System and Organization Controls (SOC):

Latest SOC 2® guidance updates and impacts for issuers and recipients.

April 10, 2018

BAKER TILLY

Agenda

01 Key updates for SOC 2® Trust Services Criteria

02 2018 Description Criteria

03 Distinctions between SOC2® and SOC for Cybersecurity

04 Open discussion and questions

Learning objectives

1 **SOC 2 Trust Services Criteria:** List key implementation updates in the SOC 2® guide, and how they impact the reports.

2 **2018 Description Criteria:** Recognize how the new Description Criteria differs for reports issued with periods ending after Dec. 15, 2018 and what service organizations and users need to do now to prepare.

3 **SOC 2® and SOC for Cybersecurity:** Identify distinctions between SOC 2® examinations and SOC for Cybersecurity examinations.

Key updates for SOC 2® Trust Services Criteria

Updates for SOC 2® Trust Services Criteria

AICPA released new guidance on SOC 2® Trust Services Criteria and Description Criteria

The guide is effective as of

Jan. 1, 2018

BAKER TILLY

Updates for SOC 2® Trust Services Criteria

- **The guide includes** updates from SSAE 18 that are effective now; however, much of the guidance is related to implementing the 2018 Description Criteria and the 2017 Trust Services Criteria (which are effective for reports with examination periods ending after Dec. 15, 2018).

BAKER TILLY

Updates for SOC 2® Trust Services Criteria

Criteria Structure

There are updates to criteria within each principle:

COSO Internal Control - Integrated Framework 2013 *principles as basis for updated TSC*

Supplemental criteria *related to risk management and general information technology control areas*

Points of focus *for each criterion*

Updates for SOC 2® Trust Services Criteria

New terminology: Trust Services Categories (formerly principles)

- To avoid confusion with COSO terminology, the Trust Services Principles were renamed as the Trust Services Criteria categories, which are:
  - Security (Common), Availability, Processing Integrity, Confidentiality and Privacy

Restructure the criteria and add to better address cybersecurity

- Address incident management and other areas at a more detailed level

BAKER TILLY

Updates for SOC 2® Trust Services Criteria

The COSO framework contains ***points of focus*** that represent important characteristics of the criteria to help users apply the criteria. Similar to the points of focus included in the COSO framework, the points of focus related to the supplemental criteria also represent important characteristics of those criteria. 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 criteria does not require management or the practitioner to separately assess whether points of focus are addressed.

Excerpted from page X (10) of the SOC 2 guide

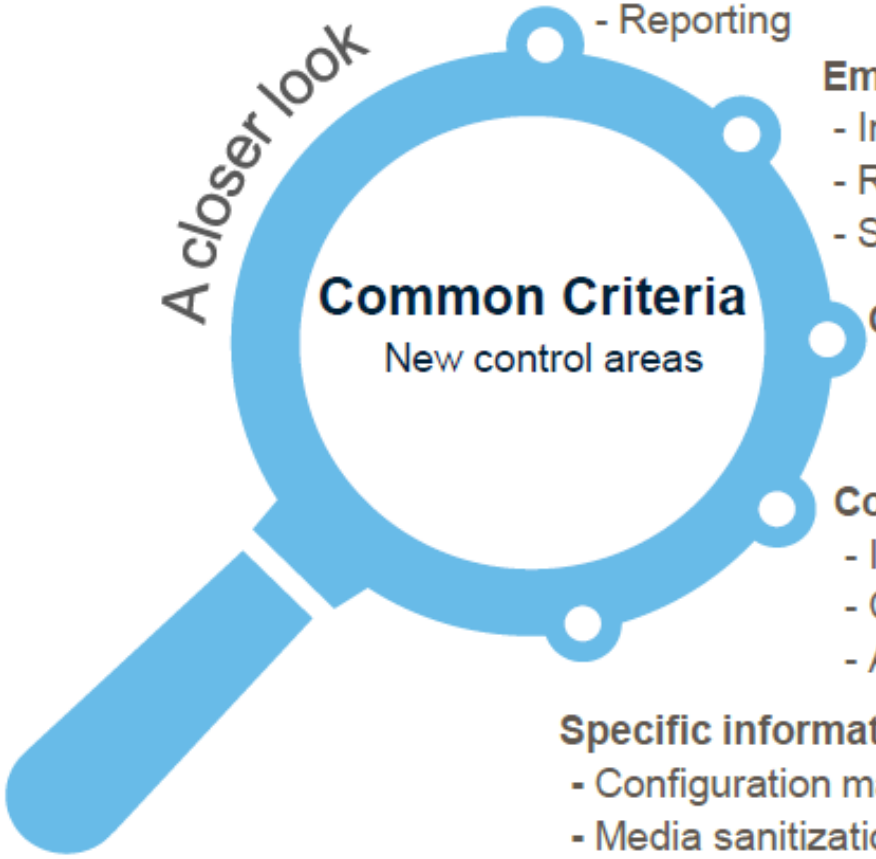
Updates for SOC 2® Trust Services Criteria

Common Criteria

- The Common Criteria has new criteria and other changes, and requires additional control considerations
- The other trust services categories/criteria were re-mapped slightly, however, the necessary controls to meet the criteria should remain unchanged
- Because the Common Criteria are required to be included as part of any SOC 2® examination, all organizations should incorporate additional planning time to review the changes.

