Haekka

Lesson 4 | SOC 2 Recap

Updated 2020-09-15

By now, you should have a basic understanding of SOC 2. Below is a quick refresher.

SOC 2 is different from SOC 1 and SOC 3. SOC 2 is focused on internal controls around security and technology. SOC 1 is focused on financial controls. And SOC 3 is for public use, while SOC 2 is restricted use, meaning it is usually only shared with partners and customers and only under NDA. There is also SOC for Cybersecurity, which is more focused on risk management than information security.

SOC 2 has 5 trust services criteria:

1. Security
2. Confidentiality
3. Integrity
4. Availability
5. Privacy

Security is the only criteria required to be in scope for all SOC 2 reports. It is referred to as the Common Criteria. The other criteria are optional and should be chosen based on the specific needs of your company and what you need to validate for your customers.

SOC 2 has two types of reports:

1. SOC 2 Type 1 Reports are a point in time assessments that evaluate if you have policies and procedures to address the SOC 2 controls that are in scope.
2. SOC 2 Type 2 Reports assess a period of time to evaluate the effectiveness of your policies and procedures (are you following them).

SOC 2 has become the industry standard for validating an information security program. While the criteria in scope and the ways in which controls are met are flexible, the SOC 2 report itself is increasingly expected by companies before they start working with you. It is often easier to be proactive about security and offering SOC 2 reports to potential customers is a great way to put them at ease about how you will handle their data.

In order to get a SOC 2 report, you need to work with an approved auditor. Auditors are approved by the AICPA. An auditor will work with you to define the scope of your report. They will then assess if you have policies and procedures in place to address in-scope SOC 2 controls. Controls apply to people, technology, and partners/vendors. There is a lot of data collection during an audit.

If you are just getting started with security auditing and setting up your information security program, it may take some time to find your gaps and to address those gaps. In terms of SOC 2 Type 1, gaps are simply controls that you need to meet and to which you do not have policies and procedures in place to meet them. For SOC 2 Type 2, gaps are when you have not implemented certain policies and procedures.

A SOC 2 Type 1 Report can typically be issued quickly as it is just a point in time assessment. SOC 2 Type 2 Reports take anywhere from 6-12 months so do not expect to have those quickly.

After the initial SOC 2 Type 1 and Type 2 reports for a company, there is not an industry standard or AICPA rule for how long reports stay relevant. Most companies will do a SOC 2 Type 2 Report each subsequent year. By following this cadence, they always have a SOC 2 Type 2 Report that is under a year old and with a recent reporting period.

This is the last lesson in this SOC 2 Primer Course. If you work for a company that has or is working to get a SOC 2 report, there is one training requirement for SOC 2 - Security Awareness Training. In order to comply with SOC 2 Common Criteria controls, specifically control CC2.2, all employees should receive some form of Security Awareness Training on a regular schedule. Most companies do this at least at onboarding and then annually.

If you want to get into the nitty-gritty of SOC 2 criteria and controls, our SOC 2 In-Depth course is a good next step.