



cutting through complexity™

Service Organization Control Reporting

The standard setter's
perspective

Dave Palmer
Managing Director
KPMG LLP

July 14, 2011

Agenda

- SAS 70 – The migration to a new standard
- SSAE 16 – How does it compare to SAS 70
- The AICPA's vision for Service Organization Control Reporting

SAS 70 – The migration to a new standard

Migration to a new standard

- Service auditor reporting has evolved over a 40+ year period
- SAS 70 became a de facto global standard
- SAS 70 is viewed as a generic term
- However, SAS 70 reports were being used in ways for which they were never intended

SAS 70 Heavily Marketed as a “Certification” or “Compliance Report”



What do the analysts say?

**Gartner says “SAS 70 is not proof of security, continuity or privacy compliance”
(July 14, 2010)**

Migration to a new standard

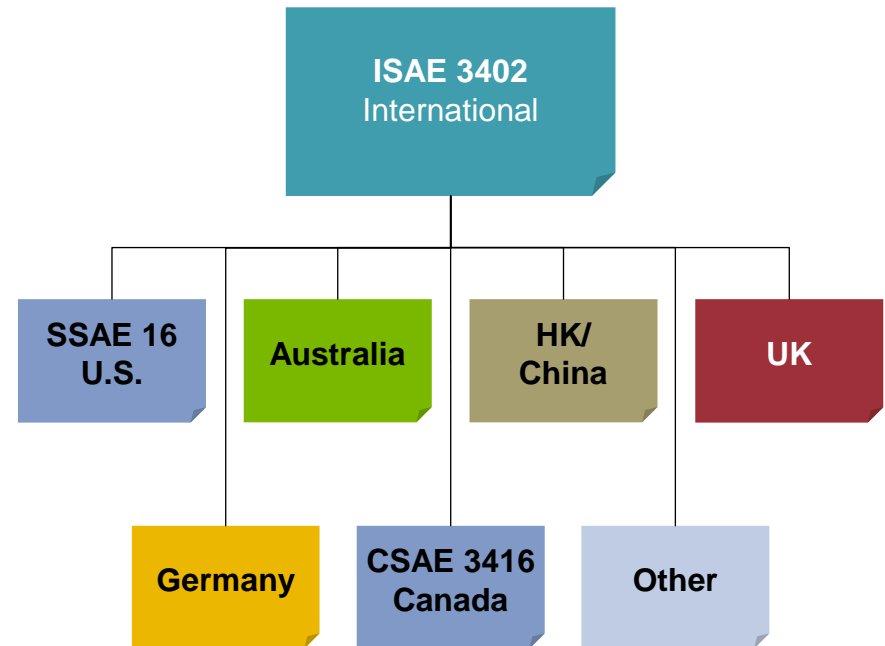
- General convergence of U.S. and International Standards
- The IAASB included service auditor reporting on its agenda in 2008, resulting in the development of an international standard:
- The U.S. Auditing Standards Board agreed to conform to the IAASB approach
- IAASB has approved International Standard on Assurance Engagements (ISAE) No. 3402
 - U.S.: SSAE 16
 - Canada: CSAE 3416
- New standard is effective for reports covering periods ending on or after June 15, 2011 (Dec 15 for Canadian standard)
- Supersedes SAS 70

What is changing?

Historically....



Now...



SSAE 16 – How does it compare to SAS 70

What's staying the same?

- Purpose and intended use of the report
 - Primary purpose – provide information to the user entities financial statement auditors
 - Focus is on controls at service organizations that are likely to be relevant to user entities' internal control over financial reporting
 - Intended for use by:
 - Management of the service organization
 - Entities that used the service organization during the period (user entities) – includes indirect or downstream users
 - Financial Statement auditors of those user entities

What's staying the same?

- Core elements of the report
 - Auditor's Opinion
 - Management Description
 - Detailed Tests of Controls (Type 2 reports)
 - Other Relevant Information
- Service Auditor's Opinion
 - Fair presentation of the description of the service organization's system
 - Suitability of the design of the service organization's controls relative to the control objectives
 - For type 2 engagements, operating effectiveness of the service organization's controls relative to the control objectives
- Options for handling subservice organizations

What's changing?

- Audit Standard vs. Attestation Standard
- Significant Terminology changes
 - No longer a “SAS 70” report
 - SSAE 16
 - Service Organization Control (SOC 1) Report
 - Service Organization’s “System”
 - Uses a broad definition of system
 - Includes policies and procedures designed, implemented and documented to provide a service to user entities
 - Criteria
 - Standards or benchmarks to present the subject matter and against which the practitioner evaluates the subject matter

What's changing?

- New performance and reporting requirements
 - Assess the suitability of the criteria used by management
 - Understand the relevance of Internal Audit work to the engagement
 - Disclose the use of work performed by Internal Audit
- New requirements impacting management
 - Management must provide a written assertion for inclusion on the report
 - Management must include the criteria used in making these assertions
 - Management must have a reasonable basis for its assertion

Management's assertion

A written assertion about whether in all material respects, and based on suitable criteria that:

- The description fairly presents the system that was designed and implemented throughout the period
- Controls were suitably designed throughout the period to achieve the control objectives
- Those controls operated effectively throughout the period to achieve the control objectives

Minimum criteria

- The standard defines the minimum criteria that should be used by Management and the Auditor for evaluating:
 - Fairness of presentation relative to the description of the system
 - Suitability of the design of controls
 - Operating effectiveness

Reasonable basis

In order to have a reasonable basis for its assertion, management should:

- Understand the criteria that should be used to make the assertion
 - **Fairness** – Does the description address all of the required elements?
 - **Design** – Do we understand the risks and have we identified the key controls that mitigate those risks?
 - **Operating effectiveness** – Do we know that those key controls were operating with sufficient effectiveness to achieve the control objectives?

