matomo

A STEP-BY-STEP **CHECKLIST** FOR **SOC 2 COMPLIANCE**

Step 1: Define Your Objectives

Understand the specific reasons your organisation seeks SOC 2 compliance.
Objectives can vary based on client demands, regulatory requirements or internal security goals.

- [ ] Engage with clients, partners and internal teams to understand their expectations. What are the most critical factors for them? Clients in highly regulated industries like finance and healthcare may prioritise privacy.
- [ ] Set clear goals and define what the results are going to be. (Improved data security posture or increased competitiveness?).
- [ ] Create a formal document outlining compliance goals and how they align with business objectives. At this point, make sure that executive management understands the importance of SOC 2 compliance and is committed to providing the necessary resources and budget for the initiative.
- [ ] Determine the tools and software necessary for compliance, such as compliance management platforms or security software. For example, consider using Matomo for analytics and monitoring user data to comply with privacy standards.

Step 2: Select Your SOC 2 Report Type

Based on organisational needs and readiness, determine whether a Type I or Type II SOC 2 report would be needed.

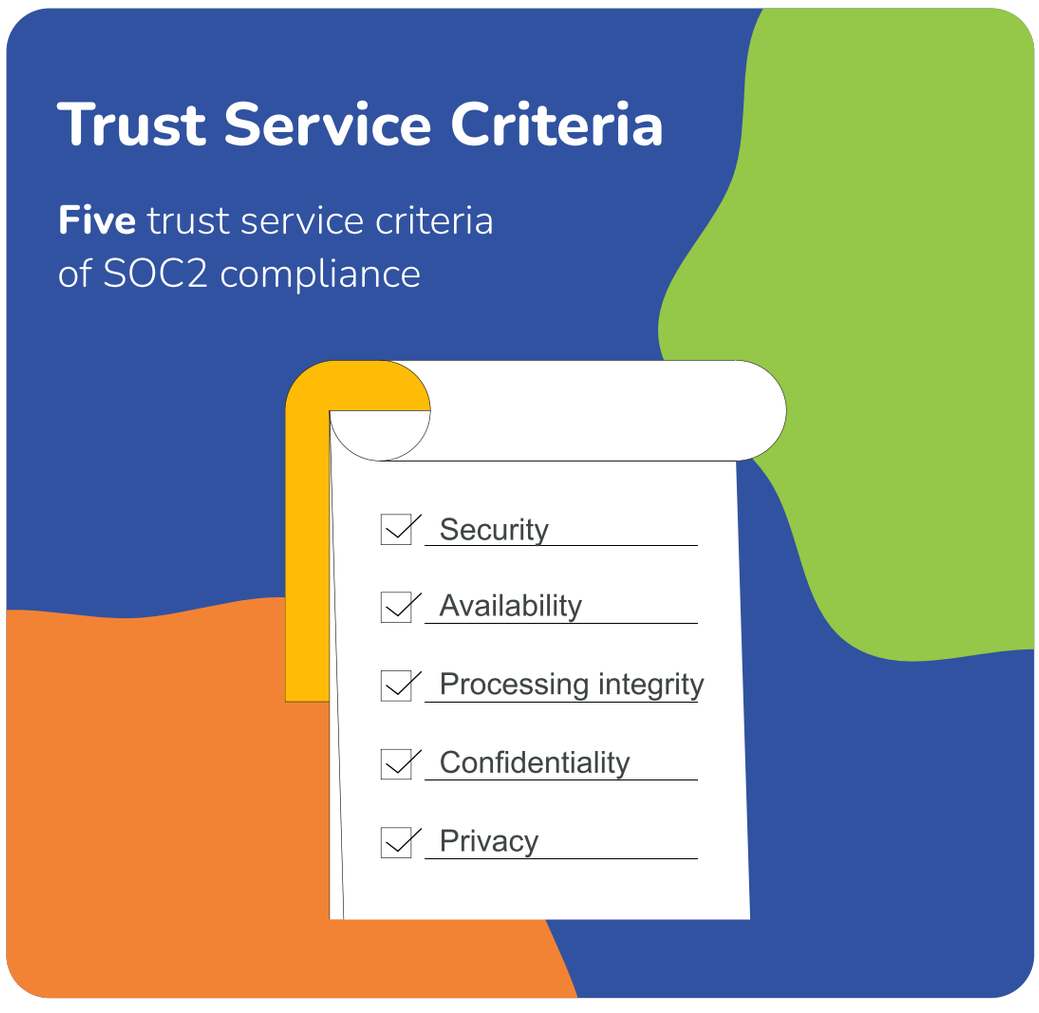
- [ ] For Type I assessment: Review existing controls and their design as of a specific date. This is suitable for organisations just starting their compliance journey.
- [ ] For Type II evaluation, Plan for a longer-term assessment of control effectiveness over a defined period (typically 6-12 months). This demonstrates a strong, ongoing commitment to data security.

