



INSIGHT ■ INNOVATION ■ EXPERIENCE

Reports on Service Organizations

Where we've been ?

Where we're going?

How do we get there?

Eric M. Wright
Shareholder

Schneider Downs & Co., Inc.
March 10, 2011



Overview

- Where we've been?
 - **History of SAS 70**
- Why Change?
 - **Times have changed**
- Where we're going?
 - **SSAE 16**
- How do we get there?
 - **Practical tips**

Schneider Downs

Agenda

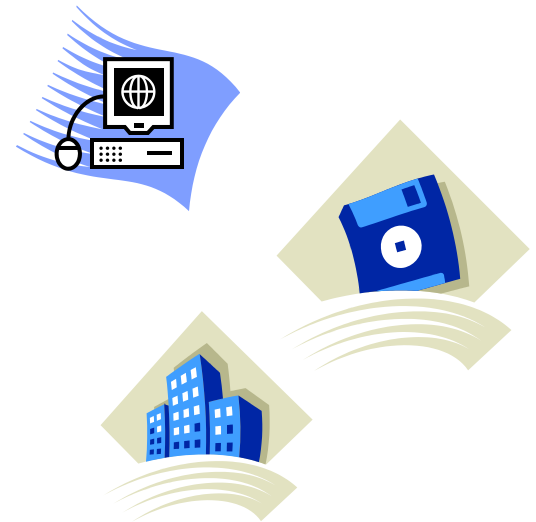
- Overview of Service Organizations
- Overview of User Organizations
- Background of SAS 70 and why need for change
- Similarities of SAS 70 and SSAE 16
- Key Differences SAS 70 and SSAE 16
- Alternatives to SSAE 16 report (AT Section 101 Attest Engagements)
- How to prepare for SAS 70 / SSAE 16 Audit
- Summary
- Questions

Service Organizations

Service Organization – provider of services that may impact a user’s (client’s) financial reporting

Such as:

- data centers
- transaction/claims processing centers
- application service providers
- bank processing centers
- Payroll processors



“Service auditor” issues an opinion on a service organization's description of controls

User Organizations

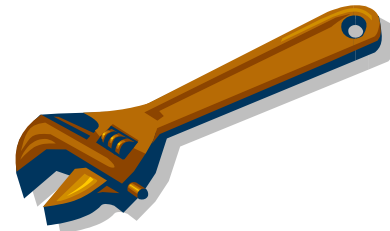
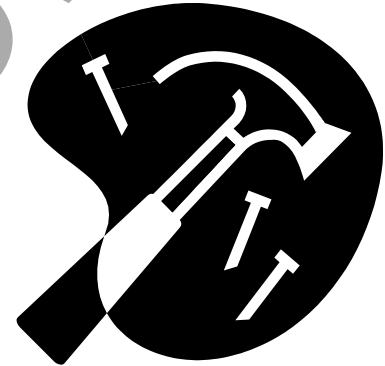
- **Users** are clients or customers of the service organization which have out sourced one or more business process to the service organization
- **“User Auditor”** is auditing the financial statements of the company who has contracted with the service organization

Where have we been ?

- *Statement on Auditing Standards No. 70* (SAS 70) issued in the early 90s
- Purpose – Provide assurance to users regarding Service Organization's controls and to deter the repetitive audits that service organizations had to endure

Why change was needed ?

- Key Factors:
 - Globalization
 - Growth in Outsourcing
 - New Technologies
 - Sarbanes– Oxley Section 404



Where are we going?

- Replacement for SAS 70
- New Standards for Reporting on Controls at a Service Organization Reporting
 - Align with the International Standards on Attestation Engagements (ISAE 3402)
 - Statement on Standards for Attestation Engagements (SSAE 16) or SOC 1
- Creation of two other reports SOC 2 and SOC 3
- Effective for Service auditor's reports for periods ending on or after June 15, 2011
- Early adoption is permitted.



