SOC 2 Type II Compliance Checklist

Step 1: Determine audit scope

□ Determine your applicable Trust Services Criteria

□ Define which systems, data, people, and software is in scope for your audit and selected TSC

□ Select an audit window (3,6,9, or 12 months)

Step 2: Conduct a risk assessment and gap analysis

□ Identify information assets and potential risks to each one

□ Determine the likelihood each risk could occur

□ Evaluate the potential business impact of identified risks

□ Rank risks based on the overall risk to your organization

□ Create a treatment plan for each risk

□ Identify gaps in your current security controls manually if not using an automated tool

Step 3: Create a remediation plan

□ Select, develop, or modify controls to address identified gaps

□ Identify owners for each risk/control and a timeline for remediation

Step 4: Implement SOC 2 controls and policies

□ Create or update policies and controls and share with employees for review

□ Complete security awareness training for employees

□ Educate employees on any disciplinary actions that may take place if they fall out of compliance with data security requirements

Step 5: Gather documentation and evidence

□ Collect and organize policy documents or screenshot evidence for your auditor throughout your audit window

secureframe

SOC 2 Type II Compliance Checklist

Step 6: Complete a readiness assessment

- □ (Optional) Select a service auditor to perform the readiness assessment. Then review the service auditor’s letter and implement any suggestions.
- □ Conduct an internal readiness assessment. Map existing controls to your chosen TSC, check for gaps, and develop a remediation plan.

Step 7: Undergo your SOC 2 audit

- □ Select an accredited SOC 2 auditor to conduct your Type II audit
- □ Obtain any feedback and implement any advice from the auditor

Step 8: Maintain compliance

- □ Hold management reviews at least annually (recommended quarterly)
- □ Perform annual risk assessments
- □ Perform ongoing control effectiveness monitoring to ensure SOC 2 policies and controls remain appropriate and effective
- □ Monitor any new or elevated risks and implement revised security controls
- □ Document and track and nonconformities and corrective actions to closure
- □ Schedule a SOC audit every 12 months