SOC 2 Examination Scoping Guide

It's really good news that you are on your way to becoming SOC 2 certified! Preparing for a SOC 2 examination requires that you understand several factors that will drive the scope and cost of your examination. With this information, you can take control and more easily solicit quotes from SOC service providers.

The factors to know include the following:

1. System Definition: You will need to define the "system" that provides products and services to your customers. It is important to understand that your definition of the system is a combination of the infrastructure, software, people, data, and procedures used in providing products and services to customers. The system can be comprehensive and include multiple processes and applications, or a specific subset of a comprehensive system. The discussion of your system is referred to as the "system description" in a SOC 2 report.

   See our guidance on helping you Define your System

2. Trust Services Categories: You will need to select the appropriate trust services categories to be included in the scope of your examination. You should understand that the selected trust services categories drive what your description addresses and what is examined by the service auditor. The selection of trust services categories depends on:

   a. The industry in which you and your customers operate, especially if it is highly regulated
   b. The product and services you provide
   c. Whether your system collects, processes, uses, transmits, or stores non-public personal information (NPPI)
   d. What trust service categories your customers are requiring

   See our guidance on Trust Services Categories and Criteria

3. SOC Examination Type: You will need to decide if you want a SOC 2, Type I or Type II examination. A SOC 2, Type I is typically only performed during your first year of certification if you are not ready for a Type II. A SOC 2 Type I examination only provides an opinion on the fairness of the description in meeting service commitments and system requirements for the selected trust services categories. A SOC 2, Type II provides an opinion on the fairness of the description and the operating effectiveness of controls described for the selected trust services categories.

4. Service period: You will need to determine the period the SOC 2 examination covers. For a SOC 2, Type I examination, the service period will be a point in time, or as of a certain date. For a SOC 2, Type II examination the service period will be over a period of time that is typically 3 to 6 months your first year and 12 months thereafter.

5. Subservice organizations: You will need to determine how supporting vendors or subservice organizations are treated. If subservice organizations are used to provide a product or service that directly or indirectly supports the provision of your product or service, they must be disclosed in your SOC report. A subservice organization may be carved out of your report, where the products or services provided are excluded from the scope of the examination, or included in the scope of the examination. If a subservice organization is included in the scope of the examination, their system is also described in your report.

6. Additional subject matter: You will need to decide if you want to include additional security and privacy compliance criteria in the scope of the examination. These criteria may be defined in NIST's Cybersecurity Framework, HIPAA/HITECH regulations, the Cloud Security Alliance's Cloud Control Matrix (CCM), ISO: 27001, or the GDPR regulation to name a few.

SOC 2 Services is here to help you understand the factors that drive the scope and cost of your examination. Please contact us at www.SOC2services.com or call us at (352) 602-8140 to determine your SOC 2 examination needs.