

Service Organization Control (SOC) Reporting

What User Auditors and User Entity Perspective on New SOC Reporting that replaces SAS 70

GA Society CPAs
North Atlanta Chapter Meeting
October 20, 2011



October 20, 2011

Dan Schroeder, Partner-in-Charge
IT Audit & Risk Advisory Services

Proficient, thorough & tirelessly committed.

That's HA&W.

About the Presenter

Dan Schroeder

CPA/ CITP, MBA, CISA, CISM, CIA

- Partner-in-Charge, HA&W IT Audit & risk Management Services
- SAS 70, SSAE 16, security and privacy trust services, IT Governance, and other compliance services
- 20+ years of IT advisory, audit and attest experience with concentration on financial services, mfg/distribution, and technology service providers
- Chair of AICPA's Information Technology Executive Committee (ITEC)
- Serves on AICPA SOC Peer Review Task Force
- Leading author of "IT Considerations for Risk Based Auditing" whitepaper
- Lead development of AICPA IT Audit School

HA&W highlights

Firm Highlights

- Largest independent CPA firm based in GA, approx. 350 associates
- Clients throughout the U.S. and 30+ other countries
- PCAOB member firm
- Premier firm in Southeast Tech Sector, specialize in helping companies from ideas to exit
- Independent member of Baker Tilly International with presence throughout U.S. and over 110 countries
- Professionals at HA&W speak 10 different languages

IT Practice

- Recognized thought leadership in SAS 70/SSAE 16/SOC services
- National SOC (SAS 70) practice
- Security Risk Management
- Privacy Risk Management
- PCI Compliance
- Data Assurance
- IT Internal Audit
- IT Governance

Session Overview

- Explosive growth in the availability and use of service organizations (e.g., SaaS, cloud, datacenters, etc.)
 - Significant/critical risks represented by service organizations – ICFR, operational, compliance
- User entity approach to managing service organization risks is generally poor, often absent
- Highlight AICPA SOC reporting standards with emphasis on user auditor and user entity implications
- New SOC framework represents great opportunity for User Entities to get this right.

Service Organization Control (SOC) Terms (1/2)

- **Service Organization.** An organization or segment of an organization that provides services to user entities:
 - which are likely to be relevant to those user entities' internal control over financial reporting
 - related to the applicable trust services criteria
- **Service Auditor.** A practitioner who reports on controls of a service organization
- **Service organization's system.** The policies and procedures designed, implemented and documented by management of the service organization to provide user entities with the services covered by the service auditor's report
- **Subservice organization.** A service organization used by another service organization

Service Organization Control (SOC) Terms (2/2)

- **User Entity.** An entity that uses a service organization
- **User Auditor.** The auditor who reports on the financial statements of the user entity
- **Controls at a service organization.**
 - The policies and procedures at a service organization likely to be relevant to user entities internal control:
 - over financial reporting (SOC 1)
 - as they relate to meeting the applicable trust services criteria (SOC 2 and SOC 3)
 - These policies and procedures are designed, implemented, and documented by the service organization to provide reasonable assurance about:
 - the achievement of the control objectives relevant to the services covered by the service auditor's report (SOC 1)
 - meeting the applicable trust services criteria (SOC 2 and SOC 3)

Purpose of SOC Reporting

- User Entity management is responsible for assessing and addressing risks faced by the user entity related to:
 - financial reporting,
 - compliance with laws and regulations,
 - efficiency and effectiveness of operations
- **Service organizations can extend or increase these risks**
- User Entity governance responsibilities extend to the Service Organization

Common User Entity Practices for Governance of Service Organizations

Common user entity practices for service organization governance

- 60% of users of cloud providers do not monitor controls of their cloud providers (Information Week 2010 Survey)
- Questionnaires: 200 – 500 questions
- On-site audits
- “SAS 70” reporting

Common SAS 70 Misunderstandings

1. Companies that use SaaS providers, can rely on the SaaS provider's third party data center SAS 70 report for all their risk management needs.
2. SAS 70 report is appropriate for any type of service provider; i.e., it also can be used to report on controls related to compliance and operational matters, such as confidentiality, privacy, processing integrity, etc.
3. SAS 70 report demonstrates something meets best practices or is world-class, etc.
4. SAS 70 is designed to help with sales.
5. SAS 70 is a "Certification" or demonstrates "Compliance."

SAS 70 (SSAE 16) Heavily Marketed as “Certification” or “Compliance” Report



Examples of Common Misrepresentations about SAS 70

“A SAS-70 Audit is voluntary, so it acknowledges a high level of commitment by {name of Service Organization} and also assists companies in meeting regulatory compliance for HIPAA (Health Insurance Portability and Accountability Act), SOX (Sarbanes-Oxley Act of 2002), GLBA (Gramm-Leach-Bliley Act of 1999, and ISO 17799.”

