Lesson 2 | SOC 2 Trust Services Criteria

Updated 2020-09-15

SOC 2 contains controls. These controls, or trust criteria, are things that you need to meet as a company. They can be very detailed.

These controls are put into buckets called Trust Services Criteria. As a company goes through SOC 2, it chooses which criteria, and corresponding controls, fall within the scope of the assessment and ultimately the SOC 2 report. These criteria and controls are the same for both SOC 2 and SOC 3 reports.

Security (the Common Criteria)

The Security category is universal to all SOC 2 audits so is not optional. It is sometimes called the Common Criteria. Many companies, especially startups and/or those doing their first SOC 2 assessment, only attest to the Security category. The Common Criteria covers information security, making it the equivalent of a cybersecurity certification. These criteria are identified as CCx.x, where x is a number.

Confidentiality

This criterion is focused on a specific type of data - confidential information. These controls require that you identify, protect, and then ensure the destruction of confidential information. These criteria are identified as Cx.x, where x is a number.

Integrity (or Processing Integrity)

This criterion contains controls to ensure the accuracy and completeness of data. The controls require that you identify data required and then monitor inputs and outputs to ensure integrity of the required data. These criteria are identified as PIx.x, where x is a number.

Availability

As the criterion name implies, the focus is on uptime and recovery. Broadly speaking, controls apply to capacity planning and disaster recovery. These criteria are identified as Ax.x, where x is a number.

Privacy

The privacy criterion contains controls that are similar to the rules of personal data protection regulations such as GDPR and CCPA. These controls require that there is transparency in the types of personal data collected, the methods of collection, and the use of personal data. There are also controls to allow users to get copies of personal data as well as request deletions and changes to their data. These criteria are identified as Px.x, where x is a number.

Beyond Security, which is required for all SOC 2 reports, the other 4 service criteria are optional and typically chosen based on the specific needs of the company.

For example, if your company offers a technology product or service that is mission-critical, meaning if the product goes down then harm is done to the users and customers of the product, Availability would be a good choice for trust service criteria to help prove to customers that the product will have minimal or no downtime.

If privacy and transparency of data use are paramount for your customers, then choosing the Privacy service criteria can help prove that you respect the privacy of data.

Work with your auditor to determine what criteria to include in the scope of your SOC 2 report. It's usually best to start with just the Common Criteria if this is your first SOC 2 assessment.