Changes to AICPA Trust Services Principles and Criteria

November 13, 2014

EKS&H

AUDIT | TAX | CONSULTING

Introducing Your Presenters

Angela Appleby, CPA, CITP, CISA, CISSP, CIA, PCI-QSA

Partner

EKS&H

E-mail: aappleby@eksh.com

303-740-9400

Amanda Heintze, CIA, CISA, CRISC, PCI-QSA

Senior Manager

EKS&H

E-mail: aheintze@eksh.com

303-740-9400

Session Outline

.

- Part 1: Introduction and Overview of SOC Reporting
- Part 2: SOC 2 Changes
- Part 3: SOC Additional Updates
- Q&A

Introduction and Overview of SOC Reporting

Comparing SOC Reports

	Who needs these reports?	Why?	What?
SOC 1	Management of the service organization, user entities, and auditors of the user entities' financial statements	Audit of financial statements	Controls relevant to user entities' internal controls over financial reporting
SOC 2	Management of the service organization and other specified parties that have sufficient knowledge and understanding	Oversight and Due diligence	Controls relevant to security, availability, processing integrity, confidentiality, or privacy
SOC 3	Any users with need for confidence in the service organization's controls	Marketing "confidence without the detail"	Seal and easy to read report on controls

Types of Service Auditor Reports

There are two types of reports for SOC 1 and 2 engagements:

Type 1

A report on management’s description of the service organization’s system and the suitability of the design of the controls to achieve the related control objectives included in the description as of a specified date.