Similarities

SSAE 16 continues the focus on the following:

- Controls likely to be relevant to their user entities' internal control over financial reporting (ICFR)
- SSAE 16 will have Type 1 and Type 2 reports similar in scope to the current SAS 70 reports
 - Type 1 – Design effectiveness
 - Type 2 – Design effectiveness and operating effectiveness
- Format of reports will NOT be significantly different

Similarities

- Narrative will still contain a description of controls
 - Basis for new narrative will need to include a description of the “system”
- Subservice organizations
 - Included (inclusive method)
 - Excluded (carve-out method)
- Restricted use – Intended users of the report
 - Service organization’s management
 - Users
 - User auditors

Similarities

- Auditor to Auditor Communication



- NOT a certification (SAS 70 or SSAE 16)

Key Differences: *SAS 70 vs. SSAE 16*

- Attest standard, not an audit standard
- Consistency with international standards and existing attestation standards
- Only focuses on service organizations with services relevant to a user organizations internal control over financial reporting (ICFR)
- **Services organizations whose services do not impact ICFR are governed by AT101 *Attest Engagements* for service organizations without ICFR relevance. AICPA has introduced two new reports to address those particular situations**

Key Differences: *Management Assertion*

A Management Assertion is required in all of the SOC reports

- Assertion will state the system is:
 - Fairly represented
 - Suitably designed and implemented
 - The related controls were suitably designed to achieve the stated control objective
 - That the controls operated effectively throughout the period covered by the report
- If inclusive method is used, management of the Subservice organization must provide a similar assertion

Key Differences: *Management Assertion*

The management assertion will also reference that management is responsible for:

- Preparing the system description
- Providing the stated services
- Specifying the control objectives
- Identifying the risks
- Selecting and stating the criteria for the assertion (e.g. monitoring activities)
- Designing, implementing and documenting controls that are suitably designed and operating effectively

Representations are similar to management rep letter issued to auditor

Key Differences: *System Description*

- Currently the narrative is a description of controls
- Management must prepare a written description of the system versus a description of controls
- More inclusive than it has been for many organizations and many CPA firms
- For inclusive subservice organizations, include
 - ✓ Related control objectives
 - ✓ Related controls activities

Key Differences: *System Description*

- Components common to existing Descriptions of Controls
 - Services covered
 - Period covered
 - Control objectives and related controls
 - User control considerations

Key Differences: *System Description*

- Criteria --Description of the system
 - Types of services and classes of transactions
 - Procedures (automated and manual)
 - Related accounting records
 - Significant events and conditions
 - Specified control objectives and controls activities implemented to achieve those objectives
 - Other relevant COSO components
 - control environment,
 - risk assessment,
 - information and communication,
 - control activities and monitoring
 - Changes to the service organization system during the period (in the case of Type 2 report)
 - Management's description does not omit or distort information while meeting common needs of a broad range of users

Key Differences: *Risks*

Management should include in system description:

- Identify the risks that threaten the achievement of the stated services
- Identify the risks that threaten the achievement of the stated control objectives
- Evaluate whether the identified controls sufficiently address the risks to achieving the control objectives



Other Key Differences

- Service auditor must disclose reliance on internal audit
- Service auditor opinion will change to conform with the new guidance

Schneider Downs

New Standards & Options

SERVICE ORG CONTROL 1 (SOC 1)	SERVICE ORG CONTROL 2 (SOC 2)	SERVICE ORG CONTROL 3 (SOC 3)
SSAE 16 – Service auditor guidance	AT 101	AT 101
Restricted Use Report (Type I or II report)	Generally a Restricted Use Report (Type I or II report)	General Use Report (with a public seal)
Purpose: Reports on controls for F/S audits	Purpose: Reports on controls related to compliance operations *	Purpose: Reports on controls related to compliance operations *

* Trust Services Principles and Criteria

AICPA Service Organization Control (SOC) Reports (formerly known as SAS 70 reports)

- **AICPA SOC 1** Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting
- **AICPA SOC 2** Report on Controls at a Service Organization that focuses on one or more of the following Trust Service principles: Security, Availability, Processing Integrity, Confidentiality and/or Privacy. Restricted use report.
- **AICPA SOC 3** Trust Services Report similar in scope to the SOC2, but the report does not contain a description of the auditors tests and results. General use report and can freely distributed or posted on a website as a seal.

