SOC Reporting / SSAE 18 Update – July, 2017
Agenda

- SOC Refresher
- Overview of SSAE 18
- Changes to SOC 1
- Changes to SOC 2
- Quiz / Questions
Various Types of SOC Reports

SOC for Service Organizations ([http://www.aicpa.org/soc4so](http://www.aicpa.org/soc4so))

- **SOC 1** — SOC for Service Organizations: Internal Controls Over Financial Reporting (ICFR)
- **SOC 2** — SOC for Service Organizations: Trust Services Criteria (TSC)
  - **SOC 2+** — for Service Organizations: TSC + Other Suitable Criteria
- **SOC 3** — SOC for Service Organizations: Trust Services Criteria (TSC) for General Use Report

- *Type 1* (report of the design of controls as of a point in time) and *Type 2* (report of the design and operational effectiveness over a period of time) formats remain unchanged.
Who are SOC reports intended for?

- **SOC 1 reports**—Management of the service organization, user entities, and the auditors of the user entities’ financial statements or internal control over financial reporting

- **SOC 2 / SOC 3 reports**—User entities and prospective user entities who have sufficient knowledge of the subject matter and services provided

- **Coming soon:**
  - SOC for Cybersecurity
  - SOC for Vendor Supply Chains
Which SOC Report is right for my Organization?

Considerations when determining the relevant SOC for service organizations report

- The nature of the service organization, system(s), service(s) provided, and relationship with subservice organizations
- Relevance to user entities’ ICFR
- Fulfilling vendor management requests
- User entity service-level requirements
- Regulatory or industry compliance
Parts of a SOC Report

- **Section I** – Auditor’s Opinion
- **Section II** – Service Organization Assertion
- **Section III** – Narrative Description of the System / environment
- **Section IV** – Matrix of controls, tests of controls, and results of testing
- **Section V** – Other information provided by the Service Organization (additional services, responses to control exceptions, etc.). Unaudited.
## SOC Report Types – Upcoming Changes

<table>
<thead>
<tr>
<th>SOC Report Types</th>
<th>SOC 1</th>
<th>SOC 2</th>
<th>SOC 3</th>
</tr>
</thead>
</table>
| **SOC 1**       | SSAE18 – AT-C 320  
(effective 5/1/17) | Restricted Use Report  
(Type I or II report) | Purpose: Report of a Service Organizations Controls relevant to the user’s Internal Controls over Financial Reporting |
| **SOC 2**       | SSAE18 - AT-C 105  
Aligns with COSO  
(effective 12/15/18) | Generally a Restricted Use Report  
(Type I or II report) | Purpose: Reports on controls related to compliance or operations |
| **SOC 3**       | SSAE18 - AT-C 105 A  
Aligns with COSO  
(effective 12/15/18) | General Use Report | Purpose: Reports on controls related to compliance or operations |
# SOC for Service Organizations

<table>
<thead>
<tr>
<th>OLD</th>
<th>NEW</th>
</tr>
</thead>
</table>
| • SOC = Service Organization Control  
• SOC1 = SSAE16  
• SOC2 / SOC3 based on Trust Services Principles & Criteria  
• Logo = | • SOC = System & Organization Control  
• SSAE18 Governs both SOC1 and SOC2/SOC3 Reports  
• SOC2 / SOC3 based on Trust Services Criteria  
• Principles are now Categories  
• Logo = |
SSAE 18 Overview

- SSAE = Statements on Standards for Attestation Engagements
- SSAE 18 supersedes all existing attestation standards (SSAEs 10-14, 16-17)
- Restructure the Attest Standards
  - AT-C 105: Concepts for All Attestation Engagements
  - AT-C 205: Examination Engagements
  - AT-C 215: Agreed-Upon Procedures Engagements
  - AT-C 320: Reporting on an Examination of Controls at a Service
    Organization Relevant to User Entities’ Internal Controls Over Financial Reporting
- SSAE 18 governs both SOC 1 and SOC 2 Reports
SSAE 18 Changes
(applies to both SOC 1 and SOC 2 Reports)