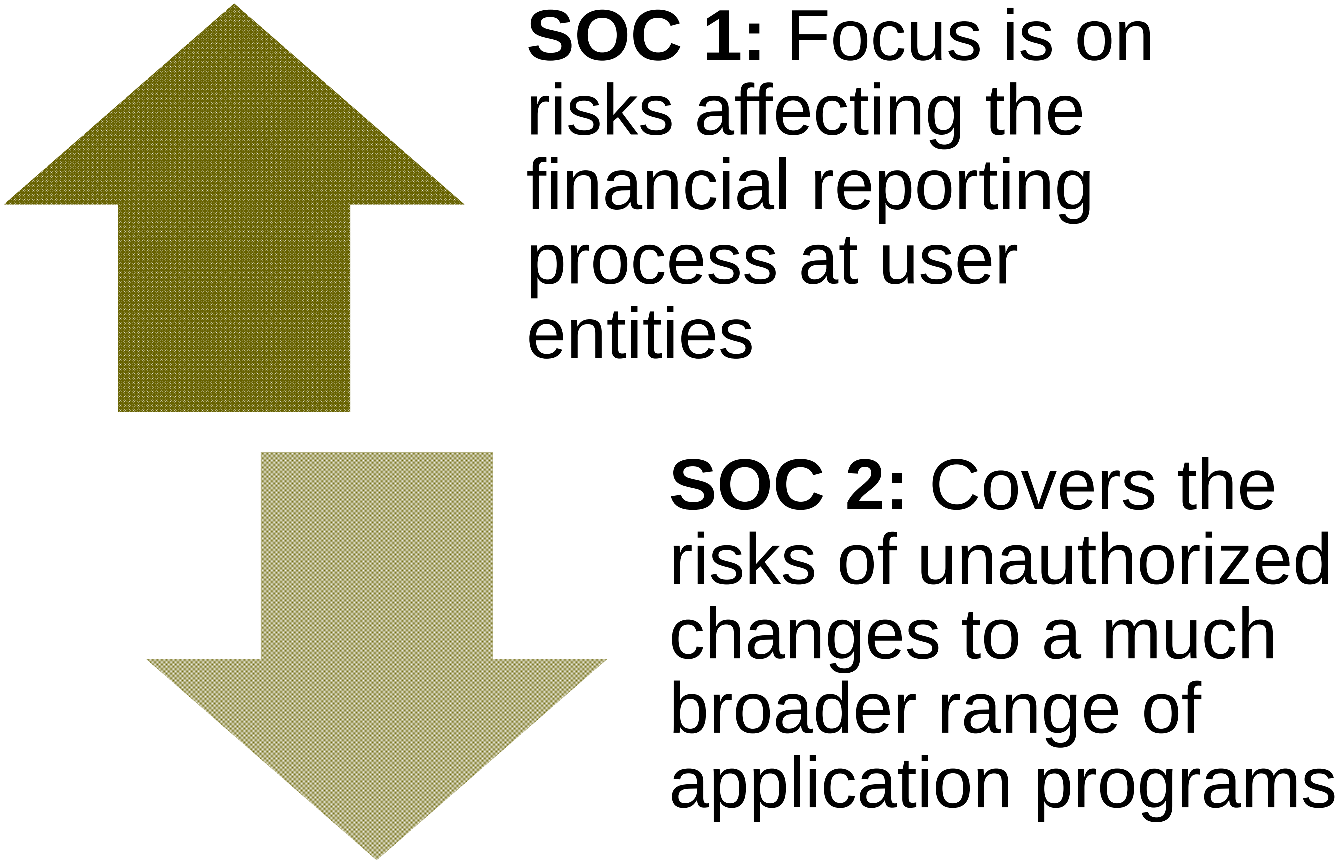
Type 2

A report on management’s description of the service organization’s system and the suitability of the design and **operating effectiveness of the controls** to achieve the related control objectives included in the description throughout a specified period.

Risks Addressed by Controls

The risks and controls that address those risks are likely to differ in SOC 1 and SOC 2 engagements

Example: Controls over Changes to Application Programs



SOC 1: Focus is on risks affecting the financial reporting process at user entities

SOC 2: Covers the risks of unauthorized changes to a much broader range of application programs

SOC 2 Reports over Security, Availability, Processing Integrity, Confidentiality, or Privacy

SOC 2 Reports – Outsourcing

With the advent of cloud computing, outsourcing will continue to grow with this available technology. Currently the growth in cloud computing technologies is outpacing traditional software technologies **4 to 1**.

SOC 2 Reports – Purpose

- Reports on Controls at a Service Organization Relevant to **Security, Availability, Processing Integrity, Confidentiality, or Privacy**

- SOC 2 engagements use the predefined criteria in **Trust Services Principles, Criteria and Illustrations**, as well as the requirements and guidance in AT section 101*, Attest Engagements* (AICPA, *Professional Standards*). In addition, see the AICPA guide, Reporting on Controls at a Service Organization, Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2).

SOC 2 Reports – System Attributes

SOC 2 reports specifically address one or more of the following five key system attributes (the principles):

Security

Availability

Processing Integrity

Confidentiality

Privacy

Overview of Trust Services Principles and Criteria

Domain	Principle
Security	▪ The system is protected against unauthorized access (both physical and logical).
Availability	▪ The system is available for operation and use as committed or agreed.
Confidentiality	▪ Information designated as confidential is protected as committed or agreed.
Processing Integrity	▪ System processing is complete, accurate, timely, and authorized.
Privacy	▪ Personal information is collected, used, retained, disclosed, and disposed of in conformity with the commitments in the entity's privacy notice and with criteria set forth in generally accepted privacy principles (GAPP) issued by the AICPA and the CICA.

SOC 2 Engagement: Definition of a System

- A system consists of five key components organized to achieve a specified objective, which are categorized as follows:

  - **Infrastructure -** The physical and hardware components of a system (facilities, equipment, and networks)
  - **Software -** The programs and operating software of a system (systems, applications, and utilities)
  - **People -** The personnel involved in the operation and use of a system (developers, operators, users, and managers)
  - **Procedures -** The automated and manual procedures involved in the operation of a system
  - **Data -** The information used and supported by a system (transaction streams, files, databases, and tables)

Boundaries of the System

- In a SOC 2 engagement, boundaries of the system must be clearly understood, defined, and communicated.

- **Example:** The boundaries of a system related to processing integrity (system processing is complete, accurate, timely, and authorized) may extend to other operations (e.g., processes at customer call centers).

(Continued on next slide)

Boundaries of the System

When the privacy principle is addressed in a SOC 2 engagement, the system boundaries cover, at minimum, all system components as they relate to the personal information life cycle, which consists of:

Personal Information Life Cycle
Collection
Use
Retention
Disclosure
Disposal or Anonymization of Personal Information

Review of the Relationship between Principles, Criteria and Controls (SOC 2)

Principles: Security, Availability, Processing Integrity, Confidentiality, and Privacy

Criteria is organized into seven categories: Organization and Management, Communications, Risk Management and Design and Implementation of Controls, Monitoring of Controls, Logical and Physical Access Controls, System Operations, and Change Management.

