# Lesson 3 | SOC 2 Reports

Updated 2020-09-15

SOC 2 Reports are increasingly used by software companies that serve other businesses as customers. These reports are a means to measure and show how your company is performing against the SOC 2 controls to which you attest.

These reports are validated by 3rd party auditors. They provide assurances to partners and customers that you have committed to certain controls and are addressing those controls. Some companies will now proactively ask if customers want to see their SOC 2 reports. In these circumstances, reports are shared under NDA.

There are two different types of SOC 2 Reports - Type 1 Reports and Type 2 Reports. It's important to understand the differences.

**SOC 2 Type 1 Reports.**

These reports audit the defined policies and procedures of an organization. For the controls that are in scope for the SOC 2 report, a Type 1 report tests to see if there are policies and procedures that address these controls. This is the first step in the SOC 2 process after the scoping of controls and trust services criteria.

This type of report can be obtained in a very short of time once you start an engagement with a 3rd party auditor.

These reports are less rigorous as they do not check to see whether the policies and procedures are actually being followed on a consistent basis. As such, they provide less assurance to customers.

**SOC 2 Type 2 Reports.**

These reports audit the implementation of policies and procedures. This type of report is issued after a Type 1 Report. Type 2 reports review internal processes and documentation to ensure that the policies and procedures from the Type 1 Report are actually implemented and being followed.

There is a defined time period between your Type 1 Report and Type 2 Report. This period of time is called your reporting period. The reporting period is the period in which the implementation of your policies and procedures is assessed. Consider the entire reporting

period to a period in which you need to show evidence that you are following your policies and procedures.

From our experience, the most common length of time for a reporting period is 12 months but we have also seen as short as 6 months. 12 months is probably the ideal but sometimes there are reasons to do a shorter reporting period. Some startups do a shorter period of time because they are eager to get a SOC 2 Type 2 Report.

The SOC 2 Type 2 Report is more rigorous than a Type 1 report so is more readily accepted by companies as evidence of good cybersecurity practices.

---

*SOC 2 Reports are valuable in building trust with your partners and customers. A SOC 2 Type 2 Report goes deeper than a SOC 2 Type 1 Report in that it assesses the operation, not just the definition, of your security program.*