



Goodbye, SAS 70! Hello, SSAE 16!

A Session to Provide Insight on the New Standard and
What Service Providers and End-Users Need to Know

January 3, 2012

Agenda

- Introduction
- Background on what was SAS 70
- Why SSAE 16 replace SAS 70?
- Key points and differences with SSAE 16
- Service Organization Controls (SOC) Reports Overview and types of reports
- SSAE 16 – The Standard
- AICPA Service Organization Reports (SOC)
 - Different Types of SOC Reports
 - Purpose of Each SOC Report
 - AT 101, 201, 601

Introduction and Disclaimer

Introduction

Sue Horn
Manager
Crowe Horwath LLP
Office: 614.365.2236
e-mail: sue.horn@crowehorwath.com

Disclaimer

- All diagrams and examples presented here are solely for illustration purposes and should not be interpreted as being used for anything other than material for developing an understanding of the SSAE 16 standard.

Background

- What is a “SAS 70 report”?
 - SAS 70 was an audit standard issued in 1992
 - Intended to cover internal controls over financial reporting only
- Since 1992....
 - Globalization
 - Rapid expansion of business process outsourcing
 - The Internet, Google, Cloud Computing, Virtualization, Smart Phones!
- U.S. & International convergence
 - Standards
 - Methodology
 - Consistency



Standards

- **International Federation of Accountants (IFAC)**
 - International Auditing and Assurance Standards Board (IAASB)
 - International Financial Reporting Standards (IFRS)
 - International Standard on Assurance Engagements (ISAE)
- **American Institute of CPAs(AICPA)**
 - Auditing Standards Board (ASB)
 - Statement on Standards for Assurance Engagements (SSAE)



Why Replace SAS 70 with SSAE 16?

- Although used internationally for years, these reports were only issued by US registered firms (or at least signed by and supervised by them).
- New International Standards were Developed
- International Standards on Assurance Engagements (ISAE) 3402 was finalized by the International Auditing and Assurance Standards Board (IAASB) of IFAC and released in December 2009.
- SSAE No. 16 is a product of the ASB's of AICPA efforts to clarify its standards and to converge with standards of the IAASB



Key Point: SSAE 16 is the U.S. equivalent to ISAE 3402, with minor differences



SSAE 16 - The Standard, aka – AT 801, SOC 1 and ISAE 3402

- **Why so many names?**

- **SSAE 16**

- AICPA makes proposed changes they come out as Statements on Standards for Attestation Engagements

- **AT section 801**

- When the guidance is accepted and effective it is included in the AICPA code
 - Attestation Standards (AT) section 801 was reserved for SSAE 16

- **SOC 1**

- The AICPA is attempting to bring more visibility to other reporting options for Service Organizations (SOC 1 = SSAE 16 = AT801)

- **ISAE 3402**

- International Standard from IFAC, (Approximates SSAE 16)

SSAE 16 – Key Points

- SSAE 16 completely replaces SAS 70
- Effective for reports with periods ending on or after June 15, 2011
- Is consistent with International guidance ISAE 3402
- Service auditor is attesting to management's description of systems and controls
- Focus is on controls at service organizations that are likely to be relevant to user entities' internal controls over financial reporting
- The report may be as of a certain date (type 1) or cover a timeframe typically between six months and one year (type 2)

 **Key Point:** The focus of SSAE 16 is the same as the focus of SAS 70

- **A comment from the AICPA:** Compliance with SSAE 16 does not result in an organization becoming SSAE 16 “certified” or gaining a certificate or designation.

SSAE 16 – Changes from the SAS 70 Standard

- Management must provide a written assertion
- Management will need to have a basis for providing their assertion
- A Type 2 opinion now covers design of the controls throughout the time period
- Any significant changes to systems (including controls) need to be disclosed, typically included in the description of systems
- Changes in scope after the auditor is engaged will require a “reasonable basis”
- Policies, procedures, and practices of the service organization need to be formally documented
- Sub-service Organization inclusive or carve-out method may be used. When using the inclusive method, the subservice organization must provide a description of controls and control objectives, written assertion, and letter of representation.

 **Key Point:** Service Organizations can not omit a control simply because it fails!

SSAE 16 – Who Might Issue an SSAE 16?