Illustrative Controls for each Criteria

System Components: Infrastructure, Software, People, Procedures, and Data

SOC 2 Report Contents

A SOC 2 Type 2 report contains the service auditor’s opinion about whether:

- **Management’s description** of the service organization’s system is **fairly presented**
- The **controls in the description** are **suitably designed** to meet the trust service criteria
- The **controls were operating effectively** to meet applicable trust service criteria
- For SOC 2 reports that address the privacy principle, **management complied with commitments**

Modified Opinions

- **Qualified Opinion Examples**
  - Fair presentation
    - Management’s description of the service organization’s system is not fairly presented, in all material respects.
  - Design
    - The controls are not suitably designed to provide reasonable assurance that the applicable Trust Services Principles and Criteria would be met if the controls operated as described.
  - Operating effectiveness
    - In the case of a Type 2 report, the controls did not operate effectively throughout the specified period to meet the applicable Trust Services Principles and Criteria stated in management’s description of the service organization’s system.
    - In the case of a Type 2 report that addresses the privacy principle, the service organization did not comply with the commitments in its statement of privacy practices.
  - Service auditor unable to obtain sufficient, appropriate evidence
    - A scope limitation exists, resulting in the service auditor’s inability to obtain sufficient, appropriate evidence.

(Continued on next slide)

Modified Opinions

- **Adverse**
  - Conclusion on the entire description
    - Fair presentation
    - Design
    - Operating effectiveness
- **Disclaimer**
  - Refusal to provide a written assertion
  - Refusal by management to provide a representation reaffirming its assertion
  - Information provided by the service organization

Management's Assertion

- Assertion should be provided prior to the service auditor forming the opinion.
- Assertion should disclose any deviations in the subject matter identified in the opinion.
- If deviations are identified that were not known, consider whether additional procedures by management are warranted in order to provide the assertion.

Representation Letter/Subsequent Events

- **Representation letter**
  - Required from parties at the service organization and subservice organization (when using inclusive method) who have appropriate knowledge of and responsibilities for the subject matter
  - Service auditor may request representation from those who are both directly and indirectly knowledgeable about and responsible for the subject matter
  - Includes a reaffirmation of the assertion
  - Dated the same date as the service auditor report
- **Subsequent events**
  - Events discovered after the end of the examination period but before the opinion date
  - Impact the examination period (e.g., fraud that was happening during the examination period) and may affect the opinion
  - A matter sufficiently important for disclosure by management (e.g., acquisition of the entity)

Key Implementation Activities for Service Organizations

- Review customer contracts
- Develop communications plan for customers
- Determine approach for subservice organizations
- Determine who within the organization will decide on trust principles, scope, and system boundaries
- Implement a process to support a reasonable basis for the assertion
- Consider other types of reports to satisfy changes to user needs (e.g., SOC 1 or SOC 3 reports)
- Controls for both SOC 1 and SOC 2 cannot be combined in one description

Reporting and Completing the Engagement – Intended Users of the Report

SOC 2 reports have the potential to be misunderstood when taken out of the context in which they are intended to be used. The service auditor’s report should state the report is intended solely for the information and use of management of the service organization and other **specified parties** with **sufficient knowledge and understanding** of the following:

Specified Parties Should Understand These Concepts:

- The nature of service provided by service organization
- How the service organization’s system interacts with user entities, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls
- Applicable Trust Services Principles and Criteria
- Risks that may threaten achievement of the applicable TSP and how controls address those risks

(Continued on next slide)

Reporting and Completing the Engagement – Intended Users of the Report

Report users who are most likely to have such knowledge include:

Examples of Report Users:
■ Management of the service organization
■ Management of the user entities
■ Practitioners evaluating or reporting on controls at user entities
■ Regulators
■ Others performing services related to controls at the service organization

Considerations for Report Users

- Understand and consider coverage period of the examination in relation to the audit of the user entity’s financial statements (Type 2 reports)
- Evaluate boundaries, principles, criteria, and controls addressed by the report and whether they meet your needs
- Identify and determine whether relevant user entity controls included in the SOC 2 report have been implemented by the user entity
- Evaluate the tests performed by the service auditor and the effect of the test results

SOC 2
Changes

SOC Changes Effective December 15, 2014

The AICPA recently issued an update to the Trust Services Principles and Criteria for Security, Availability, Processing Integrity, and Confidentiality. The **revised criteria are effective for reporting periods ending on or after December 15, 2014.** SOC 2 reports are based on the AICPA's *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (TSP section 100A)*.

Privacy principles are currently under revision and will be updated in the future.

