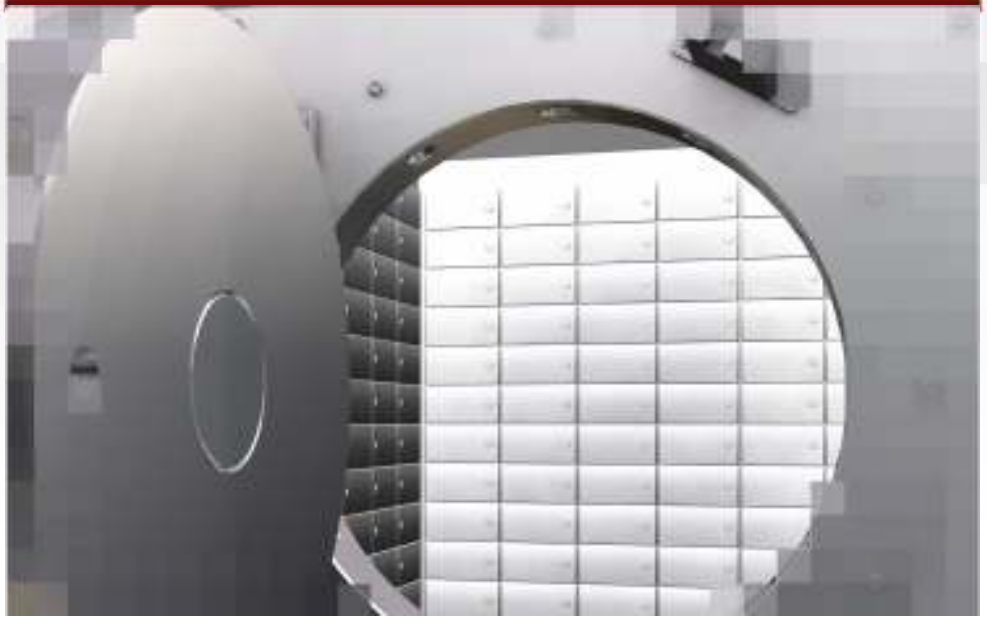
ISACA
Trust in, and value from, information systems
North Texas Chapter

SSAE 16 – Everything You Wanted To Know But Are Afraid To Ask

Kurt Hagerman CISA, CISSP, QSA
Managing Director, Coalfire
December 8, 2011



Coalfire℠

Agenda

- **SAS 70 – Misunderstood and Overused**
  - Why the change?
- **SSAE 16 – Too many SOCs**
  - SSAE 16 Overview
  - SOC 1 – SAS 70 in a new dress
  - SOC 2 – A Better Solution for Service Providers
  - SOC 3 – A New Report?
- **Which Report is the Right Fit?**
- **The Trust Services Principles**
  - Making them useful for IT Audits
  - Mapping example
- **How to Prepare to Deliver an SSAE 16**
- **Questions?**

SSAE 16 Definition

- Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization, was finalized by the Auditing Standards Board of the AICPA in January 2010 with an effective date of June 15, 2011.
- SSAE 16 effectively replaces SAS 70 as the authoritative guidance for reporting on service organizations.
- See http://www.cpa2biz.com to order a copy of SSAE 16 from the AICPA, publication number 023035.

SAS 70 – Misunderstood and Overused

- **Purpose of a SAS 70 Report**
  - Limited to internal controls related to financial statement assertions of the User Entities
  - Used by User Entity auditors to plan and perform audits of their entities' financial statements
- **How it was being overused**
  - As a litmus test by customers for vendor "compliance"
  - Part of a typical vendor due diligence process and/or vendor management program
  - Many companies didn't realize what it actually was or why they needed it – it was just on their vendor checklist
  - Often misinterpreted as a means to obtain assurance regarding controls over compliance and operations
- **Alternatives**
  - AICPA Trust Services – SysTrust and WebTrust

Why the Change?