What's changing?

- Changes impacting the report
 - Use of Internal Audit must be disclosed
 - The Service Auditor's Report
 - Expanded wording on management's responsibilities
 - Opinion on fairness of presentation and design in a type 2 report will now cover the entire period
 - One opinion addressing all three elements
 - Intended users

The AICPA's vision for service organization control reporting



“Service Organization Controls (SOC) reports are designed to help service organizations build trust and confidence in their service delivery processes and controls through a report by an independent Certified Public Accountant.”

AICPA Branding

- The AICPA has outlined 3 types of SOC reports that Each type of SOC report is designed to help service organizations meet specific user needs:
 - **SOC 1 Report** – *Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting*
 - **SOC 2 Report** – *Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy*
 - **SOC 3 Report** – *Trust Services Report for Service Organizations*

SOC 1, SOC 2, SOC 3 and Service Organization Control Reporting are registered service marks of the American Institute of Certified Public Accountants (AICPA).

SOC 1

- Remains focused on internal controls related to financial reporting (ICFR)

SOC 2

- Structured similar to SSAE 16
- Trust services principles and criteria
- Cloud computing reporting
- Non-ICFR


SOC 3

- Trust services principles and criteria
- SysTrust & WebTrust reporting
- Non-branded reports
- Non-ICFR

**SSAE 16/
ISAE 3402**

AT 101

SOC Review – Service Organization Control Reports

Report	Scope/Focus	Summary	Applicability
SOC1	Internal Control Over Financial Reporting	Detailed report for customers and their auditors	<ul style="list-style-type: none"> ■ Focused on financial reporting risks and controls specified by the service provider. ■ Applicable where the service provider performs financial transaction processing or supports transaction processing systems.
SOC2	Security, Availability, Processing Integrity, Confidentiality and/or Privacy	Detailed report for customers and specified parties	<ul style="list-style-type: none"> ■ Focused on Security, Confidentiality, Availability, Processing Integrity and/or Privacy. ■ Applicable to a broad variety of systems.
SOC3	Same as SOC2 	Short report that can be generally distributed, with the option of displaying a web site seal	<ul style="list-style-type: none"> ■ Same as above without disclosing detailed controls and testing. ■ Optionally, the service provider can post a Seal if it receives an unqualified opinion.

Note: The traditional SAS 70 construct of a Type 1 (point in time design-focused) and a Type 2 (period of time effectiveness-focused) report also applies to SOC 1, 2 and 3 reports (point in time for initial report).

Overview of Trust Services Principles

Domain	Principle
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.
Confidentiality	■ Information designated as confidential is protected as committed or agreed.
Processing Integrity	■ System processing is complete, accurate, timely, and authorized.
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 generally accepted privacy principles (GAPP) issued by the AICPA and CICA.

Use of SOC Reports – Summary of SOC2/3 Criteria Topics

Security	Availability	Confidentiality	Processing Integrity	Privacy
<ul style="list-style-type: none"> ■ IT security policy ■ Security awareness and communication ■ Risk assessment ■ Logical access ■ Physical access ■ Environmental controls ■ Security monitoring ■ User authentication ■ Incident management ■ Asset classification / mgt. ■ Systems development and maintenance ■ Personnel security ■ Configuration mgt. ■ Change management ■ Monitoring / compliance 	<ul style="list-style-type: none"> ■ Availability policy ■ Backup and restoration ■ Disaster recovery ■ Business continuity management 	<ul style="list-style-type: none"> ■ Confidentiality policy ■ Confidentiality of inputs ■ Confidentiality of data processing ■ Confidentiality of outputs ■ Information disclosures (including third parties) ■ Confidentiality of Information in systems development 	<ul style="list-style-type: none"> ■ System processing integrity policies ■ Completeness, accuracy, timeliness, and authorization of inputs, system processing, and outputs ■ Information tracing from source to disposition 	<ul style="list-style-type: none"> ■ Management ■ Notice ■ Choice and consent ■ Collection ■ Use and retention ■ Access ■ Disclosure to third parties ■ Quality ■ Monitoring and enforcement

Grouping of Criteria

Topic	Focus of Criteria
Policies	■ Policies relevant to the selected principle(s) are defined and documented.
Communications	■ Defined policies are communicated to responsible parties and authorized users of the system.
Procedures	■ Procedures have been placed in operation to achieve the service provider's objectives in accordance with its defined policies.
Monitoring	■ The service provider monitors the system and takes action to maintain compliance with its defined policies.

Comparison of Reports

Traditional SAS 70	SOC 1	SOC 2	SOC 3
Auditor's Opinion	Auditor's Opinion	Auditor's Opinion	Auditor's Opinion
—	Management Assertion	Management Assertion	Management Assertion
Detailed description of the system including control objectives and related controls	Detailed description of the system including control objectives and related controls	Detailed description of the system including controls to address the criteria	Summary description of the system including controls to address the criteria
Tests of operating effectiveness / results of testing	Tests of operating effectiveness / results of testing	Tests of operating effectiveness / results of testing	—
Restricted use	Restricted use	Restricted use	Unrestricted use and ability to display seal on a website

Questions?

Presenters' Contact Details

Dave Palmer
Managing Director, KPMG LLP

+1 312 665 1354

davepalmer@kpmg.com

Thank you



cutting through complexity™

© 2011 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

The KPMG name, logo and “cutting through complexity” are registered trademarks or trademarks of KPMG International.