SSAE 18 & SOC Reporting: What You Need to Know

ISACA Chapter Meeting

March 2017

weaver

Assurance • Tax • Advisory

What We'll Cover

- Brief Introduction
- Purpose of SOC Reporting
- Changes in Requirements
- Gaining Value from the Report
- Planning Forward
- Closing / Questions

With You Today

Neha Patel

- Firm methodology leader for in third-party audits, including service organization control (SOC) audits
- Co-presenter at national AICPA SOC School
- Passion for servicing clients that blend technology and accounting processes

With You Today

Susan Pradhan

- Over 5 years experience in evaluating control environments across various industries
- Subject matter expert in SOC audits
- Assistant Treasurer for ISACA NTX

Disclaimer

- The comments and statements in this presentation are the opinions of the speakers and do not necessarily reflect the opinions or positions of Weaver and Tidwell L.L.P.
-
- Weaver and Tidwell L.L.P expressly disclaims any liability in connection with the use of this presentation or its contents by any third party.

IT Advisory Services

weaver
Assurance • Tax • Advisory

IT Advisory Services (ITAS) is a collection of assurance and consulting services focused on information technology. We work with IT organizations, internal audit departments, security organizations and more.

Resource Optimization

- Software Selection
- Independent Verification & Validation
- IT Assessments & Planning
- IT Governance

- IT Risk Assessment
- IT Audit
- Project Risk Management
- Service Organization Control (SOC)

Risk Management

Security & Availability

- Information Security
- Data Privacy
- Business Continuity/ Disaster Recovery

- Payment Card Industry (PCI)
- Gramm-Leech Bliley
- Sarbanes-Oxley
- HIPAA
- FFIEC & FDICIA

Compliance

Purpose of SOC Reporting

What is a Service Organization Controls Audit?

weaver
Assurance • Tax • Advisory

- First released in 1993 as the Statement on Auditing Standard No. 70 (SAS 70)
  - Focus was on understanding the risks associated with significant processes that are outsourced.
  - The standard and the deliverable were known in the marketplace as “SAS 70”.
  - As technology became more predominant, technical service providers were also asked for SAS 70 reports.

What is a Service Organization Controls Audit?

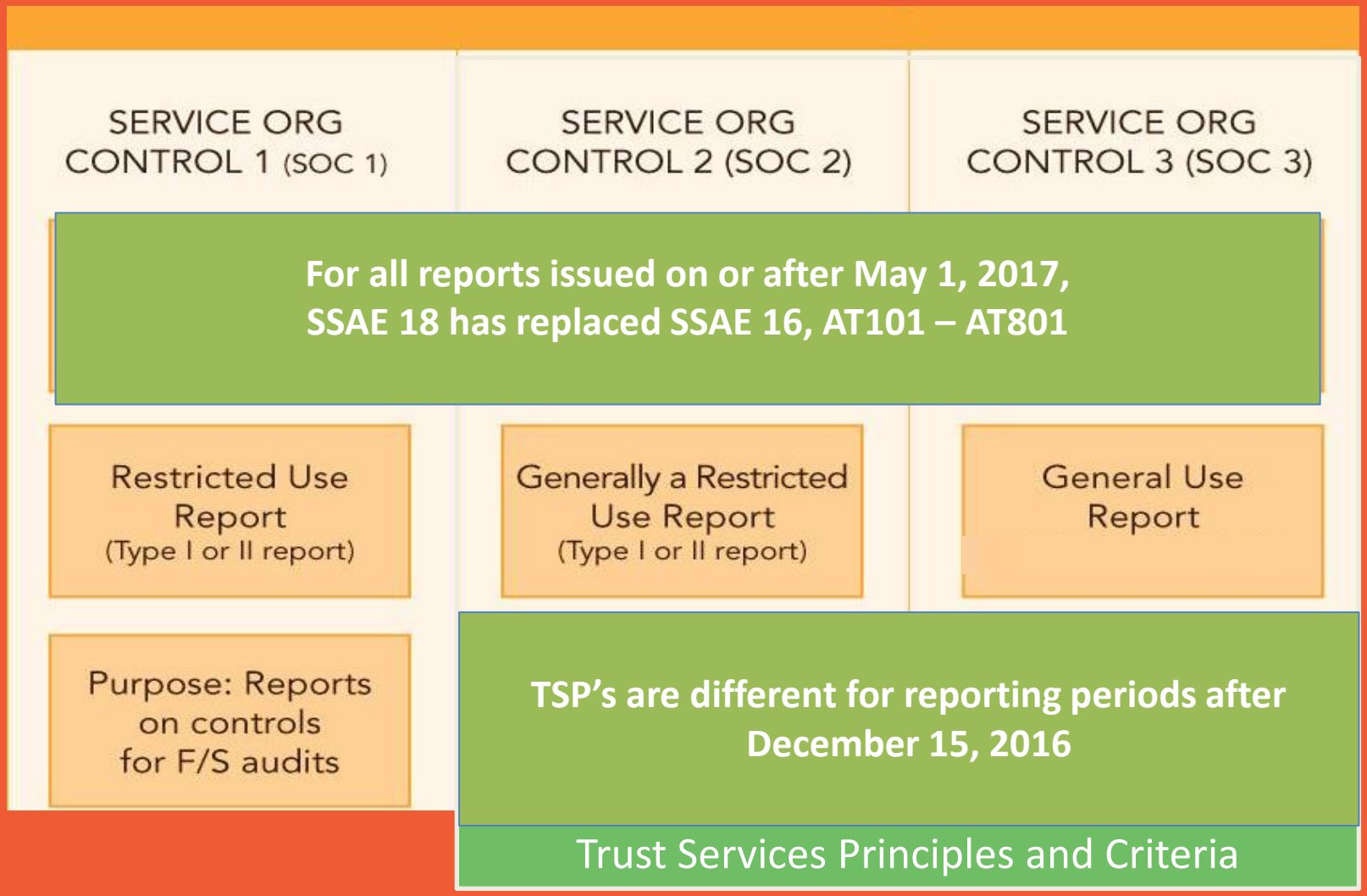
- In 2011, the American Institute of Certified Public Accountants (AICPA) refined the instructions and applicability of service organization audits.
  - Purpose was to provide a path for risks related to financial reporting, or risks that related to operational functions.
  - Customized scoping and two timeframe options, provided five (5) different report deliverable options.

