December 10, 2018

SOC 2 Examinations - What Are the Trust Services Criteria and Categories?

CYBERSECURITY, SOC
BY MARK RILEY

The 2017 Trust Services Criteria (TSC), which superseded the 2016 Trust Services Principles and Criteria (TSPC), serves as the control criteria for attestation engagements to assess and report on controls for information and systems like System and Organization Control (SOC) 2 and SOC for Cybersecurity examinations. On December 15, the principles were officially renamed to categories. Along with the name alteration, another critical change was the control criteria's integration with the 2013 COSO Framework, which stands for the Committee of Sponsoring Organizations of the Treadway Commission. Integrating this framework into SOC 2 reporting was done with the intent of expanding the assessment environment. The 2013 COSO, which has five components and 17 principles, is used to assess the design, implementation and maintenance of internal controls and evaluate their effectiveness.

Similar to the prior version of the TSPC, the new TSC still consists of 5 categories: security, availability, confidentiality, processing integrity and privacy. In addition, there is a set of criteria aligned to all five categories known as the Common Criteria.

Each category has a specific set of criteria to meet with corresponding points of focus. The American Institute of Certified Public Accountants (AICPA) defines them as the following:

- **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.

- **Availability** - Information and systems are available for operation and use to meet the entity's objectives.

- **Processing integrity** - System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.

- **Confidentiality** - Information designated as confidential is protected to meet the entity's objectives.

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

The Common Criteria are mandatory for a SOC 2 engagement and, since the Common Criteria is based off of the security category, every organization undergoing a SOC 2 engagement should include security at a minimum. For the additional categories, the criteria are made up of the Common Criteria plus the additional criteria specific to the said category.

The additional four categories should be considered based on the industry the organization operates in, the types of services the organization provides and contractual requirements from customers, as well as the information and assurance needs of key stakeholders. The 2017 TSC can also be used as the framework for a SOC for Cybersecurity examination. For more information on these reports, please refer to our recent article, *SOC for Cybersecurity Reports: Overview and Comparison to SOC 2 Reports*.

In addition to contractual requirements from customers, organizations can choose whether or not to include the additional four categories into the scope of their SOC 2 examination. If so, they may choose any combination of the four categories they deem appropriate, based on the factors described above.

At a high level, there are some industry-specific and data-specific factors that should be considered when deciding which categories to include. For instance, software-as-a-service (SaaS) and cloud computing organizations should consider the availability category. Organizations that process transactions on behalf of their customers may consider including financial controls within the processing integrity category. Organizations that maintain, store and/or process highly sensitive customer data that does not fall under the purview of privacy regulations – such as HIPAA or GDPR – should consider including the confidentiality category. Organizations that maintain, store and/or process personally identifiable information and/or protected health information should consider including the privacy category.

In short, management and key stakeholders of an organization considering undergoing a SOC 2 examination should understand and determine which categories are most relevant to the services they provide and the data they process and store. The organization can consult with auditors to determine which criteria would be most relevant for inclusion in the SOC 2 report. For additional information on SOC 2 examinations, visit Schneider Downs' *Frequently Asked Questions about SOC Reports.*

In addition, please contact us if you're interested in learning about our SOC 2 and SOC for Cybersecurity examinations and how we can help you meet your customers' and key stakeholders' requirements.

You've heard our thoughts… We'd like to hear yours

The Schneider Downs Our Thoughts On blog exists to create a dialogue on issues that are important to organizations and individuals. While we enjoy sharing our ideas and insights, we're especially interested in what you may have to say. If you have a question or a comment about this article – or any article from the Our Thoughts On blog – we hope you'll share it with us. After all, a dialogue is an exchange of ideas, and we'd like to hear from you. Email us at contactSD@schneiderdowns.com.