• Changes are effective for all reports dated on or after May 1, 2017
• Subservice Organizations (clarification of Vendor vs. Subservice organization):  
  • Requirement for the service organization to implement controls to monitor  
    the effectiveness of internal controls at all subservice organizations  
  • Complementary subservice organization controls (CSOC)  
• Auditor is required to obtain an understanding of the subject matter and identify  
  and assess the risk of material misstatement AND perform procedures in  
  response to identified risks  
  • A requirement for the Auditor to read the reports of the internal audit  
    function and regulatory examinations that relate to the services provided  
    to user entities and the scope of the engagement.
SSAE 18 Changes
(appplies to both SOC 1 and SOC 2 Reports)

• As part of collecting and assessing evidence, practitioners need to evaluate the reliability, completeness, and accuracy of information produced by the entity (IPE)
• Complementary user entity controls are limited to controls that are necessary to achieve the control objectives stated in management’s description of the service organization’s system.
• SOC 1 reports are called SOC 1 reports (not SSAE16 reports)
SSAE 18 Changes

• Changes are effective for all reports dated on or after May 1, 2017
• Subservice Organizations (clarification of Vendor vs. Subservice organization):
  • Requirement for the service organization to implement controls to monitor the effectiveness of internal controls at all subservice organizations
  • Complementary subservice organization controls (CSOC)
• Auditor is required to obtain an understanding of the subject matter and identify and assess the risk of material misstatement AND perform procedures in response to identified risks
  • A requirement for the Auditor to read the reports of the internal audit function and regulatory examinations that relate to the services provided to user entities and the scope of the engagement.
Subservice Organizations

- Differentiate between Vendor and Subservice Provider (all Subservice Providers are vendors, but not all vendors are Subservice Providers)
- Would the controls performed by the subservice organization be included if they were performed by the service organization? Are the controls relevant to achieving the controls objectives (SOC 1) or criteria (SOC 2)?
Subservice Organizations

- New requirement for the service organization to implement controls to monitor the effectiveness of internal controls at all subservice organizations.
  - This is more than just gathering SOC reports from your subservice providers, and giving them to your auditor as evidence. There needs to be a process to monitor the controls at the subservice organization. A SOC report would need to be reviewed and analyzed, and this review needs to be documented.
  - Complementary subservice organization controls (CSOC) is a new term. Similar to CUEC’s, the CSOC’s should be explicitly identified and separately documented in the SOC report.
- Subservice providers can be treated in a SOC report using the Inclusive or Carve-out Method.
  - **Inclusive** – auditor tests the controls, and subservice organization provides an assertion, and signs a representation letter.
  - **Carve-out** – The subservice organization is excluded, but is still identified in the report. CSOC's are identified.
SSAE 18 Changes

• Changes are effective for all reports dated on or after May 1, 2017
• Subservice Organizations (clarification of Vendor vs. Subservice organization):
  • Requirement for the service organization to implement controls to monitor the effectiveness of internal controls at all subservice organizations
  • Complementary subservice organization controls (CSOC)
• Auditor is required to obtain an understanding of the subject matter and identify and assess the risk of material misstatement AND perform procedures in response to identified risks
  • A requirement for the Auditor to read the reports of the internal audit function and regulatory examinations that relate to the services provided to user entities and the scope of the engagement.
Risk Assessment / Materiality

- This is a step to be executed and documented by the Auditor (requiring information / evidence from the assessed entity). Questions that the Auditor will evaluate:
  - Is the subject matter (description of the system) not fairly presented? Does it provide sufficient information?
  - Are the controls suitably designed to achieve the control objectives (SOC 1) or criteria (SOC 2)?
  - Was the correct SOC report type (SOC 1 or SOC 2) selected?
  - Are the control objectives specified (SOC 1) or the categories and criteria selected (SOC 2) by the service organization management appropriate for the circumstances?
  - Materiality in the context of a SOC report primarily relates to qualitative factors
SSAE 18 Changes

