



P21 - Service Organization Control (SOC) Reports

Presenters: Reema Anand & Emily Fremming
2011 SF ISACA Fall Conference
November 8, 2011

Back to Business

Agenda


- **SOC Reports - Overview and Structure**
 - Service Organization Control (SOC) Reports
 - SOC1 Evolution
 - SOC1 Key Differences and Similarities
 - SOC2/SOC3 Principles and Criteria
 - Report Structure and Contrasts
 - SOC2 and SOC3 Key Differences
- **Using SOC Reports**
 - Spectrum of Services and SOC Report Scenarios
 - Reference to Other Frameworks
 - Customer Adoption of SOC Reports
 - Service Organization Adoption of SOC Reports
 - Key Considerations when Evaluating Reports
 - Key Takeaways
- **Q&A**

SOC Reports Overview and Structure

Overview

- Historically, many organizations that use outsourced services have asked for SAS 70 reports without recognizing that the SAS 70 report was designed for a specific purpose – to help customers and their auditors to rely upon the controls over a service provider in the context of the customers’ financial statement and internal control over financial reporting audits.
- Many of these customers were concerned about areas such as security, availability and privacy with little or no regard for financial reporting implications.
- With the retirement of SAS 70 in June 2011, organizations need to now consider the three types of Service Organization Control (SOC) report options available to service organizations and their customers that have been defined to help service providers meet a broader set of user needs:
 - **SOC 1**
 - **SOC 2**
 - **SOC 3**

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"> • 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 they receive an unqualified opinion.

Evolution of SOC1

- 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 on or after June 15, 2011
- SOC1 report has been designed to be laser-focused on controls that could impact users' financial reporting

SOC1 Similarities to SAS 70

- 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

SOC1 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

SOC1 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/SOC3 – Background

- There is a large market need for SAS 70-style reports for services with limited or no relevance to 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.
 - SOC3 is a short form report like a traditional SysTrust report.
 - The concept of a Type 1 (point in time, design-focused) report and a Type 2 (period of time, effectiveness-focused) report also applies SOC 2 and 3 reports (point in time for initial report).

SOC2/SOC3 – Components of the System

A system consists of five key components organized to achieve a specified objective and categorized as follows:

- **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)

Overview of SOC2/SOC3 Principles

Domain	Principle
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/SOC3 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/enforcement

Grouping of Criteria

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.

Structure 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
Description of system and controls	Description of system and controls	Description of system and controls	Description of system
Control objectives, controls, tests of operating effectiveness and results of tests	Control objectives, controls, tests of operating effectiveness and results of tests	Criteria, controls, tests of operating effectiveness and results of tests	–
Restricted use	Restricted use	Restricted use	Unrestricted use & ability to display seal on a website

SOC2 Suggested Report Structure Contrasted with SOC1

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

SOC3 Report Structure

Section	Description
1	Independent Service Auditors' Report Provided by KPMG LLP
2	Management's Assertion
3	System Description <ul style="list-style-type: none">• System Overview• Infrastructure• Software• People• Procedures• Data

SOC2 and SOC3 – Key Differences

- **Report Detail**

- SOC2 includes detail on the service provider’s controls as well as the auditor’s detailed test procedures and test results of those tests.
- SOC2 report enables the reader of the report to assess the service provider at a more granular level.
- SOC3 provides an overall conclusion on whether the service provider achieved the stated Trust Services criteria.
- SOC3 may be preferred in scenarios where the service detail and description of tests of controls and results are not needed by report users or where service providers may not be willing to share a detailed report due to concerns regarding disclosing sensitive information .
- SOC 2 is not intended to supersede or replace a SOC 3 engagement.

SOC2 and SOC3 – Key Differences Continued

- **Reporting Flexibility**

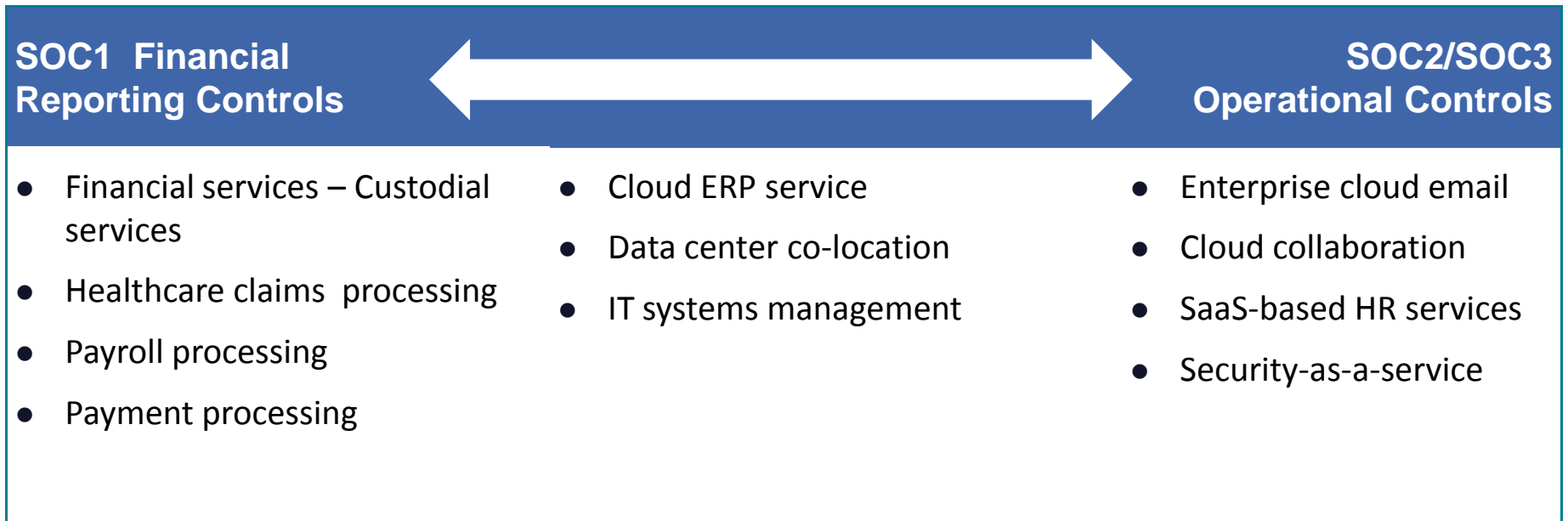
- Carve-out of supporting services provided by subservice providers supported by SOC2.
- SOC3 does not permit carve out of significant subservice provider activities. If it is not feasible to cover those activities as part of the service provider’s audit, SOC3 is not an available option.