BAKER TILLY

Updates for SOC 2® Trust Services Criteria



Board governance
- Independence
- Expertise
- Reporting

Employee performance management
- Incentives and pressures
- Retention
- Succession planning

Consideration of certain business risks
- Strategic risks
- Fraud risk
- IT assets
- Third parties

Control activities
- Identifying controls to address risks
- Continuous monitoring and/or separate evaluations
- Addressing non-compliance

Specific information technology activities
- Configuration management
- Media sanitization and disposal
- Increased incident response requirements

BAKER TILLY

Examples of New Trust Services Criteria

New 2017 Trust Services Criteria	Example Points of Focus (Supplemental B)	Example Control
CC 1.2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Operates Independently—The Board has sufficient members who are independent and objective in evaluations and decision making. Establishes Oversight Responsibilities—The Board identifies and accepts oversight responsibilities for established requirements and expectations.	A Board of Directors has been established whose membership is independent from management. The Board receives periodic updates from management that include risk management and internal control trends, organizational performance and key projects or action items.

Examples of New Trust Services Criteria

New 2017 Trust Services Criteria	Example Points of Focus (Supplemental B)	Example Control
CC 1.4: The entity demonstrates a commitment to attract, develop and retain competent individuals in alignment with objectives.	Provides Training to Maintain Technical Competencies—The entity provides training programs, including continuing education and training, to ensure skill sets and technical competency of existing personnel, contractors and vendor employees are developed and maintained.	A formal training plan is developed by employee or role to maintain technical competence.

Examples of New Trust Services Criteria

New 2017 Trust Services Criteria	Example Points of Focus (Supplemental B)	Example Control
CC 3.1: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Considers Tolerances for Risk—Management considers the acceptable levels of variation relative to achievement of objectives. Includes Operations and Financial Performance Goals—The organization reflects desired level of performance for the entity within objectives.	Business objectives are determined as part of annual strategic planning activities. Financial performance goals, risk tolerance levels and applicable laws and regulations are considered as part of objective-setting.

Examples of New Trust Services Criteria

New 2017 Trust Services Criteria	Example Points of Focus (Supplemental B)	Example Control
CC 3.3: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Considers Various Types of Fraud—Assessment considers fraudulent reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur.	Fraud risks are explicitly considered as part of the risk assessment.

Examples of New Trust Services Criteria

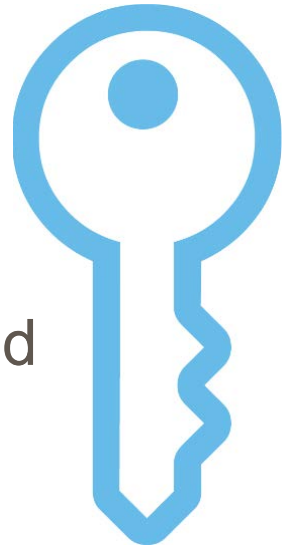
New 2017 Trust Services Criteria	Example Points of Focus (Supplemental B)	Example Control
CC 5.1: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Integrates With Risk Assessment—Controls help ensure risk mitigation is accomplished. Determines Relevant Business Processes—Management determines which business processes require control activities.	As part of the risk assessment process, existing control activities are identified that mitigate identified risks. Where risks are not already mitigated to an acceptable level and additional mitigation is required, action plans are developed to implement additional control activities.

2018 Description Criteria

2018 Description Criteria

- The description criteria are a set of benchmarks used when preparing and evaluating the SOC 2® system description.
- Applying the description criteria requires judgment. The new guide includes implementation guidance. See Supplement A.
- The description criteria must be relevant, objective, measurable and complete.

