



**Preparing for the New  
Service Organization  
Control Standards**

**SOC 1 (SSAE 16), SOC 2,  
and SOC 3**

**March 18, 2011**

# AGENDA

- Update on the new SOC 1 (SSAE 16) standards
- Changes to service organization's responsibilities
- Changes to service auditor's responsibilities
- ISAE 3402
- Opportunity to revisit reporting alternatives
- Action steps for Service Organizations
- SOC 2 and SOC 3
- Questions and Answers
- Contact information

# UPDATE ON THE NEW SOC 1 (SSAE 16) STANDARDS

# SAS 70 Terminology

**Service Organization** - An entity that performs a specialized task or function for other entities

**Service Auditor** - The auditor of a Service Organization/Entity

**User Organization / Entity** - An entity that outsources a task to a Service Organization

**User Auditor** - The auditor of the User Entity / Organization

# SAS 70 – Current State

Current – Several standards for service organization reporting

- SAS 70, Section 5970, etc.
- SAS 70 Issued by AICPA in 1992
  - To reduce internal control testing of service providers by user auditor
  - Comply with contractual obligation
  - Comply with regulatory requirements
- Enabled auditors to report on:
  - Description of the outsourced process or function
  - Nature of service provided
  - How service is performed
  - Controls over service and related control objectives

# SAS 70 – Current State

## SAS70 Report Types

- SAS70 Type 1
  - Whether description is fairly presented, and
  - Whether controls are suitably designed.
- SAS70 Type 2
  - Whether description is fairly presented,
  - Whether controls are suitably designed, and
  - Whether controls were operating effectively over a period of time.

**SAS70 is an auditing standard and is intended to serve as auditor-to-auditor communication**

# Drivers for Change

- Drivers for change
  - Globalization of business process outsourcing
  - Need for common global standard - Alignment with International Standards on Attestation Engagements (ISAE 3402)
  - Need for increased emphasis on service organization rather than the auditor
  - New Technology – Virtualization, Mobile Computing, Cloud Computing
  - Clear common misunderstandings
    - Implementation of best practices
    - SAS 70 is a certification
  - Need for other reporting options (HIPAA, PCI, etc.)

# The Future

## Future – Two substantially equivalent standards that replace SAS 70

- Global – ISAE 3402, Assurance Reports on Controls at a Third Party Service Organization
- US – Service Organization Controls (SOC)
  - SOC 1 - Reporting on Controls at a Service Organization - SSAE No. 16 (Internal Controls over Financial Reporting)
  - SOC 2 – Reporting on Controls at a Service Organization – AT 101 (Non – Financial Reporting)
  - SOC 3 – Trust Services
- Timing
  - Effective for periods ending on or after June 15, 2011
  - AICPA's planned release of the SSAE 16 Audit Guide scheduled for June 2011

# Scope of SSAE 16

- Internal control over financial reporting
- Restricted Use: User Auditors and User Entities
- Limited purpose
  - User Entity financial audits
  - Examinations of internal control over financial reporting of User Entity integrated with a financial audit
  - User Entity evaluation of internal control over financial reporting (e.g., Sarbanes-Oxley Act compliance)
- Basically same Type 1 and Type 2 reports as SAS70

# CHANGES TO SERVICE ORGANIZATION'S RESPONSIBILITIES

Knowledge | Guidance | Compliance

A-align™

# Changes To Service Organization's Responsibilities

- Unchanged from current standards
  - Specifying the control objectives
  - Designing, implementing and maintaining controls
  - Complementary user organization controls
  - Control environment elements

# Changes To Service Organization's Responsibilities

## Changes in new standards

- Written assertion by management is required and must include the suitable criteria used for its assessment
- Audit report must include a written assertion by the subservice organization if inclusive method is used
- Description of systems / processes as opposed to description of controls
- Identifying risks that threaten the achievement of the control objectives
- For Type II reports, fair presentation of the system and suitability of design is for the period covered by the report.
- Subsequent events disclosure following the date of the service auditor's report

