Trust Service Categories and Criteria

As discussed in our **SOC 2 Examination Scoping Guide**, you will need to select the appropriate trust services categories to be included in the scope of the examination. You should understand that the selected trust services categories drive what your system 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

A SOC 2 examination is performed in accordance with AICPA standards and one or more trust service categories selected by you. At a minimum, the security trust service category is always required. Trust service categories define the attributes of the description of the system being reported on, and are used to group service commitments and system requirements made to customers in common areas. The five (5) trust service categories defined by the AICPA include the following:

1. Security: Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives. Security refers to protection of information and systems used to collect, process, use, transmit, and store information.

2. Availability: Information and systems are available for operation and use to meet the entity's objectives. Availability refers to the accessibility of information and the systems used to provide products and services to customers.

3. Processing Integrity: System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives. Processing integrity applies at the system level.

4. Confidentiality: Information designated as confidential is protected to meet the entity's objectives. Confidentiality refers to the protection of information classified as confidential during its collection, use, disposition, and destruction. Confidentiality applies to various types of sensitive information, whereas privacy, as described below, applies to personal information (PI).

5. Privacy: Personal information is collected, used, retained, disclosed, and disposed of to meet the entity's objectives.

Each trust service category has specific trust services criteria that are used as benchmarks to assess the design and operating effectiveness of the description of your system and the internal control framework that supports it. For each of the trust service categories selected, the applicable trust service criteria should be addressed in your policies, procedures, and controls. Because many of the trust services criteria are high-level, there is often confusion in the interpretation of exactly what the criteria require.

Thirty-three (33) trust services criteria (referred to as common criteria) apply to every SOC 2 examination along with the security category. There are three (3) criteria for the availability trust service category, five (5) criteria for the processing integrity category, two (2) criteria for the confidentiality category, and eighteen (18) criteria for the privacy trust service category.

Note that the trust service criteria for all categories is defined in the **AICPA provided Trust Services Criteria 2016 to 2017 Mapping document.**

SOC2 Services is here to help you understand what trust service categories apply to your organization. Please contact us at www.SOC2services.com or call us at (352) 602-8140 to determine your SOC 2 examination needs.