Assurance in the Cloud

weaver
Assurance • Tax • Advisory

- AICPA Reporting
  - SOC 1
  - SOC 2
  - SOC 3
- ISO 27001
- CSA CCM
- HITRUST CSF
- PCI DSS ROC
- FedRAMP: NIST 800-53

2017 Revised SSAE 18



Note: The SOC 3 report was formerly SysTrust for Service Organizations.

Understanding SOCs

To understand Service Organization Controls (SOC), it is first important to understand who is being audited and who the report is ultimately being prepared for.

User Entity

Service Organization

Understanding SOCs

Service organizations may outsource certain processes relevant to user entity financial reporting to other organizations known as subservice organizations.

Such outsourced processes provided by subservice organizations maybe carved out or included in the scope of the SOC audit.

Type 1 vs. Type 2 Reports

Under the new standard, we still have two types of reports can be created: Type 1 and Type 2. Both types report on the fairness of the presentation of management's description of the service organization's system.

Key differences include:

- **Type 1** also reports on 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** also reports on the suitability of the design and **operating effectiveness** of the controls to achieve the related control objectives included in the description **over a specified period** (typically 6 months to 12 months)

SOC 2: Trust Service Principles

weaver
Assurance • Tax • Advisory

SOC 2 engagements are designed to evaluate an organization's information systems relevant to one or more Trust Services Principles (TSPs).

The Security Principle:

- The system is protected against unauthorized access (both physical and logical).

The Availability Principle:

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

The Processing Integrity Principle:

- System processing is complete, accurate, timely and authorized.

The Confidentiality Principle:

- Information designated as confidential is protected as committed or agreed.

Privacy is also included as a separate trust principle, and is actually a collection of principles known as *Generally Accepted Privacy Principles* (GAPP).

Change is coming…

SSAE 18

- SSAE 18 replaces all prior standards, including AT 101 (so SOC 2 and 3 will follow SSAE 18 rules)
- Effective for practioners' reports dated on or after May 1, 2017

AT-C Section in SSAE 18	Contents
AT-C 105	Common Concepts to All Attestation Engagements
AT-C 205	Examination Engagements
AT-C 315	Compliance Attestation
AT-C 320	Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting

Changes in Requirements

weaver
Assurance • Tax • Advisory

1. Complementary User Entity Controls (CUECs)
2. Complementary subservice organization controls (CSOCs)
3. Completeness and accuracy of information provided by the entity(IPE)
4. Management must determine (a) suitable criteria and (b) measurement of subject matter
5. Auditor must obtain an understanding over preparation of subject matter
6. Review of internal audits and regulatory examination reports

Changes in Requirements

- Complementary User Entity Controls (CUECs)
  - Controls that the service organization assumes, in the design of their system, will be implemented by user entities and are necessary to achieve the control objectives stated in management's description.
  - The SOC 2 guide had differentiated the difference between user entity responsibilities and user entity controls.
  - SSAE 18 clarifies and standardizes this requirement across all SOC reporting types.

