SOC 2 reporting

Changes ahead

In April of 2017, the Assurance Services Executive Committee (ASEC) of the American Institute of Certified Public Accountants (AICPA) released the 2017 Trust Services Criteria (2017 TSC), which are used in System and Organization Controls (SOC) 2 – SOC for Service Organizations: Trust Services Criteria engagements. The 2017 TSC supersedes the 2016 Trust Services Principles and Criteria (the extant criteria), which remain available for use for reports with periods ending on or before December 15, 2018. In addition, in March of 2018 the ASEC issued a new version of the Description Criteria, which are used by management when preparing the description of the service organization's system, replacing the 2015 Description Criteria. Both the new Trust Services Criteria and Description Criteria will require changes to SOC 2 reports.

Why the change?

In order to facilitate the use of the Trust Services Criteria in an entity-wide engagement, the ASEC chose to more closely align the 2017 TSC with the Committee of Sponsoring Organizations of the Treadway Commission's 2013 Internal Control—Integrated Framework (COSO). In addition, the 2017 TSC increases the flexibility of the criteria in its applicability; for example, the new TSC can be applied to SOC for Cybersecurity examinations. For additional information on a SOC for Cybersecurity examination, KPMG's white paper on the topic can be found here.

What's changed?

The alignment of the criteria used in a SOC 2 examination to the 17 COSO principles resulted in a major restructuring of the extant criteria. In addition to the 17 COSO principles, the 2017 TSC include additional criteria—Logical and Physical Access Controls, System Operations, Change Management, and Risk Mitigation—that supplement COSO principle 12: *The entity deploys control activities through policies that establish what is expected and procedures that put policies into action.* These are referred to as the "supplemental criteria."

The most notable difference between the 2016 Trust Services Principles and Criteria and the 2017 Trust Services Criteria relate to the addition of ***points of focus*** for each criterion, provided to assist in applying judgment when evaluating the TSC. Within the common criteria alone, there are over 200 points of focus. Since some points of focus may not be suitable or relevant to every entity or engagement being performed, use of the 2017 TSC does not require a control to meet each point of focus or an assessment of whether each point of focus was addressed. However, every ***relevant*** point of focus should be addressed.

Some elements that remain consistent between the 2016 Trust Services Principles and Criteria and 2017 Trust Services Criteria are the Categories (formerly "Principles") of the criteria – Security, Availability, Processing Integrity, Confidentiality, and Privacy. In addition, the use of a set of "Common Criteria" that apply to all categories being evaluated still exists. Changes to the additional criteria within Availability, Processing Integrity, Confidentiality, and Privacy are relatively minor compared to the changes in the Common Criteria.

Comparison of the Categories between the 2016 Trust Services Principles and Criteria and 2017 Trust Services Criteria

As depicted by the table below, at a high level when comparing the categories, the 2016 and 2017 Trust Services and Criteria do not appear that different. Under the 2017 TSC, additional categories for "Control Activities" and "Risk Mitigation" were introduced. However, these control areas existed under the 2016 Trust Services Principles and Criteria, so these are not new concepts. As stated earlier, the biggest changes relate to revising the underlying criteria within these categories, along with the introduction of the points of focus.

2016 Trust Services Principles and Criteria Structure – Category Level	2017 Trust Services Criteria Structure – Category Level
CC1.0 – Common Criteria Related to Organization and Management	Control Environment
CC2.0 – Common Criteria Related to Communications	Communication and Information
CC3.0 - Common Criteria Related to Risk Management and Design and Implementation of Controls	Risk Assessment
CC4.0 - Common Criteria Related to Monitoring of Controls	Monitoring Activities
Under the 2017 TSC, this additional category was introduced. However, criteria related to this category existed under the 2016 Trust Services Principles and Criteria within other categories, and therefore, these are not new concepts.	Control Activities
CC5.0 Common Criteria Related to Logical and Physical Access Controls	Logical and Physical Access Controls
CC6.0 - Common Criteria Related to System Operations	System Operations
CC7.0 - Common Criteria Related to Change Management	Change Management
Under the 2017 TSC, this additional category was introduced. However, criteria related to this category existed under the 2016 Trust Services Principles and Criteria within other categories, and therefore, these are not new concepts.	Risk Mitigation
Additional Criteria for Availability	Additional Criteria for Availability
Additional Criteria for Confidentiality	Additional Criteria for Confidentiality
Additional Criteria for Processing Integrity	Additional Criteria for Processing Integrity
Additional Criteria for Privacy	Additional Criteria for Privacy

Emphasis on a Service Organization's Service Commitments and System Requirements

The updated Description Criteria emphasize the requirement for management to establish and describe within the description of the service organization's system, included in the SOC 2 report, their service commitments and system requirements.

