2 report.

Step 4: Define the scope

Determine which of the Trust Service Categories (TSC) you want to measure against. The TSC you choose will depend on your industry and customer needs.

- □ **Security (mandatory):** Information and systems are protected against unauthorised access, unauthorised 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 authorised 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.

It's not necessary to include all five TSCs. Security is a mandatory category and depending on your business needs the other four can be included.

Step 5: Conduct a Readiness Assessment

Identify current controls and compare them against SOC 2 requirements to find gaps. You can then evaluate potential risks to data security and privacy.

This can be done by:

- □ Perform a gap analysis to see which SOC 2 criteria meets the requirements or are missing.

Step 6: Ensure Ongoing Government Controls

Establish robust logging and monitoring mechanisms and ensure SOC 2 control mandates are being achieved.

Work with your team to:

- □ Review policies
- □ Formalise the processes and procedure

Step 7: Ensure Implementation of Technology Controls

Establish adequate technical controls.

Work with your team to implement:

- □ Security logging
- □ Vulnerability management
- □ Antivirus
- □ Patching and hardening
- □ Encryption
- □ Architectural diagram

Step 8: Ensure Implementation of People Controls

Train your employees on information security best practices, incident response procedures, and their responsibilities in maintaining the organisation's security posture. Outline the processes you have in place to your customers ensuring that their data is in safe hands.

Try to outline the following:

□ Employee awareness and training

□ Ensure employees sign security and compliance policies

Step 9: Implement Monitoring and Reporting

Use tools and processes to continuously monitor compliance with SOC 2 controls.

If you haven't already:

□ Implement ongoing control reviews and evidence collection

□ Schedule security and compliance risk reviews

Step 10: Internal Audit and Review

Regularly review controls and processes to ensure they meet SOC 2 standards.

See if you have:

□ Addressed the findings by implementing corrective actions for any issues identified during the SOC 2 readiness assessment

Step 11: Undergo SOC 2 Audit

You've probably begun your SOC 2 audit process. Once you provide all the necessary information to your auditor, they will review evidence for each in-scope control, verify information, schedule walkthroughs and provide a final report.

Working with the best across industries

NETVALUE BETTER BUSINESS · Spectrum care Te Wai Kohukura Atawhai · Figured · Harmoney · HYUNDAI NEW ZEALAND · FIJI AIRWAYS · SolarZero

eventfinda · atomic · NEW ZEALAND Family Planning · OCEANIA Believe in Better · Cone Marshall · APEX

AMARU, a leading information security and compliance service provider, offering end-to-end managed cyber security services across Australia and New Zealand.

www.amaru.co.nz hello@amaru.co.nz