SSAE 16(SOC 1) Focused on Financial Reporting

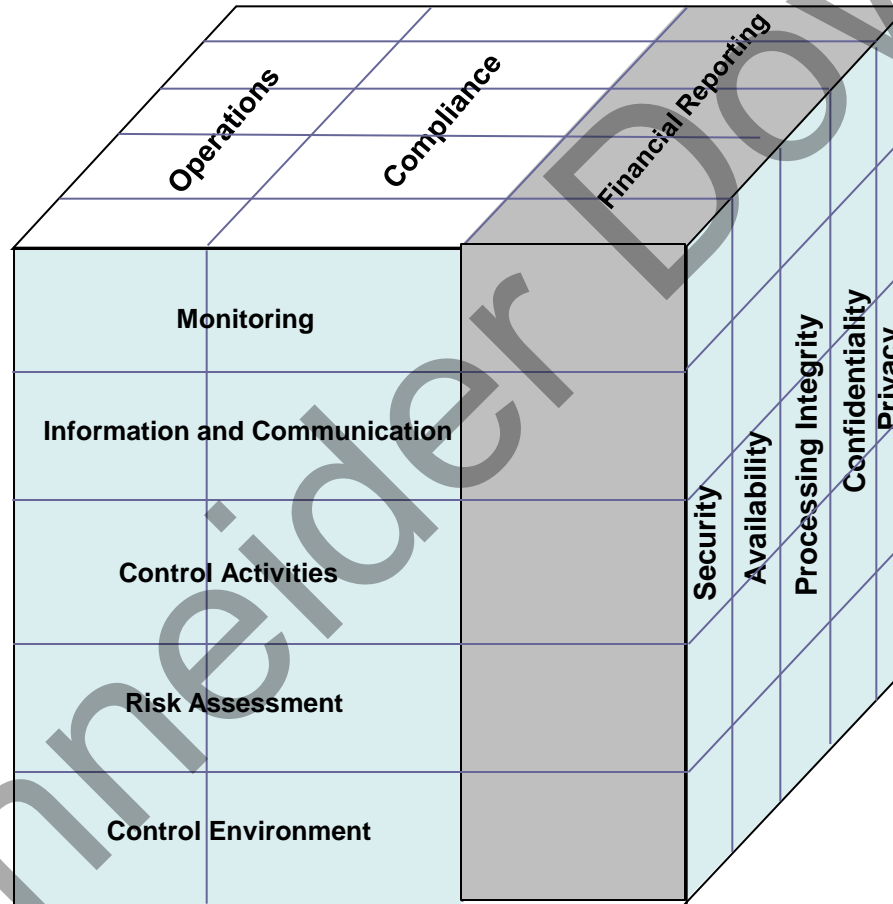
- SSAE 16 (like SAS 70) is focused on controls likely to be relevant to user entities' internal control over financial reporting
 - Intended for limited specific users
 - User auditors
 - User entities
 - Limited purpose
 - User entity financial audits
 - Examinations of internal control over financial reporting of user entities integrated with a financial audit
 - User entity evaluation of internal control over financial reporting (e.g., Sarbanes–Oxley Act compliance)
- Use beyond the intended purpose is likely to create misunderstanding
- Not intended to be a marketing document

Differences of SOC 2 & 3 with SSAE 16

- **Subject matter other than ICFR**
 - Trust Services Principles (Security, availability, processing integrity, confidentiality, privacy)
 - Boundary of the system
 - Driven by service provided
 - Broader than SSAE 16 (e.g., privacy—includes information life cycle, processing integrity—includes the purpose of the service other than financial transaction processing)
 - May relate to operations related to goods
- **Control objectives prescribed**
 - Reasonable in the circumstances
 - Provides comparability even though subject matter is highly flexible
- **Not intended to provide assurance on controls as they relate to user entity ICFR**

SOC Reports in context with select COSO Objectives and Components

COSO Framework



SSAE 16

Who Might use SOC 2 or SOC 3 reports?

