

SOC 2 Compliance Checklist

Chances are, you have a basic understanding of SOC 2 compliance and what it can do for your company to be certified. Without compliance requirements, it would be practically impossible for clients to verify which vendors have proper cybersecurity in place.

But do you know what it actually takes to get your business certified?

One of the most common compliance frameworks we see is SOC 2. Reaching SOC 2 certification is a demanding undertaking. We developed this SOC 2 checklist to help guide you and your organization through the SOC 2 compliance journey.

DEFINE AUDIT SCOPE

IDENTIFY POLICY GAPS

CLOSE POLICY GAPS

IDENTIFY PROCEDURE GAPS

CLOSE PROCEDURE GAPS

DEFINE CONTROL OWNER

During this step, you should begin implementing SOC 2 controls. Dues dates and task priority should be defined in this step as well.

SOC2 TYPE 1 INTERNAL AUDIT

Depending on what SOC 2 type you are going after will determine the next steps in this checklist. Type 1 audits only evaluate your security based on one day.

Did you know that it isn't necessary to get the Type 1 certification before Type 2? However, Trava recommends it because it helps ensure that you have all controls properly in place before months of monitoring.

READINESS ASSESSMENT

PROVIDE EVIDENCE

REVIEW EVIDENCE

IDENTIFY EVIDENCE GAPS

RESOLVE EVIDENCE GAPS

FINAL EVIDENCE REVIEW

CONTINUOUS MONITORING

EXTERNAL AUDIT

PLATFORM ACCESS TO AUDITORS

ONSITE AUDIT FIELDWORK

DRAFT REPORT DELIVERY

DELIVER FINAL REPORT

SOC2 TYPE 2 INTERNAL AUDIT

Unlike Type 1 audits, Type 2 audits are earned over an extended period of time.

REVIEW PERIOD

READINESS ASSESSMENT

PROVIDE EVIDENCE

REVIEW EVIDENCE

IDENTIFY EVIDENCE GAPS

EXTERNAL AUDIT

ONSITE AUDIT FIELDWORK

DRAFT REPORT DELIVERY

FINAL REPORT DELIVERY

Still see this process as being overwhelming? Trava can also help [guide customers through the compliance process](#). Want us to help assist?

talk to trava