Service commitments are often found in contracts, service level agreements, and published statements; they are declarations made by a service organization to their customers about the system used to provide the service. Examples of service commitments include system availability (e.g., "uptime") commitments, encryption standards used to encrypt customer data hosted by the service organization, and technical baseline configurations related to passwords, patching standards, etc.

System requirements are the specifications about how the system should function to meet the service organization's commitments. These requirements are commonly documented in system policies and procedures, system design documentation, contracts with customers, and government regulations. Some examples of system requirements include the frequency and procedures for performing user access reviews, background check requirements for new personnel, and configurations of edit checks in system design documents.

In addition, the updated Description Criteria include a new requirement for management to identify and document in the SOC 2 report system incidents that (a) were the result of controls that were not suitably designed or operating effectively or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements.

Mapping to other frameworks

Soon after the release of the 2017 TSC, the AICPA also published practice aids that map the 2017 TSC to International Organization for Standardization (ISO) 27001 and National Institute for Standards and Technology Cybersecurity Framework (NIST CSF), for example, which can be useful for organizations considering the option of an enhanced SOC 2 report or SOC 2+ report. KPMG's discussion document that goes into further details on enhanced SOC 2 reports and SOC 2+ reports, including the benefits, can be located here.

When does it go into effect?

The 2017 TSC and updated Description Criteria went into effect upon release. However, the extant criteria are available for use for reports with periods ending as of or prior to December 15, 2018, after which they will be considered superseded. For most organizations, this means the 2016 Trust Services Principles and Criteria and 2015 Description Criteria will continue to be used for the large majority of SOC 2 reports issued in 2018. However, the 2017 TSC and updated Description Criteria should be considered now as new controls and disclosures required to meet the 2017 TSC will need to be in effect and/or considered prior to the beginning of the 2019 SOC 2 reporting period. See the example transition timeline on page 4.

Who is impacted?

The 2017 TSC and updated Description Criteria impact all companies that currently have or are considering a SOC 2 or SOC 3 engagement. In addition, the TSC may be used for companies that are considering a SOC for Cybersecurity engagement, as the TSC can also be used to evaluate an entity's cybersecurity risk management program.

What are the next steps?

Service organizations with existing SOC 2 reports should undergo an internal self-assessment, or engage their service auditor, to perform a gap analysis whereby their existing SOC 2 controls are evaluated against the 2017 TSC. Once completed, the service organization may determine that additional controls should be added to the scope of their report. Under the new TSC, we anticipate for most service organizations there will be an increase in the number of controls that are required to meet the 2017 TSC compared to the extant criteria. Thus, to avoid significant challenges in meeting the 2017 criteria, it is vitally important for organizations to start this exercise early in 2018 to allow for sufficient time to implement, monitor, and remediate (as necessary) their new controls. In addition, management should be aware of the new Description Criteria and begin making updates to the system description accordingly.

Those service organizations undergoing a SOC 2 examination for the first time should plan a timeline that enables them to meet SOC 2 commitments to internal stakeholders (e.g. executive management) and/or external stakeholders (e.g. clients). This timeline should begin with a phase to evaluate their existing control environment against the new 2017 TSC.

The timeline provided on page 4 can be applied to service organizations that already have an existing SOC 2 report and need to undergo the transition from the 2016 Trust Services Principles and Criteria to the 2017 Trust Services Criteria, as well as to those service organizations planning for their first SOC 2 engagement.

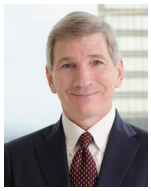
Suggested Example Transition Timeline for Existing SOC 2 Report or for a First Year SOC 2 Report

The project to transition to the new 2017 TSC is not unlike the first year effort to prepare for a SOC 2 examination (i.e., a "readiness assessment" or "diagnostic review"). Below is an example transition timeline for a SOC 2 report that covers the annual period of October 1 to September 30. The actual time it takes to be ready for an examination will depend on many factors, including the complexity of the current environment, and management's ability to identify and remediate gaps. This timeline is also applicable to those service organizations undergoing a SOC 2 examination for the first time and represents the steps we recommend take place before the actual SOC 2 examination period begins.

2017 TSC Transition Timeline	Q1 2018			Q2 2018			Q3 2018			Q4 2018		
Phase 1: Assessment of existing controls to 2017 TSC												
Phase 2: Gap Analysis												
Phase 3: Control Implementation												
Phase 4: Readiness Assessment (New Controls)												
Phase 5: Remediation Phase												
Phase 6: Ready for SOC 2 Examination Period to Begin												

Contact us

For more information on KPMG's Risk Assurance Services related to SOC 2 and the 2017 Trust Services Criteria, please contact:



Chris Mottram
Partner
T: 404-979-2100
E: cmottram@kpmg.com

Edwin Holt
Partner
T: 214-840-2116
E: eeholt@kpmg.com

Nina Currigan
Managing Director
T: 303-382-7808
E: ncurrigan@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia