SOC 2 Trust Services Criteria

Let's take a deep dive into the SOC 2 Trust Services Criteria and help you with a clear and transparent understanding as you start the process of a SOC 2 attestation. The SOC 2 Trust Services Criteria are the criteria that form the basis of a SOC 2 audit, relying heavily on info security and information privacy best practices. The subsequent 5 Trust Services Criteria may be used once acting a SOC 2 audit.

- Security
- Availability
- Confidentiality
- Processing Integrity
- Privacy

Simply explicit , after you plan to lead off the road towards SOC 2 compliance, you and your SOC 2 auditor can ultimately verify that which one of the 5 Trust Service Criteria are enclosed inside the scope of the engagement. Let's take a glance at each of them:

Security: The Security TSC is that the most ordinarily assessed and the reason being that it basically sets the foundation for the whole audit. In fact, the overwhelming majority of service organizations enterprise SOC 2 compliance elect simply the Security TSC, and nothing else. This can be usually the case as they start to move into the world of compliance. After few years, it's common to include an extra TSC's as a part of the general audit scope. Ultimately, it depends on the requirement of your customers and what they demand and expect in terms of compliance.

As to the scope of the Security TSC, it assesses a wide-range of baseline info security and operational controls. It forms the foundation of a SOC 2 audit. A number of the areas enclosed are following:

- Access management
- Risk Assessment
- Physical Security

Availability: The Availability TSC revolves round the concept of having systems online, functioning and communicating as necessary for business operations. For service organizations with cloud/SaaS offerings, the availability TSC is a vital component of a SOC 2 report.

Confidentiality: The Confidentiality TSC, should not be confused with the Privacy TSC (which it's at times), moves around the concept of identifying, designating, and ultimately, protecting confidential information. For different types of data, it may be info like person recognizable info (PII), Protected Health info (PHI), or more can be deemed as confidential. Confidentiality additionally needs fitting measures for destroying such info, as necessary.

Privacy: The Privacy TSC has become relatively necessary in recent years, due to increasing need for the use, disclosure, and notification of sensitive data, much of it in the way of consumer data. In addition, laws like the GDPR and CCPA have shined a whole new light onto the ecosystem of information privacy. As a result, there's been a noticeable increase in terms of service organizations including the Privacy TSC inside the scope of their SOC 2 audit.

Processing Integrity: The process Integrity TSC is probably the least utilized out of all the TSC's from a SOC 2 compliance perspective. Process INTEGRITY controls relate to the input of data, and so how the information is processed, and the way the info is then output. Assume payroll firms (data in, information processed, and information out), medical claims charge, etc.

Please contact us if you would like to know more about data security or need any help to perform a SOC/ GDPR certification for your organization. Visit our website https://accorppartners.com/soc/index.php to read more articles related to SOC reporting.