SOC Reporting Changes

In an effort to eliminate the redundancy and cross-referencing involved with the original Trust Services Principles and Criteria, the new criteria have been restructured to group all common criteria. The criteria used to be grouped together by the four different areas for each trust principle:

1. Policies
2. Communications
3. Procedures
4. Monitoring

Trust Services Principles and Criteria

The new Trust Services Principles and Criteria group common criteria that apply to all principles into the following seven categories:

1. Organization and management
2. Communications
3. Risk management and design and implementation of controls
4. Monitoring of controls
5. Logical and physical access controls
6. System operations
7. Change management

In addition to these seven categories, service organizations must consider the additional criteria that are specific to availability, confidentiality, and processing integrity. Be aware that streamlining the common criteria does not mean that there are fewer controls that need to be in place as those seven categories apply to all principles being reported on.

Significant Areas of Change and Focus

Some of the most significant areas of change and focus that service organizations should address:

- Greater focus on risk assessment
- Code of conduct and background screening procedures are now required, whereas in the past it was an illustrative control for a specific criteria.
- Criteria surrounding disaster recovery and incident response-related controls are more specific.
- More focus on defined organization structure and reporting lines
- More focus on performing root cause analysis over incidents that occur and their respective remediation efforts
- Clearer communication of certain security criteria to internal and external users is now required.
- Streamlined criteria that provides enhanced presentation for SOC 2 reporting
- Documentation prepared to explain to internal and external users the limitations of the system as well as each user’s responsibilities

What Do You Need to Do Differently?

A service organization that currently or has previously provided a SOC 2 or SOC 3 report to stakeholders should understand the impact of these changes on SOC reporting processes. If your client has not completed a SOC audit but provides outsourced services to customers, this is particularly important, especially for those being audited by their customers surrounding those processes and who are completing checklists to provide information on their internal control environment to their customers. This is also important if compliance initiatives, such as HIPAA, GLBA, ISO 27001, and NIST 800-53, need to be achieved.

Service Organization’s Steps to Take

- Begin assessing current controls to ensure alignment with the newly issued criteria.
- Discuss any needed changes with your client’s SOC service auditor.

SOC
Additional Updates

SOC Additional Updates

- SOC 3 Seal Program cessation
- Updates to SOC 2 guide (dependent on updates to AT 101)
  - More alignment with latest SOC 1 guide
  - Vendor versus subservice organization
- Updates to privacy principle
- SOC 3 guide in process
- Peer review requirements
- Reporting on additional subject matter
  - Cloud security alliance
  - The Health Information Trust Alliance (HITRUST)

Extending/Customizing SOC 2 Reporting

User entities may request that a service organization add additional criteria not included in the Trust Services Principles and Criteria for the principle being reported on (e.g., criteria related to regulatory requirements, or service level agreements).

Reporting on Additional Subject Matter

1.39 A service organization may request that the service auditor's report address additional subject matter that is not specifically covered by the criteria in this guide. An example of such subject matter is the service organization's compliance with certain criteria based on regulatory requirements (e.g., security requirements under the Health Insurance Portability and Accountability Act of 1996) or compliance with performance criteria established in a service-level agreement. In order for a service auditor to report on such additional subject matter, the service organization provides the following:

- An appropriate supplemental description of the subject matter
- A description of the criteria used to measure and present the subject matter
- If the criteria are related to controls, a description of the controls intended to meet the control-related criteria
- An assertion by management regarding the additional subject matter

1.40 The service auditor should perform appropriate procedures related to the additional subject matter in accordance with AT section 101 or AT section 601, *Compliance Attestation* (AICPA, *Professional Standards*) and the relevant guidance in this guide. The service auditor's description of the scope of the work and related opinion on the subject matter should be presented in separate paragraphs of the service auditor's report. In addition, based on the agreement with the service organization, the service auditor may include additional tests performed and detailed results of those tests in a separate attachment to the report.

Cloud Security Alliance

February 25, 2013 – The Cloud Security Alliance (CSA) has drafted the CSA Position Paper on AICPA Service Organization Control Reports as a means to educate its members and provide guidance on selecting the most appropriate reporting standard.

After careful consideration of alternatives, the CSA has determined that for most cloud providers, a SOC 2 Type 2 attestation examination conducted in accordance with AICPA standard AT Section 101 (AT 101) utilizing the CSA Cloud Controls Matrix (CCM) as additional suitable criteria is likely to meet the assurance and reporting needs of the majority of users of cloud services.

https://cloudsecurityalliance.org./research/collaborate/#_aicpa

HITRUST

July 31, 2014 – HITRUST, the leading organization supporting the healthcare industry in advancing the state of information protection and responsible for the development of the Common Security Framework (CSF), announced a collaboration with the AICPA to develop and publish a set of recommendations to streamline and simplify the process of leveraging the CSF and CSF Assurance programs for the AICPA's Service Organization Control SOC reporting, the accounting standards for reporting service organization controls.