- **Report Distribution**

- SOC 2 to be shared with current customers and prospective customers.
- SOC3 report is for general distribution.
- Option to display and maintain SOC3 seal on organization website , provided all examination criteria successfully met.

Using SOC Reports

Spectrum of Services (Examples)



Usage of SOC Reports

- **SOC1**
 - Expected that service providers that provide core financial processing services (e.g., payroll, transaction processing, asset management, etc.) will move to the SOC1 report in 2011.
 - Even some cloud service providers who provide financial processing services (e.g., cloud ERP services) will complete SOC1 reports.
- **SOC2**
 - Expected that IT service providers that have no impact or an indirect impact on customers' financial reporting systems will start to move to the SOC2 report in 2011.
 - Most cloud service providers, where customers are highly concerned with non-financial domains (including security, availability and privacy) will move to the SOC2 report.
- **SOC3**
 - Expected to be used where there is a need to communicate a level of assurance to a broad base of users without having to disclose detailed controls and test results.
 - Some organizations may complete a combined SOC2/SOC3 examination with two reports, geared for different constituencies.

Reference to Other Frameworks

- Industry surveys consistently rate security and availability as top concerns when considering cloud adoption.
- Cloud providers are increasingly basing their security programs on industry security standards and frameworks such as ISO 27001 and FISMA and industry guidelines such as the Cloud Security Alliance Cloud Controls Matrix (CCM) for additional guidance.
- SOC2/SOC3 can provide a strong mechanism for providing third party assurance in these areas.
- Additional content may be added in the informational portion of the SOC 2 report to show how SOC2 controls relate to various framework.
- This same approach can be taken for cloud or non-cloud based services where it is beneficial or required to also reference other frameworks (e.g., FISMA, FEDRAMP, HIPAA, HITECH).

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
- Vendor Integration

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

Customer Adoption of SOC Reports

- **Customers will need to prepare for the transition:**
 - Inventory vendor relationships and assess vendor risks
 - Identify relevant service organization control reports
 - Revisit contractual audit provisions
 - Communicate with your service providers early
 - Build into due diligence / vendor management processes

Service Organization Adoption of SOC Reports

- **Service providers will need to prepare for the transition:**
 - Inventory current requirements and determine go forward requirements
 - Determine which report(s) will best meet the needs of their customers and potential customers
 - Assess the impact of new standards
 - Re-validate scope / risk assessment
 - Identify any areas not previously covered, assess audit-readiness
 - Monitoring controls / basis for assertion
 - Communication plan/FAQs for educating users on the new standards and the rationale for the service provider's approach

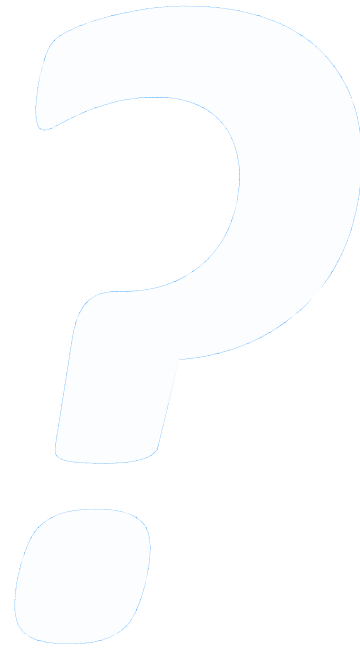
Key Considerations When Evaluating Assurance Reports

- Type of Report
- Period of Coverage
- Opinion
- Audit Firm
- Scope
- Subservice Organizations
- Control Criteria/ Objectives
- Client Control Considerations
- Description of Control Activities
- Test Procedures
- Test Results
- Changes During the Period

Key Takeaways

- **2011 will be a year of transition.**
 - SAS 70 is no more
 - 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, processing integrity, confidentiality, or privacy focus
 - Determine which principles to cover for SOC2/SOC3
 - Prepare for the transition

Q&A



Contact Details

- **Reema Anand**
Director, Advisory, Risk Consulting
KPMG LLP
reemaanand@kpmg.com
650-404-4874
- **Emily Fremming**
Manager, Advisory, Risk Consulting
KPMG LLP
efremming@kpmg.com
415-963-5590