Key updates with new description criteria



- DC1: The types of services provided
- DC2: Disclosure of principal service commitments and system requirements
- DC3: The components of the system used to provide the services, including the following:
  - Infrastructure
  - Software
  - People
  - Procedures
  - Data

DC2: Service commitments and system requirements

Service organization management must provide reasonable assurance that its service commitments and system requirements were achieved

Must identify risks that threaten the achievement of commitments and requirements

'Principal' service commitments and system requirements must be stated in the system description

Service commitments and system requirements

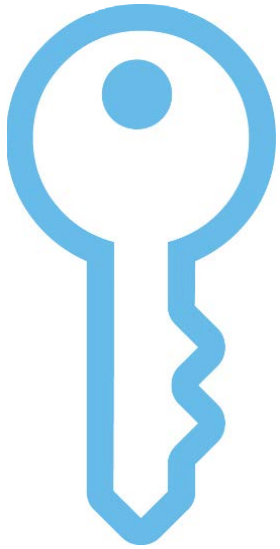
Example commitments

- The hours a system will be available
- Published password standards

Example requirements

- Background checks established in government banking regulations
- System edits that restrict the values accepted for system input

Key updates with new description criteria



- DC4: Required disclosures about system incidents
  - Includes the nature of the incident
  - Timing of incident
  - Extent of incident and disposition

- Judgement is needed when assessing whether to disclose an incident.

Key updates with new description criteria

- DC5: The applicable trust services criteria and the related controls designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved.

- DC6: Complementary User Entity Controls (CUECs)
  - Controls that are assumed are implemented by user entities and that are necessary

Key updates with new description criteria

- DC7: Subservice Organizations / Inclusive vs. Carve-out
  - Complementary Subservice Organization Controls (CSOCs)
- DC8: Trust Services Criteria that are not relevant to the system
  - Include within description explanation of why not applicable
- DC9: For Type 2 reports – If significant changes occur during the period to the system or controls, include relevant details of those changes

Vendor management and subservice monitoring

- There is an increased focus on vendor management and monitoring and including those controls in the SOC report.
- Service organizations should revisit and augment their vendor management procedures as needed to be able to formally demonstrate these controls.

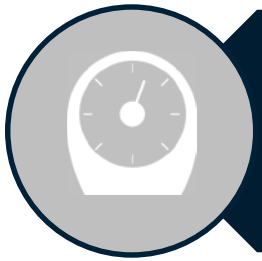
Vendor management and subservice monitoring

- When using the carve-out method, the description would identify the types of complementary subservice organization controls (CSOCs) that the subservice organization is assumed to have implemented.

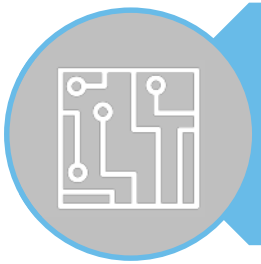
Vendor management and subservice monitoring

When a separate SOC 2® report exists for a subservice organization, obtaining and reading the SOC 2® report and paying particular attention to the complementary user entity controls (CUECs) identified by the subservice organization in the report helps the service auditor evaluate whether controls at the service organization are suitably designed.

Planning ahead - transitioning to the new TSC and DC



What is the examination timing for our next SOC 2 report?



When do we need to implement controls related to the new TSC?

What other planning activities must be completed?

2018 Description Criteria

Organizations will need to review and enhance their existing System Descriptions to describe the additional control processes.

2018 Description Criteria

Prior to undergoing the examination, organizations should complete the following readiness activities:

Review the new TSC and DC and familiarize yourself with its requirements

Map your organization's current control activities to the new TSC

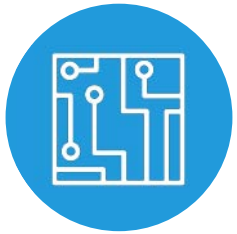
Identify criteria without sufficient control coverage

Design and implement controls to address criteria

BAKER TILLY

Distinctions between SOC 2® and SOC for Cybersecurity

Key elements of SOC for Cybersecurity



Reports on the controls within an entity's cybersecurity risk management program.

Whether management's description of it's cybersecurity risk management program meets the description criteria for Management's Description of an Entity's Cybersecurity Risk Management Program

Whether controls are effective to satisfy the criteria for security, availability and confidentiality within 2017 Trust Services Criteria

SOC for Cybersecurity

Nine categories are included in the description criteria for Management's Description of an Entity's Cybersecurity Risk Management Program

1. Nature of the business and operations
2. Nature of information at risk
3. Cybersecurity risk management program objectives
4. Factors that have a significant effect on inherent risks related to the use of technology
5. Cybersecurity risk governance structure
6. Cybersecurity risk assessment process
7. Cybersecurity communications and quality of cybersecurity information
8. Monitoring of the cybersecurity risk management program
9. Cybersecurity control processes

Other major differences between SOC 2® and SOC for Cybersecurity

	SOC 2®	SOC for Cybersecurity
Scoping	Focused on the customer facing/supporting system	Typically focuses on the whole organization
Reporting formats	Test procedures included	Test procedures not included
Intended users	Restricted use – Management, auditors, regulators or business partners of current or prospective customers	General use – Organization's stakeholders (e.g., management, directors, investors, analysts, business partners)

Disclosure

The information provided here is of a general nature and is not intended to address the specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought.

Baker Tilly refers to Baker Tilly Virchow Krause, LLP, an independently owned and managed member of Baker Tilly International.