SOC 2 Compliance Checklist

Service providers can implement and maintain SOC 2 in many ways. It may be challenging to understand the sequence of events when starting the SOC 2 process.

So, are you ready to begin your SOC 2 audit preparations?

01 Choose objectives

The first action item of the SOC 2 audit checklist is to determine the purpose of the SOC 2 report. Service providers usually start with a SOC2 Type 1 report and then build up to SOC2 Type 2.

02 Choose appropriate TSCs

The second action item is to determine the applicable TSCs (security, availability, confidentiality, privacy, and processing integrity) based on the type of data stored or transmitted by the service provider.

03 Perform gap analysis and remediation

Next, a SOC 2 compliance team will examine the procedures and practices of the service provider and compare its compliance posture with that of SOC 2 best practices.

The team will draw up a remediation plan to tackle the identified gaps. Depending on what the gap analysis reveals, the remediation period could take between two months and nine months.

It forms the bulk of the process wherein the service provider could end up bringing in new employees or altering their software development process to meet requirements.

04 Implement stage-appropriate controls

Controls required for large enterprises are quite different from those needed by startups. A compliance team identifies methods to save time and money by implementing strategic processes and tools.

05 Perform a risk assessment

The SOC 2 compliance team performs a risk assessment when control implementation is nearly 80% complete. This is a crucial step as it identifies any risks associated with growth, location, or infosec best practices.

06 Prepare for SOC 2 audit

After risk assessment and mitigation, the service provider gathers evidence of controls implemented effectively and compiles it for the auditor.

It also puts together an internal team that will work with the auditor during the audit process and field questions.

07 Execute the SOC 2 audit

SOC 2 audits may take between two weeks to six months, depending on the volume of corrections or questions raised by the auditor.

Although technically a service provider cannot “fail” a SOC 2 audit, it will want to correct discrepancies to ensure that it receives a good report.

08 Maintain compliance over a 12-month period

Since SOC 2 audits must happen annually, it helps to put in place automation tools that gather evidence and track practices over time.

This saves team members’ time while keeping data secure.