- As part of collecting and assessing evidence, practitioners need to evaluate the reliability, completeness, and accuracy of information produced by the entity (IPE)
- Complementary user entity controls are limited to controls that are necessary to achieve the control objectives stated in management’s description of the service organization’s system.
- SOC 1 reports are called SOC 1 reports (not SSAE16 reports)
IPE

• IPE = information produced by the entity. Could be populations, screenshots, reports, other evidence, etc.
• For those familiar with Sarbanes-Oxley (SOX), we are moving closer to that method of IPE / evidence validation.
• The auditor is now required to document how that validated IPE. Optionally can include this as test procedures in the SOC report.
• What are acceptable methods for meeting this new IPE requirement?
  • Observe populations being created
  • Re-validate that a population can be generated again with the same results.
  • Observe screenshots being taken
• There is quite a bit of subjectivity here…
SSAE 18 Changes

- As part of collecting and assessing evidence, practitioners need to evaluate the reliability, completeness, and accuracy of information produced by the entity (IPE).
- Complementary user entity controls are limited to controls that are necessary to achieve the control objectives stated in management’s description of the service organization’s system.
- SOC 1 reports are called SOC 1 reports (not SSAE16 reports).
Complementary User Entity Controls (CUEC’s)

- CUEC’s are listed separately in the SOC report. They list controls that the customer is responsible for.
- In some cases, these lists go far beyond the scope of the customer responsibility.
- CUEC’s are now limited to controls that are necessary to achieve the controls stated in management’s description of the service organization’s system.
- Examples of appropriate and inappropriate CUEC’s:

<table>
<thead>
<tr>
<th>Appropriate</th>
<th>Inappropriate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer are responsible for creating new user accounts, and setting password parameters for new users in the XX Application.</td>
<td>Customers are responsible for the accuracy of all payroll calculations.</td>
</tr>
<tr>
<td>Control</td>
<td>Type</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Customer are responsible for creating new user accounts, and setting</td>
<td>CUEC</td>
</tr>
<tr>
<td>password parameters for new users in the XX Application.</td>
<td></td>
</tr>
<tr>
<td>Application code changes are authorized and tested prior to</td>
<td>Standard</td>
</tr>
<tr>
<td>migration to production.</td>
<td></td>
</tr>
<tr>
<td>Production servers are physically protected from unauthorized access</td>
<td>CSOC</td>
</tr>
<tr>
<td>via badge readers.</td>
<td></td>
</tr>
</tbody>
</table>
SOC 2 Specific Changes

• Changes are effective for audit periods ending on or after December 15, 2018
  • Until then, service organizations can choose to early adopt, or continue with current TSP.
• Trust Services Principles & Criteria (TSP) being renamed to Trust Services Criteria (TSC). The Principles are being renamed to Categories.
• The Common Criteria (28) are being remapped to the COSO 2013 Framework plus some additional criteria for a total of 33 Common Criteria. The Additional Categories have been further reduced. The illustrative risks / controls have been replaced with points of focus.
• There is a proposed Cybersecurity Standard with 31 criteria (no current estimated release or effective date)
A SOC2 Report is based upon the below five Trust Principles. A report must include the Security Principle (Common Criteria), and may include any or all of the additional principles. Each principle contains criteria which must be met as part of the SOC2 audit.

**Security**
The system is protected against unauthorized access, use, or modification.

28 required (common) criteria

**Availability**
The system is available for operation and use as committed or agreed.

3 additional criteria

**Confidentiality**
Information designated as confidential is protected as committed or agreed.

8 additional criteria

**Processing Integrity**
System processing is complete, valid, accurate, timely, and authorized

6 additional criteria

**Privacy**
This principle addresses the system’s collection, use, retention, disclosure, and disposal of PII in accordance with commitments and system requirements.