- “SSAE No. 16 is applicable when an entity outsources a business task or function to another entity (usually one that specializes in that task or function), and the data resulting from that task or function is incorporated in the outsourcer’s financial statements” * *Credit: AICPA FAQ*

- Some examples of service organizations...
 - A company that develops & hosts banking software
 - Outsourced payroll processors
 - A bank offering trust and investment services
 - Medical claims processors
 - A company that computes commission payments for your sales team

SSAE 16 – Why Review an SSAE 16?

- To gain comfort over a service organization's internal controls over financial reporting
- To better understand the service organization's systems and controls
- To identify any errors or exceptions noted by the independent service auditor, which will allow you to consider if there's any potential impact on your financial statements, and take appropriate remedial action.

Statement of Controls (SOC) Reports - Overview

- CPA's are being asked to provide assurance on topics other than financial statements, which can not be done under SAS 70
- AICPA created separate reports for internal controls over financial reporting and reports on other types of controls
- The AICPA has added two additional new reporting options.
 - The three reporting options are :
 - SOC 1 – Report on controls over financial reporting (SSAE 16 / SAS 70 purpose)
 - SOC 2 – New reporting option
 - SOC 3 – New reporting option
 - And, AT 101, AT 201 and AT 601 are still in effect



Key Point: Types of SOC Reports

Report	Report's focus	Audience
SOC 1	Report on internal controls over financial reporting	Restricted Use
SOC 2	Report on controls related to Security, Availability, Processing Integrity, Confidentiality and/or Privacy (Trust Services Principals)	Restricted Use
SOC 3	Report on controls related to Security, Availability, Processing Integrity, Confidentiality and/or Privacy (Trust Services Principals)	General Purpose

* Courtesy of AICPA

SOC Reports – SOC 1 (SSAE 16 Report)

- SOC 1 reports are prepared in accordance with SSAE 16
- Report on controls as a service organization that may be relevant to a user entities' internal control over financial reporting.
- Report is restricted use
- Generally, most service organizations that were issuing a SAS 70 will be issuing an SOC 1 (SSAE 16) report
 - *Although there will be exceptions for service organizations that had been issuing SAS 70 reports but now more appropriately fall under SOC 2 or SOC 3 criteria or AT 101 or AT 601.*



Key Point: The SOC 1 report has the same focus (on internal controls over financial reporting) as SAS 70.

SOC Reports – SOC 2

- SOC 2 is a new reporting option
- Prepared in accordance with AT Section 101 (Attestation Standards)
- Report on controls other than those likely to be relevant to user entities' internal control regarding financial reporting
 - Non-financial and/or process-oriented controls
 - Scope is restricted to the Trust Services Principles: Security, Availability, Processing Integrity, Confidentiality, Privacy
- The report contains a detailed description of the service auditor's tests of controls and results (similar to SOC 1)
- Restricted use
- Examples of service organizations that may issue an SOC 2 report
 - Cloud computing provider
 - A server collocation facility
 - Managed network security provider
 - Non-financial data entry

SOC Reports – SOC 3

- SOC 3 is a new reporting option, replacing the previous SysTrust and Privacy principle documents
- Prepared in accordance with AT Section 101 (Attestation standards)
- Service auditor reports on whether an entity maintained effective controls over its system as it relates to all five of the Trust Services Principles: security, availability, processing integrity, confidentiality and privacy.
- Intended for audiences that don't necessarily have the expertise to read or want to read a SOC 2 report
- A seal that can be displayed on the company web site



 **Key Point:** A SOC 3 report does not contain a description of the service auditor's tests and results

Attestation Standard AT 101

- Sets forth guidance on Service Standards
 - General Standards
 - Training and proficiency
 - Adequate Knowledge of subject matter
 - Suitability and availability of criteria
 - Independence
 - Due Professional Care
 - Standards of Fieldwork
 - Planning and supervision
 - Obtaining sufficient evidence
 - Standards of Reporting
 - Identifying the subject matter or assertion and state character of the engagement in the report
 - State conclusions about subject matter or assertion
 - State all of the significant reservations
 - State who the report is intended for, if limited use report

