



## SSAE 16: Lessons learned from initial compliance

- 1) A brief perspective on SAS 70 and SSAE 16
- 2) Requirements defined in Statement on Standards for Attestation Engagements “Reporting on Controls at a Service Organization”
- 3) Important lessons from service organization controls reporting (SOC 1)

## Section 1

# A BRIEF PERSPECTIVE ON SAS 70 AND SSAE 16

## AICPA replaced SAS 70

- > Effective for audit periods ending after June 15, 2011

## Why

- > Confusion in the market – “we are SAS 70 certified”
- > Frequently misused to report on controls not relevant to financial reporting – market demand for expanded scope of report
  - Security
  - Availability
  - Processing integrity
  - Confidentiality
  - Privacy

## Why - continued

- > Growth of the service organization landscape
- > Convergence of US and international standards

## So what's next?

- > New attest standard: SSAE 16
- > New reporting options: SOC 1, SOC 2, SOC 3

## SOC 1

(Service organization control 1)

Applicable to services that are likely to be relevant to user entities' internal control over financial reporting

Reports on controls supporting financial statement audits

Restricted to customers during the audit period

Example organizations: payroll processors, transaction processors

## SOC 2

(Service organization control 2)

Applicable to services that don't directly impact financial reporting

Reports on controls related to operations

Restricted to those familiar with the subject matter

Example organizations: Direct mailers, call centers

## SOC 3

(Service organization control 3)

Applicable to services that don't directly impact financial reporting

Reports on controls related to operations

General use report

Example organizations: Direct mailers, call centers

## Section 2

# **REQUIREMENTS DEFINED IN STATEMENT ON STANDARDS FOR ATTESTATION ENGAGEMENTS "REPORTING ON CONTROLS AT A SERVICE ORGANIZATION" (SSAE 16)**

## Sections

1. **Service auditor's report (the opinion)**
2. **Management's assertion**
3. **System description**
4. **Tests of controls and results**
5. **Additional information provided by the service organization**

### Three separate opinions in the report:

- > Whether the system description is fairly presented
- > Whether the controls were suitably designed
- > In a Type 2 – Whether the controls operated effectively

### Timing aspects can vary:

- > Type 1 is as of the report date
- > Type 2 is for the range specified in the report

The assertion is management's commitment to the suitability and accuracy of the description. Key elements of your assertion include:

- > The specific criteria used in preparing the system description:
  - How the system processes relevant transactions
  - Representation to the completeness of the description and lack of distorted or misrepresentative information about the service
- > A statement on the suitability of the design of controls and the criteria management used to make that statement
- > A statement on the operating effectiveness of controls and the criteria management used to make that statement

The system description is management's objective description of the service provided. The description must:

- > Provide the reader with information about the system that may be relevant to the user entity's internal control over financial reporting
- > Include the type of service provided, including classes of transactions processed and the related accounting records
- > Include the procedures used to initiate, authorize, record, process, correct, and report transactions, as well as how the system captures and addresses other significant events
- > Identify any deficiencies in general computer controls and their impact on the operation of programmed procedures
- > Include information about the frequency and nature of the controls
- > Include any required complementary user entity controls

**The service auditor provides a description of the tests performed and test results. The report must:**

- > Identify the controls that were tested
- > Indicate whether all items in a population were evaluated, or a selection thereof
- > Provide enough detail about tests performed to allow a user auditor to determine the effect of the tests on their risk assessments.