It is also a good idea to engage with a third-party auditor to understand which report type best suits an organisational context.

Step 3: Establish The Scope

Establish the scope of efforts to maximise the results.

- [ ] Determine which specific services or systems the SOC 2 audit will cover. For example, if an organisation offers cloud storage services, those should be included in the scope.
- [ ] Identify which Trust Service Criteria (TSC) are most relevant. Choose applicable criteria from:
  - [ ] Security
  - [ ] Availability
  - [ ] Processing integrity
  - [ ] Confidentiality
  - [ ] Privacy



- [ ] Remember that not all five TSCs need to be included in the audit. A targeted approach allows better focus on the most valuable criteria.
- [ ] Outline the scope in a formal document to guide future compliance activities.

matomo

Step 4: Facilitate Internal Communication And Assign Owners

Assigning specific responsibilities ensures that all team members understand their roles in the compliance process.

- [ ] Specify who is responsible for each task in the audit checklist. For example, the IT security manager will implement technical controls related to security and confidentiality. Create accountability structures and use project management tools to track responsibilities and deadlines.
- [ ] Schedule regular meetings to discuss progress, address challenges and share updates.

Step 5: Align Your Controls With TSC

Check whether you address specific controls required by the selected TSC.
To do this, here are some things you can do for specific TSC:

- [ ] **Security controls implementation:** Set up access controls, firewalls and intrusion detection systems.
- [ ] **Availability measures:** Develop redundancy plans, load balancing strategies and disaster recovery protocols.
- [ ] **Processing integrity checks:** Implement data validation processes and error-checking mechanisms.
- [ ] **Confidentiality safeguards:** Use data encryption and access restrictions for sensitive information.
- [ ] **Privacy protocols:** Establish privacy policies that comply with regulations like GDPR or CCPA.

Step 6: Conduct An Internal Risk Assessment

Identify potential data security and compliance risks by evaluating the likelihood and impact of various threats.

- [ ] Conduct sessions with key stakeholders to brainstorm and compile potential risks.
- [ ] Create a scoring system to evaluate risks based on their likelihood and impact. For example, score 1 for a rare risk and 5 for almost certain. Or 1 for an insignificant risk and 5 for a catastrophic one.
- [ ] Maintain a risk register that details identified risks along with mitigation strategies.

Step 7: Perform Gap Analysis And Remediation

Evaluate existing controls against SOC 2 requirements to identify discrepancies.

- [ ] Review each control against SOC 2 requirements to identify deficiencies.
- [ ] Rank gaps based on risk level and impact on compliance efforts.
- [ ] Develop an incident response plan outlining roles, responsibilities and procedures for managing security incidents.
- [ ] Train staff on the new plan so everyone understands their role in responding quickly.

Step 8: Implement Relevant Controls And Test Them

Put the necessary controls identified during previous steps in place and check for their functionality.
Key activities:

- [ ] Identify which SOC 2 controls are currently in place. Based on the gaps identified, determine which additional controls need to be implemented. Develop detailed plans for implementing each control, including timelines and responsible parties.
- [ ] Create procedures for testing the effectiveness of controls (e.g., penetration testing, vulnerability scanning, and control walkthroughs).
- [ ] Schedule periodic tests to verify that controls are functioning as intended.

Step 9: Undergo Readiness Assessment

Conduct an internal review to confirm that all necessary preparations are in place before the formal audit begins.

- [ ] Perform internal audits that simulate the actual SOC 2 audit process.
- [ ] Keep all policies, procedures and evidence well-documented and accessible.
- [ ] Identify any remaining/last-minute concerns or gaps that need resolution.

Step 10: Complete The SOC 2 Audit

Engage an independent auditor to assess compliance efforts and generate the final report.

- [ ] Choose a reputable firm experienced in SOC audits.
- [ ] Be available for questions and clarifications throughout the audit process.

Step 11: Monitor Continuously

Regularly assess controls to maintain compliance over time. Key tasks:

- [ ] Set up systems for ongoing monitoring of controls (e.g., automated alerts).
- [ ] Schedule periodic reviews of compliance status with relevant teams.
- [ ] Revise policies and procedures in response to changes in regulations or business practices.