Pharmacy Benefit Management Website – July 2011

Data Centers are central to our modern economy, their risks are significant, but grossly ignored / misunderstood

“We have over 700 companies that use our data centers. Almost all of them want a SAS 70 report simply to check the box. Less than ten of them ask appropriate questions about real risks we represent, which in the case of availability, can be very significant. “

*Director, Risk and Compliance Management
Leading National Multi-Tenant Data Center*

Amazon Web Services (AWS)

“Amazon Web Services has successfully completed a Statement on Auditing Standards No. 70 (SAS70) Type II Audit SAS70 certifies that a service organization has had an in-depth audit of its controls....which in the case of AWS, relates to operational performance and security to safeguard customer data.”

Posted Fall 2009 to <http://aws.amazon.com/>

“Major Amazon Outage Ripples Across Web”

April 21, 2011 numerous publications

*“Amazon Web Services Reports Outage in the U.S. Late Monday”
(Aug 8, 2011)*

Epsilon Marketing Services

- 2004 Press Release:
 - *"The SAS70 endorsement helps provide credible proof to our clients that their critical data is secure when using our database marketing services," said "This recognition supports our ongoing commitment to provide database marketing operational excellence with the highest levels of security and reliability."*
- April 2011 News reported everywhere
 - *Massive Breach at Epsilon Compromises Customer Lists of Major Brands*

Introducing the AICPA Service Organization Controls (SOC) reporting framework

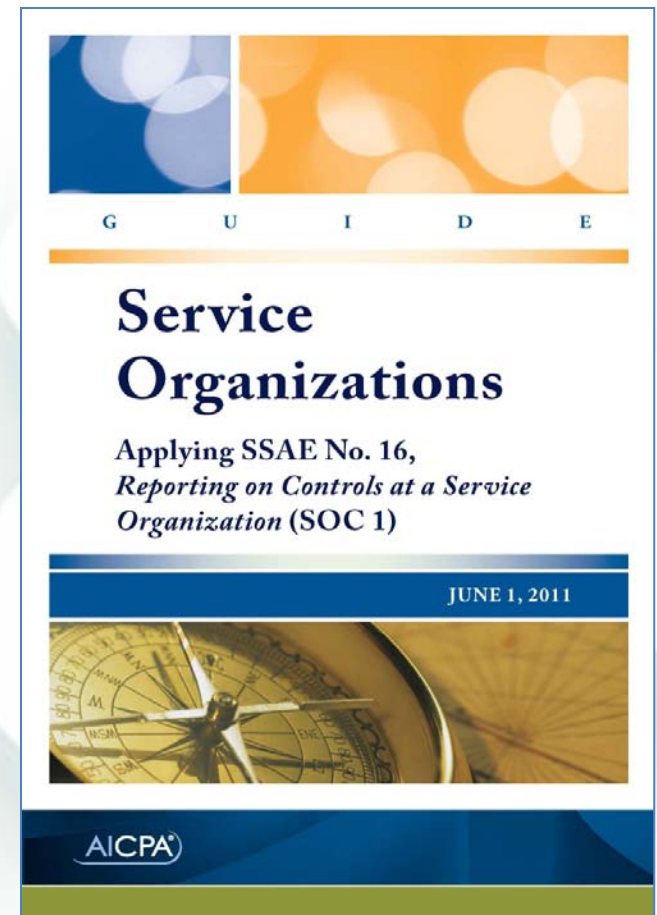


SOC Reports from User's Perspective

| Report | Users | Why | Interest |
|--------|---|--|--|
| SOC 1 | Users' financial management and control, User Auditors | Financial Audit/SOX 404 | Controls relevant to user financial reporting |
| SOC 2 | User Management (operations and compliance) "Informed" Prospects Regulators | GRC programs Oversight Due diligence | Detailed System Description, Controls, and test of controls over 1 or more Trust Service Principle domains |
| SOC 3 | Any users with need for confidence in service organization's controls | Limited due diligence | General confidence in efficacy of controls over 1 or more Trust Service Principle domains |

SOC 1/SSAE 16 has replaced SAS 70

- **SOC 1: SSAE No. 16, Reporting on Controls at a Service Organization** (AICPA, Professional Standards, AT sec. 801), and the AICPA Guide *Service Organizations: Applying SSAE No. 16, Reporting on Controls at a Service Organization*
- **Effective 6-15-2011**



SOC 1 Report Purpose

- **Provide User Auditor** with information and a CPA's opinion about controls at a service organization that **may be relevant to a user entity's internal control over financial reporting.**
- **Enable User Auditor** to perform risk assessment procedures and, if a type 2 report is provided, to use the report as audit evidence that controls at the service organization are operating effectively.
- **Avoid redundant auditing** of service organization.