- Cloud Computing / SaaS becoming very common.
- Service Organizations need assurance and reporting approach that represents effective internal control and meaningful reporting to users and other stakeholders.
- User Entities (and prospective users) need transparency of system providing services and assurance that relevant inherent risks are effectively mitigated.
- **No one-sized fits-all approach to risk management and assurance reporting**

How Clients Should Prepare For SAS 70/SSAE 16 Audit (Recurring)

1. Determine effective date and report period for your organization
2. Communicate with your users and re-evaluate the user needs and the user auditor needs
3. Discuss reporting guidance with auditor and revise nature and content of report as necessary (SOC 1, SOC 2, SOC 3)
4. Review scope and impact subservice organizations will have on report and new guidance (carve out or inclusive)
5. Review any new customer contractual agreements and impact on report
6. Create project plan and assign responsibilities
7. Review System description (services, scope, third parties, risks, control objectives, control activities, testing strategy)
8. Update narrative Section II to include system of controls including COSO type framework on control environment, risk assessment, etc.
9. Educate management on the additional disclosure responsibilities related to management assertions
10. Proactive communication with process owners, auditors, users,

How Clients Should Prepare For SAS 70/SSAE 16 Audit (First Year Implementation)

1. Determine who the user organizations are
2. Determine what controls are relevant to or required by user organizations
3. Identify risks (What could go wrong?)
4. Establish testing locations and parameters
5. Identify internal control objectives and activities
6. Determine the proper length of the testing period (match with user auditor needs - nonprofits 6/30, vs 12/31 year ends)
7. Ensure there is proper evidence to support that controls to be tested should be retained
8. Sometimes, system changes to retain evidence will affect the performance of your system.
9. Control environment should be assessed for sustainability
10. Changes in processes, systems and the control environment must be considered and incorporated into the description of controls.

How Clients Should Prepare For SAS 70 / SSAE 16 Audit (First Year)(cont.)

Additional procedures that service organizations should consider when preparing for a SAS 70 audit include:

- **Conducting a self assessment** or readiness assessment to determine whether controls are in place and properly designed. Readiness assessments can help identify opportunities for control optimization and for improvement opportunities to processes and controls. They can also facilitate evaluation of documentation maintained to support operation of controls.
- Appointing one or two (one operational and one IT) service organization personnel as **project managers** to facilitate coordination of the SAS 70 audit procedures and documentation requests
- Conducting **training of service organization employees** to communicate the importance of the SAS 70 audit, to set expectations for the audit, to build awareness of the SAS 70 audit requirements, and to support a control-minded culture

Common Mistakes/Best Practices

- During the walk-through or process identification stage, process owners interviewed are not accurate in describing the process.
 - Inaccurate narratives
 - Inaccurate testing plan
 - Results in duplication of effort as process is re-defined
- No accountability at the service organization to manage the process
 - Inefficient process for management and auditor
 - Need a proactive review of narrative and tests of controls each year to incorporate changes - fresh look
- Insufficient documentation to evidence the control exists or can be tested
 - Inconclusive testing
 - Removal of control from report, which could affect achievement of the control objective
- Have controls to capture data for entire period to ensure completeness of the populations used for testing
 - Inability to conclude on the full size of the population

Common Mistakes/Best Practices (Cont.)

- Lack of ownership as to who will write or prepare Section II of the report
 - Report delays/missed deadlines
 - Poorly written narratives not aligned with control objectives (and system description as required by SSAE 16)
- Report flow of Section II narrative is not cohesive or not aligned with Section III
 - Controls described in narrative not included or tested in Section III
 - Controls listed and tested within Section III not described in narrative
 - SSAE 16 will help to rectify this potential mistake

Summary Conclusion

- SSAE 16 (SOC 1 Report) replaces SAS 70 (June 2011)
 - reports impacting User ICFR
- Requires Management Representation in Report
- Narratives beefed up to describe system (COSO)
- Audit opinion covers period – not an “as of” date
- Alternative Reports Attestation Engagements
 - SOC 2 – Non ICFR – restricted use
 - SOC 3 – Non ICFR – general use

Questions – Contact information

- **Questions / comments**

- For more information on Reports on Service Organizations visit www.schneiderdowns.com or contact the following:
 - Steven D. Thompson – Assurance and Advisory Shareholder
Sthompson@schneiderdowns.com
 - Eric Wright – Technology Advisory Services Shareholder
Ewright@schneiderdowns.com
 - Michael Renzelman – Assurance and Advisory Shareholder
Mrenzelman@schneiderdowns.com