



cutting through complexity™

The Retirement of SAS 70: A New Breed of Service Organization Control (SOC) Reports

ISACA San Francisco Chapter

March 2011

San Francisco

June 15, 2011

SAS 70 Exists No More

With the retirement of the SAS 70 standard, traditional SAS 70 reports are being replaced by Service Organization Control Reports (or SOC reports.) In the past, the SAS 70 report was intended to assist service organizations' customers and their auditors in the

context of a financial statement audit. Now, three types of SOC reports have been defined to replace SAS 70 and help service organizations meet a broader set of specific user needs such as addressing the security and availability concerns related to the cloud.

Ren
follo
imp
The
that
rela
the
beh
of a
exp
in li



Agenda

- Service Organization Control (SOC) Reports
- SOC1
- SOC2 and SOC3
- Using SOC Reports
- Q&A

Service Organization Control (SOC) 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. • Most applicable when 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"> • Pre-defined security criteria form the baseline. • Can also include Confidentiality, Availability, Processing Integrity and/or Privacy criteria. • Financial reporting is not the primary concern.
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 they receive an unqualified opinion.

Note: The traditional SAS 70 concept 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).

SOC1

SOC1 Background

- SAS 70 and its predecessors have been in place for 40 years
- Post-SOX, SAS 70 became a de facto global standard
- New standards developed to serve global user base:
 - ISAE 3402 developed by International Auditing and Assurance Standards Board (IAASB)
 - SSAE 16 developed by AICPA based on ISAE 3402
- SAS 70 superseded for periods ending after 6/15/11
- New attestation standard for service organizations, audit standard for users

SOC1 Similarities

- Underlying work effort expected to be substantially the same as SAS 70
- Two types of reports (Type I or Type II)
- Type II reports should cover a minimum of six months
- Restriction on use – remains the same
 - Intended for customers and their auditors when assessing the risks of material misstatements of user entities' financial statements
- Service auditor's tests included in report
- Sample sizes disclosed only when exceptions are identified

Key SOC1 Differences

- Management assertion required
- Criteria established to support management assertion
- Reasonable basis for management assertion
- Type 2 opinion now covers period of time for the description and design, as well as for effectiveness.

Criteria – Fair Presentation of Description

- Description presents how the system was designed and implemented to process relevant transactions, including:
 - Classes of transactions processed
 - Automated and manual procedures for processing and reporting transactions
 - Related accounting records of the system
 - How the system captures and addresses significant events and conditions, other than transactions
 - Process to prepare reports provided to users
 - Control objectives and controls designed to achieve those objectives
 - Other aspects that are relevant to processing and reporting transactions of users
- Description does not omit or distort information relevant to the scope
- Description includes relevant details of changes to the service organization's system during the period

Criteria – Design and Operating Effectiveness

- The risks that threaten the achievement of the control objectives stated in the description have been identified by the service organization.
- The controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.
- The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

SOC2

and

SOC3

SOC2/SOC3 Background

- There is a large market need for SAS 70-style reports for services with limited or no relevance to financial reporting.
- SOC1 has been designed to be laser-focused on controls that could impact users' financial reporting.
- SOC2 has been developed to have the look and feel of a SOC1 report but using criteria that are more broadly applicable.
- SOC2 leverages the Trust Services principles and criteria that support SysTrust and WebTrust reporting.
- Final SOC2 guidance expected to be published in April.
- SOC3 is a short form report like a traditional SysTrust report.

SOC2/SOC3 – Components of the System

- **Infrastructure.** The physical and hardware components of a system (facilities, equipment, and networks)
- **Software.** The programs and operating software of a system (systems, applications, and utilities)
- **People.** The personnel involved in the operation and use of a system (developers, operators, users, and managers)
- **Procedures.** The automated and manual procedures involved in the operation of a system
- **Data.** The information used and supported by a system (transaction streams, files, databases, and tables)

Layers of Activity Covered by a SOC2 or SOC3 Examination

Topic	Summary
Policies	<ul style="list-style-type: none">• Policies are defined and documented.
Communications	<ul style="list-style-type: none">• Defined policies are communicated to responsible parties and authorized users of the system.
Procedures	<ul style="list-style-type: none">• Procedures have been placed in operation to achieve the service provider's objectives in accordance with its defined policies.
Monitoring	<ul style="list-style-type: none">• The service provider monitors the system and takes action to maintain compliance with its defined policies.