# Changes To Service Organization's Responsibilities

**Suitability of Fair Presentation Criteria:** Management has used suitable criteria for the fair presentation: *Description of the system should present how system was designed and implemented including:*

- Types of services provided and classes of transactions processed
- Procedures (automated and manual) for transaction flow
- Related accounting records
- How system captures and addresses significant events and conditions other than transactions
- Process used to prepare reports and other info for user entities
- Specified control objectives and controls and as applicable, complementary user org controls

# Changes To Service Organization's Responsibilities

## Suitability of Fair Presentation Criteria (Contd.):

Management has used suitable criteria for the fair presentation:

*Description of the system should present how system was designed and implemented including:*

- Other aspects of the service organization's control environment, risk assessment info control activities and assessment, and communication systems , activities, monitoring that are relevant to the services provided
- Provides details of changes to the service organization system during the period (in the case of Type 2 report)
- Does not omit or distort information relevant to the system, while meeting common needs of a broad range of user entity/user auditor needs.

# Changes To Service Organization's Responsibilities

**Suitability of Design Criteria:** *Controls are suitably designed to achieve the control objectives stated in management's description of the service organization system if:*

- Management has identified the risks that threaten the achievement of the stated control objectives.
- The controls would (if operating as described) provide reasonable assurance that those risks would be mitigated.

# Changes To Service Organization's Responsibilities

## Suitability of Operating Effectiveness Criteria:

Criteria should include at a minimum, whether:

- Controls were consistently applied as designed
- Throughout the specified period,
- Whether manual controls were applied by individuals having appropriate competence and authority

# CHANGES TO SERVICE AUDITOR'S RESPONSIBILITIES

Knowledge | Guidance | Compliance

A-align™

# Changes To Service Auditor's Responsibilities

- Unchanged from current standards
  - Opinion on fairness of management's description of the system (formerly controls)
  - Opinion as to suitability of the design and operating effectiveness of controls to achieve the control objectives
  - Perform tests of controls and present an opinion on operating effectiveness

# Changes To Service Auditor's Responsibilities

## Changes in new standards

- Standards move from audit standards to assurance/attestation standards
- For Type II reports, fair presentation of the system and suitability of design is for the period covered by the report
- Meant to improve clarity of guidance
- Suggested wording for control objectives
- Additional considerations on using the work of internal audit
- Requires description of the internal auditor's work
- Description of service auditor's procedures with respect to the work
- Opinion / Report Format

# Changes To Service Auditor's Responsibilities

## Fair Presentation Evidence

- Are all major aspects of the service provided that could reasonably be expected to be relevant to common needs of broad range of user auditors, included in the scope of the engagement?
- Are control objectives reasonable in circumstances – do they relate to assertions of financial statements for users that services could be expected to impact?
- Have all controls identified been implemented?
- Have complementary user entity controls, if any, been adequately described?
- Are services provided by sub-service org(s), if any, adequately described, including whether the inclusive or carve-out been used?

# Changes To Service Auditor's Responsibilities

## Suitability of Design Evidence

- Assess which of the controls at the service organization are necessary to achieve the control objectives.
- Identify risks that threaten the achievement of the control objectives.
- Evaluate the linkage between the controls defined in management's description and the identified risks.

# Changes To Service Auditor's Responsibilities

## Operating Effectiveness Criteria / Evidence

- Understand changes to system during the period
- Test controls necessary to achieve control objectives
- Perform other procedures in combination with inquiry to obtain evidence:
  - How the control was applied
  - Consistency of control application
  - By whom or what means control applied
- Determine whether control depends on other controls
- Determine effective method for selecting items to be tested; e.g., Audit Sampling

# Changes To Service Auditor's Responsibilities

## Materiality

- Was not included in SAS70
- With SSAE 16, need to consider whether there is a condition related to the control objectives, principles & criteria, or testing that would be considered “material” to the user of the report
  - Similar concept of materiality for a financial statement audit report
  - Would knowing this affect the decision of the user of the report?