- **Demand for a more detailed understanding of Service Provider control programs**
  - Service Providers desire to clearly communicate the effectiveness of their control program to their many clients in an efficient manner
  - User Entities demand for transparency of Service Provider controls and assurance that risks are being effectively mitigated
- **Explosion in the number of Service Providers and the number and complexity of the outsourced services available**
  - Cloud Computing and SaaS have become more common
  - More concern over the security of the increased volume of sensitive information entrusted to Service Providers
- **No one-size fits all approach to risk management and assurance reporting**

SSAE 16 – Too Many SOCs

SSAE 16 Overview

- **SSAE 16 provides three options for reporting. The type of report is selected based on the intended use and audience based on the following:**

SOC 1	**Report on controls for Financial Statement audits**	**Restricted Use Report (Type 1 or 2)**	**Auditor judgment for relevance & materiality**
SOC 2	Report on controls related to compliance or operations		Trust Services Principles & Criteria Apply
SOC 3		General Use Report (w/Public Seal)	

SOC 1 – SAS 70 In A New Dress

- **SOC 1 report is essentially the same as a SAS 70 report**
- **Scope and Use**
  - Internal control over financial reporting
  - Restricted Use: User Auditors and User Entities
  - Limited purpose:
    - Integrated with User Entity financial audits
    - To satisfy SOX compliance
- **Report Types**
  - Type 1 – Report on management's description of its system and the suitability of control design to meet the defined control objectives **at a point-in-time**
  - Type 2 - Report on management's description of its system and the suitability of control design to meet the defined control objectives **over a specified time period**

SOC 2 – A Better Solution for Service Providers

- **Report on controls relevant to the Trust Principles and Criteria**
- **Scope and Use**
  - Based on Trust Services Principles and Criteria Categories
    - **Principles:** Security, Availability, Processing Integrity, Confidentiality, Privacy
    - **Criteria Categories:** Policies, Communications, Procedures, Monitoring
  - Each Principle incorporates all Criteria Categories with varying numbers of principle specific criteria per category
  - Can select criteria based on applicability to services
  - Follows requirements and guidance in AT Section 101, Attest engagements of SSAEs
  - Contains a detailed description of the auditor's tests of controls and results of those tests as well as the auditor's opinion on the description of the service provider's system
  - Primary users of SOC 2 reports are management of the Service Provider and management of the User Entity
- **Reports**
  - Type 1 and Type 2

SOC 2 – Trust Principles

- **Five Trust Principles**
  - **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 GAPP (Generally Accepted Privacy Principles).
    - GAPP – Set of 10 principles designed to address the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and disposal of personal information.

SOC 2 – Trust Principle Criteria

- **Four Criteria**
  1. **Policies:** The entity defines and documents its policies for the {Insert Principle} of its system.
  2. **Communications:** The entity communicates the defined {Insert Principle} policies to responsible parties and authorized users.
  3. **Procedures:** The entity placed in operation procedures to achieve its documented system {Insert Principle} objectives in accordance with its defined policies.
  4. **Monitoring:** The entity monitors the system and takes action to maintain compliance with its defined {Insert Principle} policies.

SOC 2 – Engagement Criteria

- **Scope that is likely to be useful to intended users**
  - Define the scope of the system to include all relevant services including the infrastructure, software, people and processes used to deliver them.
- **Management accepts their responsibilities**
  - Written assertion required
  - Management's basis and criteria for the assertion
  - Service auditor's responsibility to assess managements assertion
- **Suitable Criteria**
  - Select the set of criteria from each Trust Principle that are applicable to the services being provided. Security, Availability and Confidentiality are typically the most applicable.
  - Ensure that the selected criteria are aligned and mapped to the appropriate controls in the Service Provider's control program.

SOC 2 – Engagement Criteria (continued)

- **Skillset of Auditor**
  - Technical training and proficiency
  - Knowledge of the subject matter
  - Knowledge of the
    - service organization's industry and business
    - industries of the user entities
    - systems and technology
  - Experience evaluating
    - risks related to the suitability of the design of controls
    - the design of manual and IT controls related to the selected trust services principles, performing tests of such controls, and evaluating the results of the tests

SOC 2 - Examples

- **Cloud Service Provider**
  - Offers virtualized computing environments and services and wishes to assure its customers that they maintain the confidentiality of their information in a secure manner and that the information will be available when it is needed.
  - A SOC 2 report addressing security, availability and confidentiality provides customers with a description of the provider's system and the controls that help achieve those objectives.
- **Medical Claims Processor**
  - Processes claims for health insurers and wishes to assure those users that its controls over the processing of claims will protect the information in those claims, which is subject to privacy laws and the HIPAA/HITECH regulations.
  - A SOC 2 report addressing security, confidentiality and privacy would provide customers with this assurance.