SOC2/SOC3 Principles

Topic	Summary
Security	<ul style="list-style-type: none">• The system is protected against unauthorized access (both physical and logical).
Availability	<ul style="list-style-type: none">• The system is available for operation and use as committed or agreed.
Confidentiality	<ul style="list-style-type: none">• Information designated as confidential is protected as committed or agreed.
Processing Integrity	<ul style="list-style-type: none">• System processing is complete, accurate, timely, and authorized.
Privacy	<ul style="list-style-type: none">• 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.

Summary of SOC2/3 Criteria Topics

Security (Baseline Criteria)			
<ul style="list-style-type: none"> ■ IT security policy ■ Security awareness and communication ■ Risk assessment ■ Logical access 	<ul style="list-style-type: none"> ■ Physical access ■ Environmental controls ■ Security monitoring ■ User authentication 	<ul style="list-style-type: none"> ■ Incident management ■ Asset classification and management ■ Systems development and maintenance 	<ul style="list-style-type: none"> ■ Personnel security ■ Configuration management ■ Change management ■ Monitoring and compliance
Availability	Confidentiality	Processing Integrity	Privacy
<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

Cloud Service Provider (CSP) – Control Requirements

Information Security Management System

- **Security Policy**
- **Organization of Information Security**
- **Asset Management**
- **Human Resources Security**
- **Physical and Environmental Security**
- **Communications and Operations Management**
- **Access Control**
- **Information Systems Acquisition, Development, and Maintenance**
- **Information Security Incident Management**
- **Business Continuity Management**
- **Compliance**

Areas of Added Emphasis for CSPs

- **Data Protection/Segregation**
- **Privacy**
- **Encryption Standards**
- **Logging**
- **Authentication to the Cloud**
- **Configuration Management**
- **Monitoring/Compliance Function**

The SOC2 and SOC3 assurance framework can be used to demonstrate the effectiveness of the CSP's controls in these areas.

SOC Report Structure

Traditional SAS 70	SOC1	SOC2	SOC3
Auditor's opinion	Auditor's opinion	Auditor's opinion	Auditor's opinion
---	Management assertion	Management assertion	Management assertion
Description of system and controls	Description of system and controls	Description of system and controls	Description of system
Controls, tests of operating effectiveness and results of tests	Controls, tests of operating effectiveness and results of tests	Controls, tests of operating effectiveness and results of tests	---

Report Comparison

Traditional SAS 70 and SOC1			SOC2 (DRAFT)			
Control Objective 1: XXXXXXXX			Security Principle: The system is protected against authorized access (both physical and logical)			
			1.0 Policies: the entity defines and documents its policies for the security of its system.			
Control	Test Procedures	Results of Tests	Criteria	Control	Test Procedures	Results of Tests
XXXXX	<ul style="list-style-type: none"> • XXXXXX • XXXXXX 	XXXXX	XXXXX	XXXXX	<ul style="list-style-type: none"> • XXXXXX • XXXXXX 	XXXXX
XXXXX	<ul style="list-style-type: none"> • XXXXXX • XXXXXX 	XXXXX	XXXXX	XXXXX	<ul style="list-style-type: none"> • XXXXXX • XXXXXX 	XXXXX
...	<ul style="list-style-type: none"> •	<ul style="list-style-type: none"> •
Control Objective 2: XXXXXXXX			2.0 Communications: The entity communicates its defined system security polices to responsible parties and authorized users.			
Control	Test Procedures	Results of Tests	Criteria	Control	Test Procedures	Results of Tests
XXXXX	<ul style="list-style-type: none"> • XXXXXX • XXXXXX 	XXXXX	XXXXX	XXXXX	<ul style="list-style-type: none"> • XXXXXX • XXXXXX 	XXXXX
XXXXX	<ul style="list-style-type: none"> • XXXXXX • XXXXXX 	XXXXX	XXXXX	XXXXX	<ul style="list-style-type: none"> • XXXXXX • XXXXXX 	XXXXX
...	<ul style="list-style-type: none"> •	<ul style="list-style-type: none"> •
Control Objective 3: XXXXXXXX			3.0 Procedures: The entity uses procedures to achieve its documented system security objectives in accordance with its defined policies.			
Control	Test Procedures	Results of Tests	Criteria	Control	Test Procedures	Results of Tests
XXXXX	<ul style="list-style-type: none"> • XXXXXX • XXXXXX 	XXXXX	XXXXX	XXXXX	<ul style="list-style-type: none"> • XXXXXX • XXXXXX 	XXXXX
XXXXX	<ul style="list-style-type: none"> • XXXXXX • XXXXXX 	XXXXX	XXXXX	XXXXX	<ul style="list-style-type: none"> • XXXXXX • XXXXXX 	XXXXX
...	<ul style="list-style-type: none"> •	<ul style="list-style-type: none"> •