# Changes To Service Auditor's Responsibilities

## Use of Internal Audit

- When planning the audit, determine whether work of Internal Audit is likely to be adequate
- To use the work from the Internal Audit function, evaluate and perform procedures on that work to determine its adequacy
- If Internal Audit work used in performing tests of controls (for Type 2 report), the description of tests should include
  - description of Internal Audit's work and
  - service auditor's procedures with respect to that work.

# ISAE 3402 INTRODUCTION

Knowledge | Guidance | Compliance

A-align™

# ISAE 3402 - Assurance Reports on Controls at a Service Organization

- Work began in March 2006 to develop the standard.
- ISAE would enhance the consistency of service auditor performance, and consequently the consistency of user auditor performance when a service auditor's report is used as audit evidence in an audit of financial statements.
- Need for substitute global standard rather than US SAS 70, for IFRS purposes
- Issued by the International Auditing and Assurance Standards Board in December 2009
- Effective for service organization's reports ending on or after Dec. 15, 2011
- Complements ISA 402 – Audit Considerations Relating to an Entity using a Service Organization

# Differences Between SSAE 16 And ISAE 3402

- Deviations can be treated as “anomalies,” and not testing exceptions, under certain circumstances.
- SSAE 16 requires an assessment of the risk and impact on deviations if they were intentional, while ISAE 3402 does not.
- Must disclose only events that take place after the period of the audit but before the date of the service auditor’s report

# Differences Between SSAE 16 And ISAE 3402

- Requires disclosure of subsequent events that have a significant effect on the report; however, SSAE 16 requires disclosure after the report has been issued, if they existed as of the report date.
- Users of the report are more clearly defined in the SSAE 16 than ISAE 3402.
- SSAE 16 permits the use of direct assistance of internal audit, while ISAE 3402 does not address it.
- SSAE 16 requires engagement documentation to be completed on a timely basis after the date of the report and no later than 60 days following the report release date.

# Differences Between SSAE 16 And ISAE 3402

- ISAE 3402 notes engagement documentation is to be completed timely, but does not specify a date.
- Engagement acceptance and continuance procedures require that the service organization's management acknowledge and accept responsibility for providing written representations to the service auditor under SSAE 16, while ISAE 3402 requires only written representations and not acknowledgement.
- If service organization management doesn't provide written representations, the service auditor must disclaim an opinion under ISAE 3402, while under SSAE 16 the service auditor may also withdraw from the engagement.

# OPPORTUNITY TO REVISIT REPORTING ALTERNATIVES

Knowledge | Guidance | Compliance

A-align™

# Opportunity To Revisit Reporting Alternatives

- New standards provide an opportunity to challenge the value and re-visit the scope of your current reporting and compliance obligations
- Suggested considerations
  - Comments currently received from clients regarding current reports
  - Does the current scope reflect the depth & breadth of operations?
  - On-site audits performed that potentially could be avoided
  - Additional regulations that could be partially addressed through service organization report (e.g., Gramm–Leach–Bliley Act)
  - Additional organization features and differentiators that could be better highlighted in reports (e.g., availability, new systems)
  - Adding Trust Services reports (WebTrust, SysTrust) or ISO 27001 / ISO 27002 certifications to service organization reporting process

# ACTION STEPS FOR SERVICE ORGANIZATIONS

Knowledge | Guidance | Compliance

A-align™

# Action Steps For Service Organizations

- Review and modify your client contracts
  - Contracts that specifically require a SAS 70
  - Other changes needed to address change in the standards (for example wording of control objectives)
- Educate your customers / personnel regarding the change
  - Identify communication channels
  - Inform personnel on changes and organization's approach to enable informed discussions with clients/prospective clients
- Benchmark current description of controls to identify any modifications

# Action Steps For Service Organizations (Contd.)

- Consider alternatives that could enhance value of reporting (see prior page)
- Perform a risk assessment and benchmark to current control objectives
- Monitor the operational effectiveness of control activities
  - Supervisory review of controls
  - Oversight by management
  - Quality assurance monitoring
  - Standardized management reporting
  - Internal audit testing
- Proactively communicate with service auditor on proposed approaches/changes

# SOC 2 and SOC 3

# Historic Perspective



# New Standards

SERVICE ORG CONTROL 1 (SOC 1)	SERVICE ORG CONTROL 2 (SOC 2)	SERVICE ORG CONTROL 3 (SOC 3)
SSAE16 - 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 or operations	Purpose: Reports on controls related to compliance or operations
	Trust Services Principles & Criteria*	

# SOC 2

## Overview

- Many entities outsource tasks or entire functions to service organizations that operate, collect, process, transmit, store, organize, maintain, and dispose of information for user entities.