SOC 2 – Slow Adoption – Why?

- **Lack of market knowledge/acceptance**
  - Trust Principles not widely understood or promoted
  - Resistance to change (have always asked for SAS 70)
- **Trust Principles and Criteria ≠ Controls**
  - Difficulty mapping trust principles and criteria to control programs
- **Few SysTrust or WebTrust assessments conducted**
  - Unfamiliar with Trust Services Principles
- **Highly Technical and Complex Service Offerings**
  - Cloud service providers
  - IaaS/PaaS/SaaS
  - Virtualization, cutting edge networking and security solutions
  - Requires higher degree of technical knowledge and experience

SOC 3 – A New Report?

- **Scope and Use**
  - Based on the Trust Services Principles and Criteria like a SOC 2
  - Provides only the auditor's report on whether the system achieved the trust services criteria with no description of tests and results or opinion on the description of the system.
  - The same as the prior SysTrust report
  - Can distribute the report to customers and publicly display a seal of approval using the SOC 3 Report: SysTrust for Service Organizations seal.
- **Reports**
  - Single Type: General Use Report (with a public seal)

SOC 3 - Example

- **Large Online Retailer with an Affiliates Program (think Amazon)**
  - Program permits affiliates (small specialist retailers) to use the transaction processing systems of the online retailer.
  - Affiliates want to assure their customers that the retailer's processing systems are secure and maintain the confidentiality and privacy of customer information.
  - The online retailer has a SOC 3 report prepared covering its processing system addressing security, confidentiality and privacy and then allows its Affiliates to distribute the report to its customers via a link on their websites and display the SOC 3 Report: SysTrust for Service Organizations seal.

Which Report is Right for My Organization?

Use Case	Appropriate SOC Report
Are your users focused on internal control over financial reporting?	SOC 1
Are key compliance & operational controls of primary interest?	SOC 2 or SOC 3
Do your customers need detail about the systems and processes?	SOC 1 or SOC 2
Will the posting of a summary report/seal suffice?	SOC 3
Will the report be used by your customers as part of their SOX compliance?	SOC 1
Do your customers have the need to understand the details about your services, controls and the tests and results of the tests performed by your auditor?	Yes - SOC 2 No - SOC 3

Making the Trust Services Principles Useful for IT Audits

- **Study and understand the Trust Principles and Criteria**
- **Develop a Common Controls Framework**
  - Cross map the Trust Principles and Criteria against other common frameworks and regulations

ISO 27002

HITRUST

FISMA

GLBA

FFIEC

- **Consolidate assessment work for multiple requirements**
  - Single assessment with multiple reports
  - More efficient and cost effective for both the auditor and service provider

Coalfire

Trust Principle Criteria Mapping Sample

Security Principle and Criteria Table The system is protected against unauthorized access (both physical and logical)			
1.0		Policies: The entity defines and documents its policies for the security of its system.	
1.1		The entity's security policies are established and periodically reviewed and approved by a designated individual or group.	PCI 12.1, 12.1.3
1.2		The entity's security policies include, but may not be limited to, the following matters:	
	a.	Identifying and documenting the security requirements of authorized users	PCI 12.4
	b.	Classifying data based on its criticality and sensitivity and that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements	PCI 9.7.1
	c.	Assessing risks on a periodic basis	PCI 12.1.2
	d.	Preventing unauthorized access	PCI 7.1, 7.2, 9.1, 12.3.1, 12.3.2
	e.	Adding new users, modifying the access levels of existing users, and removing users who no longer need access	PCI 12.5
	f.	Assigning responsibility and accountability for system security	PCI 12.5
	g.	Assigning responsibility and accountability for system changes and maintenance	PCI 12.5

Sample Mapping from Coalfire Common Controls Framework

Preparing to Deliver an SSAE 16 Report

- Understand your customer's business and their customer's needs
- Determine if you have the requisite technical skills and experience to evaluate the services and underlying technologies
- Understand your customer's security controls program
- Provide your customer with a preliminary selection of the Criteria you believe are appropriate and have them do the same, then meet to compare, discuss and agree on the final set of criteria.

Questions?

Thank You

Kurt Hagerman, CISA, CISSP, QSA

Managing Director, Coalfire Dallas

khagerman@coalfire.com

5001 Spring Valley Road. Suite 1160E

Dallas, TX 75244

972-763-8010

www.coalfire.com