Some of the benefits to healthcare organizations include:

- Leveraging the HITRUST CSF controls in SOC 2 engagements
- Realizing significant time efficiencies and cost savings through synergies between the CSF controls and Trust Services Principles and Criteria
- Reducing the inefficiencies and costs associated with multiple control frameworks and reporting requirements

http://hitrustalliance.net/content/uploads/2014/07/AICPA-and-HITRUST-Press-Release_final-for-wire.pdf

SOC 2 Plus Report – Main Differences

- Opinion – Suitability of the design and operating effectiveness of its controls relevant to security and availability based on the criteria for security and availability in TSP Section 100A, Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Technical Practice Aids) and **the suitability of the design and operating effectiveness of its controls in meeting the criteria in the CCM**
- **Similar modifications to management's assertion**

(Continued on next slide)

SOC 2 Plus Report – Main Differences

G. Relationship between CCM Criteria, Description Sections, and Trust Services Principles and Criteria:

The description sections and the trust services principles and criteria address the CCM as follows (this example mapping represents one approach to providing this information):

CCM Area (Based on version 1.4)	Relevant Description Section	Trust Services Principles and Criteria
1. Compliance		
2. Data governance		
3. Facility security		
4. Human resources security		
5. Information security		
6. Legal		
7. Operations management		
8. Risk management		
9. Release management		
10. Resiliency		
11. Security architecture		

(Continued on next slide)

SOC 2 Plus Report – Main Differences

An alternative approach may be to map the controls into three areas:

1. A mapping of the Trust Services Principles and Criteria to the service organization’s controls
2. A mapping of the CCM to the service organization’s controls
3. A listing of the service organization’s controls with test descriptions

(Continued on next slide)

SOC 2 Plus Report – Main Differences

1.0 Policies

Source: Trust Services Principles and Criteria for Security (S) and Availability (A)
S1.1 The entity's security policies are established and periodically reviewed and approved by a designated individual or group.
A1.1 The entity's system availability and related security policies are established and periodically reviewed and approved by a designated individual or group.

CCM ID	CCM Criteria	Control	Tests of Controls	Results of Tests
IS-03	Management shall approve a formal Information Security Policy document, which shall be communicated and published to employees, contractors, and other relevant external parties. The Information Security Policy shall establish the direction of the organization and align to best practices and regulatory, federal/state, and international laws where applicable. The Information Security Policy shall be supported by a strategic plan and a security program with well-defined roles and responsibilities for leadership and officer roles.	**Content** The Information Security Policy is reviewed by XXXX to ensure it includes: • Strategic plan considerations, • Applicable laws for the respective territories, and • Roles and responsibilities for leadership and officers. **Updates** Responsibility for and maintenance of the Information Security Policy is assigned to the director of information security under the direction of the chief technology officer (CTO). The Information Security Policy is updated at least annually. **Communication** Example Cloud Service Organization publishes and communicates the Information Security Policy to employees, contractors, and external parties at least annually.	Inspected the Information Security Policy dated XX/XX/XXXX and noted that it included: • Strategic plan considerations, • Applicable laws for the respective territories, • Roles and responsibilities for leadership and officers, and • Evidence of review of the update, which occurred within the last year. Obtained evidence of the Information Security Policy being communicated to all employees, Contractors, and vendors via annual written communications and confirmation with each respective party	No deviations noted.

Summary

- **SOC Reporting**
  - Types of reports
  - Risks addressed
- **SOC 2 Reports**
  - Outsourcing, Purpose, System Attributes, Trust Service Principles
  - Engagement, System Boundaries, Report Contents, Modified Opinions
  - Management’s Assertion, Representation Letter, Completing the Engagement, and Implementation Activities
- **SOC 2 Changes**
  - Effective December 15, 2014
  - TSP&C
  - Significant areas of change
  - Steps to take
- **SOC Additional Updates**
  - Extending/customizing reporting
  - Reporting additional subject matter
  - HITRUST
  - SOC 2 Plus Report
  - Differences

?

Questions

Contact information:
angelaappleby@eksh.com
amandaheintze@eksh.com