August 1, 2018

SOC 2 Reporting Standards Updated: Effective 12/15/2018

RISK ADVISORY/INTERNAL AUDIT, SOC
BY SCHNEIDER DOWNS PROFESSIONAL

The AICPA recently updated the SOC 2 reporting standards to align with the COSO 2013 Internal Control Framework. The specific updates pertain to the updated 2017 Trust Services Criteria (TSC) and the 2018 SOC 2 Description Criteria (DC). Service organizations must use the 2017 TSC and 2018 DC for SOC 2 reporting periods ending on or after December 16, 2018, regardless of the SOC 2 report issue date. The 2018 DC were intended to be used with the 2017 TSC; therefore, if a service organization uses the 2018 DC, then they must use the 2017 TSC. When using the 2015 DC, service organization may choose to use the 2016 TSC or 2017 TSC.

The following list summarizes the most significant changes that have taken place as a result of the update to the 2017 TSC:

- **Renames the Trust Services Principles and Criteria.** The COSO 2013 framework uses the term *principles* to refer to the elements of internal control. To avoid confusion, the *Trust Services Principles and Criteria* will be renamed as the *Trust Services Criteria* (the term *Principles* has been removed). In addition, the five principles (Security, Availability, Processing Integrity, Confidentiality and Privacy) will now be referred to as the *Trust Services Categories*.

- **Restructures and aligns the TSC with the COSO 2013 framework.** This is a significant change that will most likely require service organizations to restructure their controls. Service organizations will have to ensure that their controls meet the 17 principles in the COSO 2013 framework and the additional supplemental criteria noted below.

- **Restructures and adds supplemental criteria to better address cybersecurity risks in engagements using the TSC.** In addition to the 17 principles in the COSO 2013 framework, new supplemental criteria were developed and organized into the following categories:

  - Logical and physical access controls. The TSC relevant to how an entity restricts logical and physical access, provides and removes that acces, and prevents unauthorized access.

  - System operations. The TSC relevant to how an entity manages the operation of system(s) and detects and mitigates processing deviations, including logical and physical security deviations.

  - Change management. The TSC relevant to how an entity identifies the need for changes, makes the changes using a controlled change management process, and

prevents unauthorized changes from being made.

- Risk mitigation. The TSC relevant to how an entity identifies, selects and develops risk mitigation activities and how the entity assesses and manages risks associated with vendors and business partners.

- **Adds points of focus to all TSC**. The points of focus may assist management and the practitioner in evaluating whether the controls are suitably designed and operating effectively; however, use of the TSC does not require management or the practitioner to separately assess whether points of focus are addressed.

The following list summarizes the most significant changes that have taken place as a result of the update to the 2018 DC:

- **Principal Service Commitments.** The service commitments a service organization makes to user entities and others are based on the needs of those entities. In identifying the service commitments to be disclosed, service organization management may begin by reviewing the commitments it made to user entities. Service commitments may be communicated to user entities in many ways, such as through contracts, service-level agreements, and published policies (for example, a privacy policy). No specific form of communication is required.

- **Principal System Requirements.** System requirements may result from the service organization's commitments relating to one or more of the trust services categories (for example, a commitment to programmatically enforce segregation of duties between data entry and data approval creates system requirements regarding user access administration).

- **Identified Security Incidents.** For identified security incidents as of the date of the description (for a Type 1) or during the period of time covered by the description (for a Type 2), as applicable, the following information might need to be disclosed, depending on the type of security incident that occurred:
  - Nature of each incident;
  - Timing surrounding the incident; and
  - Extent (or effect) of the incident and its disposition.

For more information on SOC Reports and the impending changes, please visit our SOC FAQ page or feel free to contact a member of our SOC Reporting team. Stay tuned for our future post on the best strategies to prepare for the impending SOC 2 requirement changes.

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.

this information should be relied upon when coordinated with individual professional advice.