AT101 – Key Points

- Management Assertion should be obtained in most cases
- Report is for entities that wish to report on controls over a specified set of objectives (this is not limited to financial transaction processing)
- The opinion is based on a defined criteria or an assertion by Management. The opinion is issued for a high level of assurance (Examination). A negative assurance letter is issued for a level of moderate assurance (Review)
- Use of the report is for general use, reports could also be restricted by the auditor
- The report may be as of a certain date, cover a timeframe, or cover multiple periods
- The Report Includes:
 1. Service Auditor's Report
 2. Subject Matter and/or Management's Assertion
 3. Other Information Provided by the Service Organization

AT201 – Key Points

- AT201 is the standard that Agreed Upon Procedures are conducted under
- Follows Attestation Standards outlined in AT101
- Scope of the report is whatever management and the users of the report have agreed to with the auditor
- Users must agree to the procedures performed
- Distribution is limited to those who have formally agreed to the procedures

AT601 – Key Points

- Management Assertion is Required unless the engagement is required by law
- Follows Attestation Standards outlined in AT101
- For organizations that have a specific regulation or law that sets the “Criteria” such as GLBA or HIPAA
- Opinion:
 - Examination: Opinion is based on the entity's compliance with specified requirements or the entity's assertion about compliance with specified requirements.
 - Agreed-Upon Procedures: No opinion.
- Use of the report:
 - For Examination: A statement restricting use to specified parties may be included.
- Information reported on can be compliance with specified requirements. Also the information may be financial or nonfinancial.
- Timeframe of the report may be as of a certain date or cover a timeframe .

SSAE 16 (SOC 1) Report – Walkthrough

SOC 1 - Report Sections

Management Assertion

Service Auditor Opinion

Description of Systems

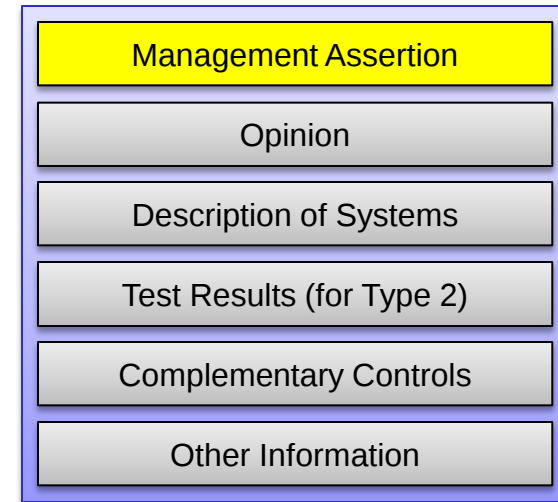
Test Results (for Type 2)

Complementary Controls

Other Information

Management Assertion

- **The written assertion must cover:**
 - Fair presentation of the description of systems
 - Suitability of the design of controls
 - Operating effectiveness (Type 2 only) of controls
- **Management must have a “reasonable basis”**
 - The basis is the reason management believes that the controls were appropriately designed and operating effectively throughout the period
 - May rely on Internal Audit testing
 - May not rely on testing done by **independent** service auditor
- The written assertion is provided to the service auditor by management



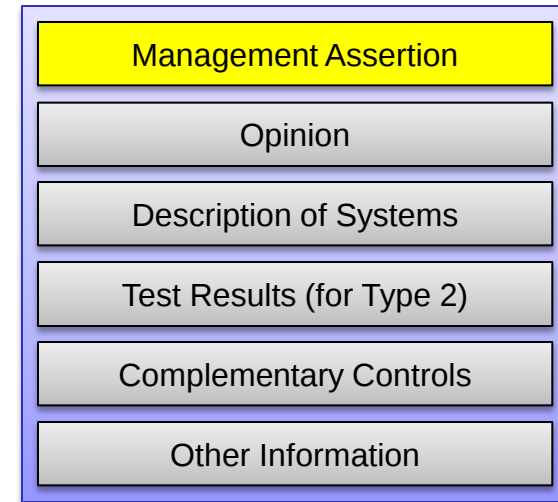
Reviewing the Management Assertion

- **What to look for when reviewing:**

- Is the time period appropriate?
- Does it cover the application and/or service you are using?
- Does it fully acknowledge management's responsibilities?

