KFI WHITE PAPER:
SOC 2 Reporting Changes

During 2018, SOC 2 reports will be changing in two very significant ways:

1. In April of 2017, the AICPA's Assurance Services Executive Committee (ASEC) released the 2017 Trust Services Criteria (2017 TSC) that supersedes the 2016 Trust Services Principles and Criteria (2016 TSP). The 2017 TSC are found in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy.*

2. In March of 2018, the ASEC issued a new version of the Description Criteria (2018 DC), which are used by management when preparing the description of the service organization's system, replacing the 2015 Description Criteria. The 2018 DC are found in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report.*

The purpose of this whitepaper is to evaluate these changes and the impact that they will have on service organizations who receive SOC 2 reports and the service auditors who conduct the engagements. The 2017 TSC and 2018 DC will be required for Type 1 SOC 2 reports with as-of dates after December 15, 2018 and Type 2 reports with periods ending after December 15, 2018.

Updated Trust Services Criteria

The 2017 TSC are intended to be more flexible than the previous version — the 2016 TSP — and are specifically designed to address cybersecurity risks. The updates to the 2017 TSC represent the most significant change to the criteria since the inception of the SOC 2 report.

Overview of the 2017 TSC

Use of the COSO 2013 Framework

The 2017 TSC were restructured and aligned with the 17 principles from the Committee of Sponsoring Organizations of the Treadway Commission's 2013 Internal Control-Integrated Framework (COSO 2013), which was developed to help companies of all sizes to design effective systems of controls.

By Jamie Kilcoyne, CPA, CISA, CITP, CIA, CFE - K Financial

kfi AUDIT & ADVISORY

COSO 2013 is widely used by public companies in their SOX 404 compliance programs. The 17 COSO 2013 principles are summarized as follows:

Control environment	Risk assessment	Control activities	Information and communication	Monitoring activities
1. Demonstrates commitment to integrity and ethical values	6. Specifies suitable objectives	10. Selects and develops control activities	13. Uses relevant quality information	16. Conducts ongoing and/or separate evaluations
2. Exercises oversight responsibilities	7. Identifies and analyzes risk	11. Selects and develops general controls over technology	14. Communicates internally	17. Evaluates and communicates deficiencies
3. Establishes structure, authority, and responsibility	8. Assesses fraud risk	12. Deploys through policies and procedures	15. Communicates external	
4. Demonstrates commitment to competence	9. Identifies and analyzes significant change			
5. Enforces accountability				

The COSO 2013 framework uses the term "principles" to refer to the elements of internal control that must be present or functioning for the entity's internal control to be considered effective. To avoid confusion between the terminology used in the COSO 2013 framework and that used in the Trust Services Principles and Criteria, the latter were renamed the *Trust Services Criteria.* In addition, the 5 principles (security, availability, processing integrity, confidentiality and privacy) are now referred to as *Trust Services Categories.*

The 17 COSO principles are included within the SOC 2 common criteria and are organized as follows:

- Control environment (CC1 series)
- Communication and information (CC2 series)
- Risk assessment (CC3 series)
- Monitoring activities (CC4 series)
- Control activities (CC5 series)

To supplement the 17 COSO principles and better address cybersecurity risks, the 2017 TSC also include the following:

- Logical and physical access controls (CC6 series)
- System operations (CC7 series)
- Change management (CC8 series)
- Risk mitigation (CC9 series)

kfi AUDIT & ADVISORY

Differences between the Old and New TSC

When the new TSC are placed side by side with the old common criteria, there are many consistencies:

2017 TSC	2016 TSP
CC1 Control environment	*CC1.0 Organization and management*
CC2 Communication and information	*CC2.0 Communications*
CC3 Risk assessment	*CC3.0 Risk management and design and implementation of controls*
CC4 Monitoring activities	*CC4.0 Monitoring of controls*
CC5 Control activities	----------
CC6 Logical and physical access controls	*CC5.0 Logical and physical access controls*
CC7 System operations	*CC6.0 System operations*
CC8 Change management	*CC7.0 Change management*
CC9 Risk mitigation	----------