User Entity

Service Organization

Changes in Requirements

- Complementary subservice organization controls (CSOCs)
  - Controls that the service organization assumes, in the design of their system, will be implemented by subservice organizations and are necessary to achieve the control objectives stated in management's description.
  - The SOC 2 guide had already included consideration for criteria that are fulfilled by subservice organizations.
  - SSAE 18 clarifies and standardizes this requirement across all SOC reporting types.

Changes in Requirements

weaver
Assurance • Tax • Advisory

- Information provided by the entity(IPE)
- Three types of reports to consider:
  - Information that is generated directly from the service organization's systems for the purpose of the audit. Ex. Population of tickets, population of new hires for the reporting period.
  - Information generated by the service organization used in the performance of management's controls. Ex. GL account details used in reconciliations,
  - Reports that are produced and relied upon by user entities.
- Continued focus on completeness and accuracy
- Although no explicit requirement to document in the report – but service auditors should provide enough context for user entities to rely

Changes in Requirements

- Management must determine (a) suitable criteria and (b) measurement of subject matter
  - Subject matter – risks relevant to user entities surrounding the outsourced service
  - Criteria – benchmark used to evaluate subject matter (e.g., attributes of the control)
  - Suitable – the criteria is appropriate to evaluate the risk factor and the criteria are free from bias.
  - Measurable – permit reasonably consistent measurements, qualitative or quantitative, of subject matter. (e.g., frequency, documentation)

Key Difference

Rather than performing an independent assessment, need to focus on management's evaluation of control design and implementation.

Auditor must obtain an understanding over preparation of subject matter by:

- Understanding management's process for identifying and evaluating risks that are relevant for user entities
- Evaluating the linkage of controls to those risks
- Determining that controls have been implemented

Examples of Design

- Management is responsible for their description, including identification of risks and controls relevant to their system of internal control.
- Examples of how to document:
  - Risk and control matrices
  - Risk assessments that tie back to control activities, process owners and frequency of controls

Changes in Requirements

- Review of internal audits and regulatory examination reports
  - New standards require that auditors review internal audit reports and other regulatory examination reports published by management.

The good news…

- SOC reports will still be referred to as "SOC".
  No need to reference the standard (SSAE 18).
  And definitely don't call it SAS 70!

- All reports issued on or after May 1, 2017 will follow SSAE 18. No need to remember the old way!

- SOC 2 & 3 audits have already incorporated several of these requirements.

Gaining Value from the Report

Value in the SOC Report

Sections in the Report

- Section I: Independent Auditor's Report (i.e., Opinion)
- Section II: Management Assertion
- Section III: Description of the System
- Section IV: Description of Test of Controls and Results
- Section V: Additional Information (optional / unaudited)

What Matters to Users?

- **Section I: Independent Auditor's Report (i.e., Opinion)**
- Section II: Management Assertion
- Section III: Description of the System
- **Section IV: Description of Test of Controls and Results**
- Section V: Additional Information (optional / unaudited)

What Matters to Users?

- Section I: Independent Auditor's Report (i.e., Opinion)
  - Provides user entities with the overall evaluation over the areas reviewed in the report.
  - If qualified, the opinion will outline the areas that could not be achieved (i.e., failure) or the areas that were not available for review (i.e., scope limitation).

What Matters to Users?

weaver
Assurance • Tax • Advisory

- Section IV: Description of Test of Controls and Results
  - Provides user entities with detail regarding the individual criteria, testing procedures performed and results by control / criteria.
  - SOC 3 reports will NOT include this detail.

Planning Forward

Planning Forward

weaver
Assurance • Tax • Advisory

Service Organization

1. Do we need an SOC audit?
2. What services do we offer and how does it mitigate risk for our customers?
3. Do our services relate to financial reporting processes or operational aspects?
4. Have we considered how to document the new requirements?

Planning Forward

User Entity

1. Do we need to obtain a SOC report?
2. What services do we use and how is our risk mitigated?
3. Does the report provide context for us to place reliance?


weaver
Assurance • Tax • Advisory
Discussion