- **Management must acknowledge in writing:**

- That their description doesn't omit or distort information
- The criteria they used when making the assertion that the description is presented fairly
- That their description includes any relevant details of changes to systems that occurred during the time frame
- That it has identified risks that threaten the achievement of the control objectives (risk assessment)
- The controls & control objectives specified provide reasonable assurance that identified risks would not prevent the control objectives from being achieved



Independent Service Auditor's Opinion

- **What's in the opinion:**

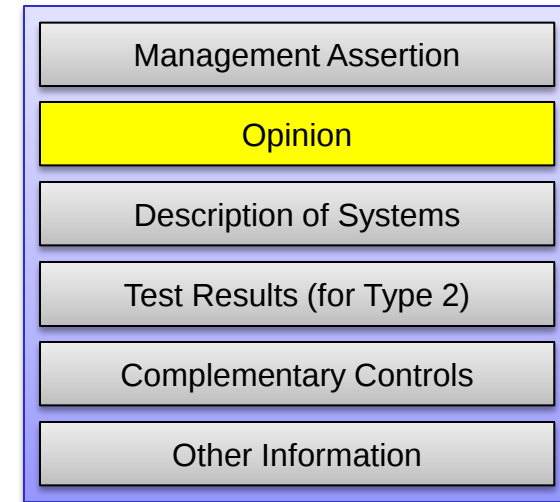
- A reference to management's assertion
- Description of tests of controls that were performed
- Service auditor's opinion on:
 - Fairness of management's description of systems
 - Controls were suitably designed
 - Operating effectiveness of controls tested (Type 2 only)

- **The Type 1 Opinion covers:**

- Design of controls, as of a single point-in-time

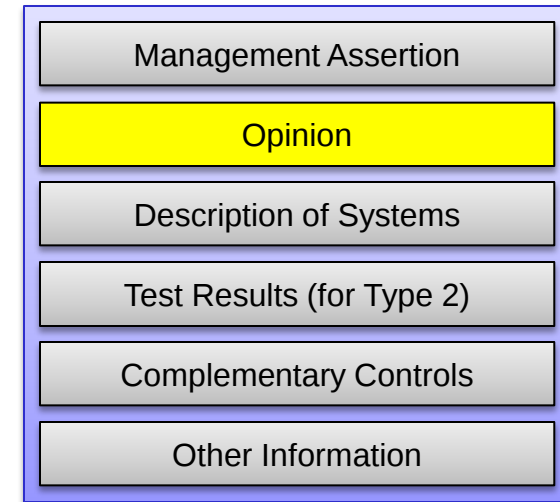
- **The Type 2 Opinion covers:**

- Operating effectiveness over the entire reporting period
- Suitability of the control design over the entire reporting period *
- The fair presentation of the system implemented over the entire reporting period *
- * these are different from the SAS 70 standard



Reviewing the opinion

- **What to look for when reviewing the opinion:**
 - Is the report's scope appropriate?
 - Is the time period covered appropriate?
 - Is it qualified or unqualified?
 - Is it a Type 1 or Type 2?
 - Is the opinion inclusive or does it contain a carve-out?
- **If the opinion is qualified ("except for")**
 - Why is it qualified? What control objective(s) failed?
 - How significant is the failure?
 - Consider potential impact (if any) on financial reporting
- **If there's a sub-servicer carve-out**
 - Service auditor expresses no opinion over controls of sub-servicers
 - Consider the significance of what is being carved out



Key Point: Type 1 Report vs Type 2 Report

Assertion/Opinion	Type 1	Type 2
Fair presentation of management's description of the system	Point in time	Entire period
Suitability of the design	Point in time	Entire period
Operating effectiveness of controls	N/A – not included in a Type 1	Entire period