20 additional criteria
SOC2 Categories

(Required for reports with audit periods ending after 12/15/2018)

A SOC2 Report is based upon the below five Categories. A report must include the Security Category (Common Criteria), and may include any or all of the additional categories. Each category contains criteria which must be met as part of the SOC2 audit.

- **Security**: The system is protected against unauthorized access, use, or modification.
  - 33 required (common) criteria

- **Availability**: The system is available for operation and use as committed or agreed.
  - 3 additional criteria

- **Confidentiality**: Information designated as confidential is protected as committed or agreed.
  - 2 additional criteria (was 8)

- **Processing Integrity**: System processing is complete, valid, accurate, timely, and authorized.
  - 5 additional criteria (was 6)

- **Privacy**: This principle addresses the system’s collection, use, retention, disclosure, and disposal of PII in accordance with commitments and system requirements.
  - 18 additional criteria (was 20)

Common Criteria Framework
SOC 2 – New Common Criteria

Adds eight new common criteria related to the alignment with COSO principles:

- CC1.2—Board oversight
- CC2.1—Use of information to support internal control
- CC3.1—Sufficiency and clarity of the entity’s objectives
- CC3.4—Identification and assessment of changes
- CC5.3—Controls deployed through formal policies and procedures
- CC7.1—Procedures to identify new vulnerabilities
- CC9.1—Business disruption risk mitigation
- CC9.2—Vendor and business risk management
SOC 2 – Modifications to Confidentiality Criteria

Modifies confidentiality criteria to streamline into the relevant common criteria:

- Moves C1.1 (Protect information throughout system changes) to CC8.1 (Formal change management process)
- Moves C1.2 (Controls to protect against unauthorized access) to CC6.1 (Logical access and authentication controls)
- Moves C1.3 (Controls over access from outside the system boundary) to CC6.6 (Logical access controls to protect against external threats)
- Moves C1.4 and C1.5 (Third party and vendor confidentiality commitments) to CC9.2 (Vendor and business party management)
- Moves C1.6 (System changes are communicated to external users and third parties) to CC2.2 and CC2.3 (Communication to internal and external users)
SOC 2 – Modifications to Privacy Criteria

Modifies privacy criteria to streamline into the relevant common criteria:

- Moves P1.2 (Privacy commitment communications) to CC2.3 (Communication to external users)
- Moves P6.5 and P6.6 (Compliance with commitments periodically assessed) to CC9.2 (Risk mitigation and assessment)
Criteria Mapping

- TSP mapped to the new TSC (excel sheet)
## New TSC Statistics

<table>
<thead>
<tr>
<th>Principle</th>
<th>Number of Criteria</th>
<th>Points of Focus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Criteria</td>
<td>33</td>
<td>197</td>
</tr>
<tr>
<td>Availability</td>
<td>3</td>
<td>15</td>
</tr>
<tr>
<td>Processing Integrity</td>
<td>5</td>
<td>18</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>Privacy (organized in eight categories)</td>
<td>18</td>
<td>59</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>61</strong></td>
<td><strong>297</strong></td>
</tr>
</tbody>
</table>

How many controls does this equate to??
Quiz

• Who is responsible for designing and implementing the controls?
• Who is responsible for validating that the controls are properly designed?
• Who is responsible in a SOC 2 scenario for mapping the criteria to the controls at the service organization?
• Who is responsible for the assertion?
• Who documents that IPE was accurately provided?
• Who is responsible for determining whether to use the inclusive or carve-out method for a subservice organization?
• Who is responsible for determining which report to pursue (SOC 1 or SOC 2)?
Quiz (continued)

- Can IT general controls (access, change management, etc.) be included in a SOC 1 report?
- Who is responsible to write the system description (section III of the SOC report)?
- Can availability controls be included in a SOC 1 report?
- Can transaction processing controls be included in a SOC 2 report?
- Is it possible to fail a SOC audit?
- What is a scope limitation?
- What is a SOC 2 + Report?
Questions?