Although CC5 *Control Activities* and CC9 *Risk Mitigation* are broken out separately in the 2017 TSC, the concepts associated with these criteria were generally included in the 2016 TSP within other categories. Despite the consistencies noted above and many identical criteria found in the 2017 TSC and 2016 TSP, there are also changes to be aware of and several new criteria that will need to be addressed. Some of the more significant changes in the 2017 TSC that may require companies to implement additional controls are:

CC1.2 / COSO Principle 2: *The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.* In order to address this criteria, companies should have an independent board of directors and the duties and oversight responsibilities of the board should be set forth in a charter document. Many smaller organizations that do not currently have a board of directors or whose board members are not independent are going to find this criteria to be very challenging to address.

CC3.3 / COSO Principle 8: *The entity considers the potential for fraud in assessing risks to the achievement of objectives.* In order to address this criteria, companies should specifically address fraud in their risk assessments and risk management programs. There was not as much emphasis on performing a fraud risk assessment under the 2016 TSP. Many organizations will need to update their risk assessment process to address this criteria.

CC9.1: *The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.* In order to address this criteria, companies should have policies and procedures to respond to and recover from security events that disrupt business operations. This is similar to controls that were required historically when the availability principle was in scope under the 2016 TSP. But now disaster recovery and business continuity controls will be required for all SOC 2 engagements regardless of whether availability is in scope.

CC9.2: *The entity assesses and manages risks associated with vendors and business partners.* In order to address this criteria, companies should specifically address vendor and business partner risks in their risk assessments and risk management programs and / or perform separate vendor and business partner risk assessments.

Another notable difference between the 2017 TSC and the 2016 TSP is that the updated criteria include points of focus that represent important characteristics of the criteria to help users apply them and design effective controls. Applying the trust services criteria and determining whether individual points of focus are relevant requires judgment. Within the common criteria alone, there are over 200 points of focus. Use of the criteria does not require users to specifically address each of the points of focus. However, if a point of focus is relevant and important to meeting an organization's service commitments or system requirements, then a control should be in place to address the point of focus.

Revised Description Criteria Requirements

The Description Criteria (DC) were established for use by service organization management when preparing the description of the service organization's system. The DC are also used by service auditors when evaluating the fair presentation of the system description and underlying controls in a SOC 2 examination. The AICPA has published useful implementation guidance for the 2018 DC, which was not available with the 2015 description criteria under DC Section 200A. In general, the 2018 and 2015 DC are not that different and the required elements of the system description are quite similar. The required elements are just re-organized in the 2018 DC and unique identification numbers have been assigned to each criteria (DC 1 through DC 9). The most significant changes in the 2018 DC are:

DC 2: *The principal service commitments and system requirements.* Service organization management must now explicitly disclose the principal service commitments and system requirements in the description. Service commitments are the declarations made by the service organization to their customers about the system used to provide the service. Commitments can be communicated in contracts, service-level agreements or published statements. Some examples of service commitments include system availability, encryption standards used to encrypt customer data hosted by the service organizations, 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. Requirements are often specified in the service organization's system policies and procedures and system design documentation. Some examples of system requirements include the frequency and procedures for performing user access reviews, background check requirements for new personnel and system configurations.

DC 4: *For identified 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, 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:*

a) Nature of each incident
b) Timing surrounding the incident
c) Extent (or effect) of the incident and its disposition

These disclosures are intended to enable report users to understand the nature of the risks faced by the service organization and the impact of the realization of those risks. Service organizations and service auditors should expect to have detailed discussions during the planning and execution of SOC 2 examinations about incidents that may require disclosure in the SOC 2 report.

Conclusion

SOC 2 reports are going to look much different once the 2017 TSC and 2018 DC are adopted. However, most of the information that has historically appeared in SOC 2 reports will continue to be there — just in a different format. Management of service organizations should expect to spend extra time in 2018 and 2019 updating their system descriptions in the period that the new DC criteria are adopted. And service auditors should expect to spend extra time evaluating the fair presentation of system descriptions during this period. Similarly, management of service organizations should expect to have several additional controls in scope for SOC 2 engagements to address the incremental changes between the 2016 TSP and 2017 TSC.