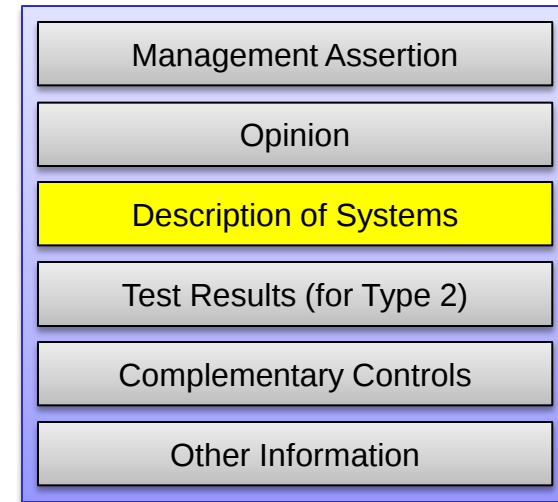
Description of Systems

- **What's in the description**

- Description of management's systems
- List of control objectives specified by management
- List of individual controls that support each objective
- ... *all of the above are provided by management*

- **What to consider when reviewing this section:**

- Is the description adequate?
- Are the control objectives adequate?
- *Consider: If this service or application were being run in house, what kinds of controls would your organization have in place? Then, Does the service organization have them?*



Results of Testing (Type 2 Only)

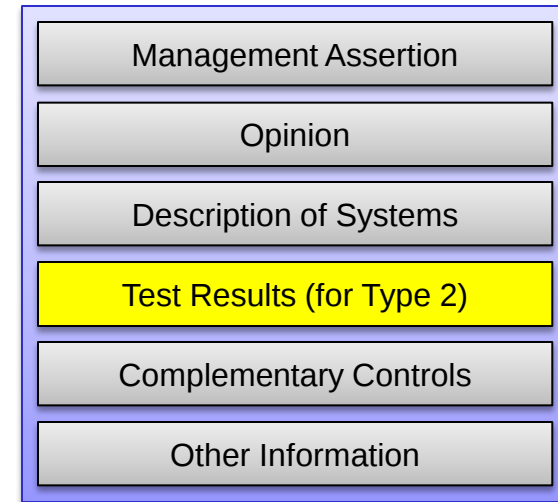
■ What's in this section:

- Lists of control tests that the service auditor performed
- Results of service auditor's testing of each control
- ... *all of the above provided by the service auditor*

■ What to consider when reviewing this section:

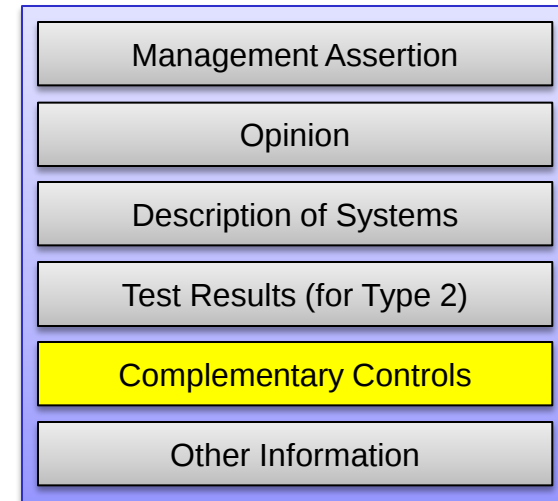
- Adequacy of control objectives being tested
- Test exceptions or errors (if any)
- Consider the impact of any exceptions or errors

- **Note:** As with previous SAS 70 Type 2 reports, you may see differences in terminology among CPA firms, some may title this section "Control Objectives and Related Controls", some may call it "Tests of Operating Effectiveness" section of the report.

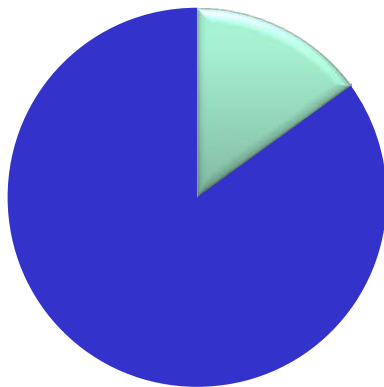


Complimentary User Entity Controls Considerations

- **Complimentary user entity controls are essential!**
- Identify the controls that apply to your organization
 - The scope of the report may cover multiple services
 - The report may cover multiple business units
 - Hosted applications may have multiple modules



Control Environment



- User Entity
- Service Org

The control environment is not complete without implementation of applicable complimentary controls