Using SOC Reports

Case Studies

SOC1 Financial Reporting Controls		SOC2/SOC3 Operational Controls				
Business Process Controls	IT General Controls	Security	Availability	Confidentiality	Processing Integrity	Privacy

- Financial services – custodial services
- Healthcare claims processing
- Payroll processing
- Payment processing
- Cloud ERP service
- Data center colocation
- IT systems management
- Enterprise cloud email
- SaaS-based HR/personnel services
- Security-as-a-service
- Cloud collaboration/ office productivity
- Consumer online entertainment content
- Social media

Key Considerations When Evaluating Assurance Reports

Topic	Considerations
Type of Report	<ul style="list-style-type: none"> • Is the report a SOC report or another type of report?
Period of Coverage	<ul style="list-style-type: none"> • Does the report provide coverage for a relevant period of time (e.g., 6 months or 12 months) or does it cover a point in time?
Opinion	<ul style="list-style-type: none"> • Does the report provide an examination/audit level of assurance? • Was the opinion unqualified or qualified?
Audit Firm	<ul style="list-style-type: none"> • Is the audit firm known as having qualifications in IT Attestation?
Scope	<ul style="list-style-type: none"> • Does the report cover all relevant aspects of the services provided to the client?
Subservice Organizations	<ul style="list-style-type: none"> • Are organizations that support the service included in scope or carved out? • If carved out, are audit reports available for the carved out entities?

Key Considerations When Evaluating Assurance Reports (continued)

Topic	Considerations
Control Criteria/ Objectives	<ul style="list-style-type: none"> • From a scoping perspective, does the audit report cover the relevant control objectives/principles and criteria?
Client Control Considerations	<ul style="list-style-type: none"> • Does the audit report highlight specific control activities for which the user is responsible?
Description of Control Activities	<ul style="list-style-type: none"> • Does the report describe the provider's key controls at a sufficient level of detail?
Test Procedures	<ul style="list-style-type: none"> • Does the report include the auditor's test procedures? • Are these procedures sufficiently detailed (e.g., including observation and inspection of detailed evidence and system configurations)?
Test Results	<ul style="list-style-type: none"> • Are test exceptions identified in the audit report? • What is the impact of such exceptions and what is the cloud provider's management response to any such exceptions?

Key Takeaways

- 2011 will be a year of transition.
 - SAS 70 goes away in 3 ½ months
 - Replaced by 3 types of Service Organization Control (SOC) reports
 - Varying levels of awareness
- Service providers and customers will need to determine what type of reports they require going forward
 - SOC1 if significant financial reporting impact
 - SOC2 or SOC3 if security, availability, privacy focus
 - Also need to determine which principles to cover for SOC2/SOC3

Key Takeaways

- Customers will need to prepare for the transition:
 - Revisit contractual audit provisions
 - Communicate with your service providers early
 - Build into due diligence / vendor management processes
- Service providers will need to prepare for the transition:
 - Determine which report(s) will best meet the needs of their customers and potential customers
 - Re-validate scope
 - Identify any areas not previously covered
 - Risk assessment
 - Monitoring controls / basis for assertion
 - Communication plan/FAQs for educating users on the new standards and the rationale for the service provider's approach

Q&A



Presenters' Contact Details

Mark Lundin

Partner

mlundin@kpmg.com

415-963-5493

Reema Anand

Manager

reemaanand@kpmg.com

650-404-4874

Thank you!



cutting through complexity™

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2011 KPMG LLP, a Delaware limited liability partnership and the U.S. 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 Cooperative ("KPMG International").