## Scope and Use

- Predefined criteria: Trust Services Principles, Criteria, & Illustrations
- Requirements and guidance in AT Section 101
- Restricted Use:
- Unlike SSAE No. 16, the primary users of SOC 2 reports generally are not user auditors, they are management of the service organization and management of the user entities.
- Type 1 or type 2 report may be issued

# SOC 2

Five attributes of a system are known as principles and are defined as follows:

- **Security** - The system is protected against unauthorized access (both physical and logical).
- **Availability** - The system is available for operation and use as committed or agreed.
- **Processing integrity** - System processing is complete, accurate, timely, and authorized.
- **Confidentiality** - Information designated as confidential is protected as committed or agreed.
- **Privacy** - Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy notice and with criteria set forth in GAPP

# SOC 2 - Scoping

## Selecting the right principle(s)

- Scope of services delivered
- User entity inherent risk, expectations and needs for compliance/ operational controls
- Service organization needs for internal controls
- Security pervasiveness – are security considerations in confidentiality and availability adequate
- Do the criteria for one or more principles align to the control needs of the service organization

# Performing An SOC 2 Engagement

- Description of the System is Fairly Presented, Controls Have Been Implemented and Suitability of the Design of Controls
- Materiality Relating to the Fair Presentation of the Description
- Complementary User Entity Controls
- Subservice Organizations
- Operating Effectiveness of Controls in a Type 2 Engagement
- Tests of Controls (Type II)
- Testing Compliance With Privacy Commitments
- Using the Work of the Internal Audit Function and Effect on the Service Auditor's Report
- Written Representation of Management's Assertion

# SOC 3

## **SOC 3 is SysTrust for Service Organizations.**

### Use

Distribute the SOC 3 report to customers and publicly display a seal of approval using the SOC 3 Report: SysTrust seal.

### Scope

SOC 3 reports can be issued on one or multiple Trust Services principles (security, availability, processing integrity confidentiality, and privacy).

# So Which Report Is Appropriate?

## Intended users of the report

- If the focus is on internal control over financial reporting - then an SOC 1 (SSAE 16) report may be most appropriate.
- If focus is on compliance & operational controls - then a SOC 2 or SOC 3 report may be most appropriate.

## Understand the best communication mechanism for your users

- If the users of the report need detail about the systems and processes – then an SOC 1 or SOC 2 report may be most appropriate.
- If summary information will suffice - then a SOC 3 report may be most appropriate.

# AICPA Resources

- Online source center: [www.aicpa.org/SOC](http://www.aicpa.org/SOC) and [www.aicpa.org/infotech](http://www.aicpa.org/infotech)
- Online [brochure](#) to provide an introduction to the concept of Service Organization Control (SOC) reports.
- [AICPA Alert](#): Service Organizations: New Reporting Options—2010/11 (NEW - IT Section members receive 10% off the purchase starting 01/11/11!)
- SSAE 16 Publication: [http://www.cpa2biz.com/AST/Main/CPA2BIZ\\_Primary/AuditAttest/Standards/SSAEs/PRDOVR~PC-023035/PC-023035.jsp](http://www.cpa2biz.com/AST/Main/CPA2BIZ_Primary/AuditAttest/Standards/SSAEs/PRDOVR~PC-023035/PC-023035.jsp)
- Two Service Organization Control (SOC) guides are under development

# QUESTIONS AND ANSWERS

Knowledge | Guidance | Compliance

A-align™

# Contact Information

Neil Gonsalves

Director

A-align CPAs, LLC

[neil.gonsalves@aligncpa.com](mailto:neil.gonsalves@aligncpa.com)

1.888.702.5446 X104