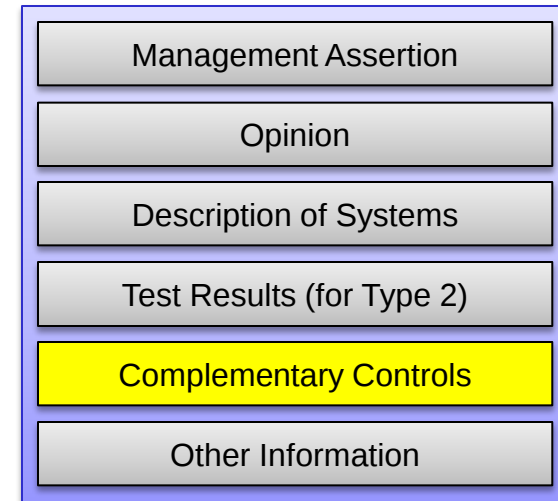
Reviewing the Complementary Control Considerations

- **For any listed controls that you have implemented:**

- Consider the design of your controls
- Consider the operating effectiveness of the controls
 - When were the controls last tested?
 - Who did the testing?
 - Were the results satisfactory?
 - If not, has remediation & re-testing been performed?

- **For any controls that you have NOT implemented:**

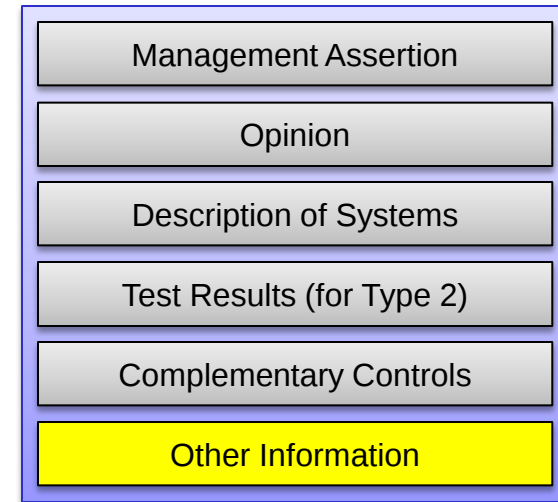
- Document the reason for non-implementation.
- Consider the risk of not implementing the control?
- Are there other/stronger controls that mitigate the risk?



Key Point: The control objectives specified in the SSAE 16 can only be achieved if the specified complementary user entity controls are suitably designed, implemented and operating effectively by the user entity (a/k/a you, the user of the service)

Other Information

- This information is provided by management
- It is not part of the description of systems
- Examples of Other Information
 - “Forward looking” information
 - Business Continuity & Disaster Recovery Plans
 - Discussion of future service enhancements
 - Planned infrastructure upgrades
- The service auditor is only required to read for material inconsistencies



 **Key Point:** This section is unaudited by service auditor

SOC Reports – Which Report Should You Request?

Criteria	Report to Use
Are you & your auditors using the report to plan and perform an audit or integrated audit of your financial statements?	SOC 1
Will the report be used by you as part of your compliance with the Sarbanes-Oxley Act or similar law or regulation?	SOC 1
Will the report only be used by you to gain confidence and place trust in your service organization's systems?	SOC 2 or 3, or AT 101, AT 601
Do you have the need for and ability to understand the details of the processing and controls at the service organization, the tests performed by the service auditor and results of those tests?	If Yes - SOC 2 or AT 101 or AT 601 If No, SOC 3
Do you need the report to be generally available and not restricted use?	SOC 3

* Courtesy of AICPA

For more information, contact:

Sue Horn, CISA, CPA

Manager

Crowe Horwath LLP

Office: 614.365.2236

e-mail: sue.horn@crowehorwath.com

Crowe Horwath LLP is an independent member of Crowe Horwath International, a Swiss verein. Each member firm of Crowe Horwath International is a separate and independent legal entity. Crowe Horwath LLP and its affiliates are not responsible or liable for any acts or omissions of Crowe Horwath International or any other member of Crowe Horwath International and specifically disclaim any and all responsibility or liability for acts or omissions of Crowe Horwath International or any other Crowe Horwath International member. Accountancy services in Kansas and North Carolina are rendered by Crowe Chizek LLP, which is not a member of Crowe Horwath International. This material is for informational purposes only and should not be construed as financial or legal advice. Please seek guidance specific to your organization from qualified advisers in your jurisdiction. © 2011 Crowe Horwath LLP