**If deviations are identified, the results must include:**

- > The number of items tested
- > The number and nature of deviations

Occasionally, service organizations wish to include additional information which doesn't relate to internal control over financial reporting at a user entity. In such cases:

- > Management of the service organization should provide this information in a clearly identified separate section of the description
- > The service auditor reviews the additional information to determine whether it contains any material inconsistencies or misstatement of fact

## What's in the report?

- > **Formal audit letter**
- > **Management's assertion**
- > **Management's system description, including specified control objectives**
- > **Tests of controls and results**

## Impacts to service organizations

- > **Written assertion about the accuracy and relevance of the system description and the design and operating effectiveness of controls**
- > **Specify the criteria used in making the assertion**
- > **Management must have a reasonable basis for its assertion**
- > **Document and disclose changes in controls during the period**

## Impacts to user entities

- > **Can be used to support financial statement audit**
- > **Need to evaluate exceptions and determine relevance and any additional analysis**
- > **Should be evaluated and confirm compliance with user control considerations**

## Section 3

# **IMPORTANT LESSONS FROM SERVICE ORGANIZATION CONTROLS (SOC 1) REPORTING**

1. Descriptions of controls
2. Testing
3. Relevance
4. Basis for assertions
5. Other lessons learned

It is management's responsibility to prepare its description of its system.

> Including control objectives and related controls to achieve them

Must fairly present the system that was designed and implemented during the period.

> Focus on key controls

> Cannot omit or distort relevant information

### Must be fact based / data driven

- > Relevant to the user organization financial statement controls

### Must be validated

- > Example - balance score card metrics don't belong
- > No marketing matters
- > No subjective commentary

Management must identify risks that threaten the achievement of the control objectives stated in the description.

- > Risk mapping required
- > For ongoing engagement – this may take additional up front effort to determine if any additional risks exist
  - Risk assessment (not “one and done”)
  - Review and assess each engagement

## Timing of testing

- > Interim testing may be beneficial – depends on length of period
- > Does service organization also require a financial statement audit? If performed by same auditor as SOC 1, potential efficiencies obtained
- > Planning ahead necessary by audit team and service organization

Have information and applicable process owners available and timely.

Appropriately performing a Type 1 vs Type 2?

- > Review customer contracts

### Control deviations and exceptions noted

- > Effect on assertions and audit report
- > Has it been remediated?
- > Response by management
- > How significant is deviation? May result in qualified or adverse

## Determined by service organization

- > Auditors are not able to determine relevance
- > Service organizations must determine based on relevance to user entities' internal control over financial reporting
  - Going from SAS 70 to SSAE16: historical SAS 70 controls may be non-financial
- > User controls
- > Determining the best period to test? (6 - 12 months)
  - Any changes to system during period?

### Must be a reasonable basis

- > Criteria need to be available to user entities to enable them to understand basis for management's assertion about fair presentation of management's description

Management's monitoring activities may provide evidence of the design and operating effectiveness of controls in support of management's assertion.

### Timing of management providing assertion

- > Any time after end of period covered
- > Date of report can be no earlier than date management provides assertion
- > Typically provided by those that sign rep letter

### Materiality – qualitative

- > “Would knowing this affect my decision as a user of the report?”

### Changes to system during the testing period

- > Requires testing of control both before and after change
- > Applicable to changes material to user only
- > Is description still fairly stated?

### Subsequent events

- > Any event after period covered, up to date of report
- > If have a significant effect on management's assertion
- > Disclose in auditor's report

### Restricted use of report

- > Can report be provided to prospective clients?

### SOC 1 seal on website

- > Can service organizations use after examination completed?

Pursuant to the rules of professional conduct set forth in Circular 230, as promulgated by the United States Department of the Treasury, nothing contained in this communication was intended or written to be used by any taxpayer for the purpose of avoiding penalties that may be imposed on the taxpayer by the Internal Revenue Service, and it cannot be used by any taxpayer for such purpose. No one, without our express prior written permission, may use or refer to any tax advice in this communication in promoting, marketing, or recommending a partnership or other entity, investment plan, or arrangement to any other party.

Baker Tilly refers to Baker Tilly Virchow Krause, LLP, an independently owned and managed member of Baker Tilly International. The information provided here is of a general nature and is not intended to address specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought. © 2012 Baker Tilly Virchow Krause, LLP