SOC 1 Report Intended Users

Intended solely for the information and use of:

1. Management of the service organization
2. User entities during some or all of the period covered by the report (for type 2 reports) and user entities as of a specified date (for type 1 reports)
3. Auditors of the user entities' financial statements (i.e., user auditors).

SOC 1 Reporting: User Auditor Responsibilities

- The requirements and guidance for user auditors is retained in AU section 324, *Service Organizations (AICPA, Professional Standards)*.
- When the clarified *SAS Audit Considerations Relating to an Entity Using a Service Organization* becomes effective, it will replace the guidance for user auditors currently in AU section 324.
 - The clarified SAS is effective for audits of financial statements for periods ending on or after December 15, 2012. (Early implementation is not permitted.)

AU 324 Review of Key User Auditor Considerations (1/4)

- Inquire about the service auditor's professional reputation, competence, and independence.
- Read the complete report focusing on:
 - The independent service auditor's report
 - The service organization's description
 - Information provided by the service auditor, which may include test of operating effectiveness

Caution: This and subsequent slides represents a partial review -- See also AU 324

AU 324 Review of Key User Auditor Considerations (2/4)

Determine if the information presented in either the type 1 or type 2 report, along with the user auditor's knowledge of the user organization, is sufficient to:

- Understand the aspects of the service organization's control that may affect the processing of the user organization's transactions
- Understand the flow of significant transactions through the service organization
- Assess whether the control objectives are relevant to the user organization's financial statement assertions. Also, are any key control objectives missing?
- Determine whether the service organization's controls are suitably designed to prevent or detect processing errors that could result in material misstatements in the user organization's financial statements

AU 324 Review of Key User Auditor Considerations (3/4)

- If a type 2 report is relevant to the user organization, the user auditor needs to determine whether:
 - The report provides adequate evidence of the nature, timing, extent, and results of tests of operating effectiveness
 - The timing of the tests operating effectiveness is appropriate for the “as of” date/period covered by the user organization’s financial statements
 - The report identifies results of tests, including exceptions and other information that could affect the user auditor’s considerations

AU 324 Review of Key User Auditor Considerations (4/4)

If controls at the service organization are operating effectively, the user auditor:

1. May be able to access control risk below the maximum for certain assertions in the user organization's financial statements and reduce substantive test
2. Should evaluate the operating effectiveness of the service organization's control in conjunction with the user organization's internal controls
3. Should consider whether the user organization has implemented complementary controls (user controls) contemplated in the service organization's design of the service organization's control
4. Read and assess testing performed and results of test
5. Consider the quantity and quality of evidence provided

SOC 1: Use of Service Org IA when preparing the report

- Planning Considerations
- Using the Work of the IA function
- Effect on Service Auditor's report:
 - No reference in opinion letter
 - Disclosure or attribution of role of IA when describing test of controls

Trust Services Principles & Criteria

Foundation for SOC 2 and SOC 3



Trust Services Principles

- 1. Security.** The system is protected against unauthorized access (both physical and logical)
- 2. Availability.** The system is available for operation and use as committed or agreed
- 3. Processing Integrity.** System processing is complete, accurate, timely, and authorized.
- 4. Confidentiality.** Information designated as confidential is protected as committed or agreed
- 5. 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)

Categories of Trust Services Criteria (other than Privacy)

- 1.0 Policies.** The entity has defined and documented its policies relevant to the particular principle.
- 2.0 Communications.** The entity has communicated its defined policies to responsible parties and authorized users of the system.
- 3.0 Procedures.** The entity placed in operation procedures to achieve its objectives in accordance with its defined policies.
- 4.0 Monitoring.** The entity monitors the system and takes action to maintain compliance with its defined policies.

TS Criteria and Illustrative Control example

3.0 Procedures: The entity placed in operation procedures to achieve its documented system security objectives in accordance with its defined policies.

Criteria

3.2 Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters:

- a. Logical access security measures to restrict access to information resources not deemed to be public.

Illustrative Controls

- Logical access to nonpublic information resources is protected through the use of native operating system security, native application and resource security, and add-on security software.
- Resource specific or default access rules have been defined for all nonpublic resources.
- Access to resources is granted to an authenticated user based on the user's identity.

Generally Accepted Privacy Principles (GAPP)

- GAPP contain **ten privacy principles and related criteria** that are essential for the proper protection and management of personal information.
- These privacy principles and criteria are **based on internationally known fair information practices** included in many privacy laws and regulations of various jurisdictions around the world and in common and leading practices.
- Development supported and endorsed by:



GAPP Principles

- 1. Management.**
- 2. Notice.**
- 3. Choice and Consent.**
- 4. Collection.**
- 5. Use and Retention.**
- 5. Access.**
- 6. Disclosure to Third Parties.**
- 8. Security for Privacy.**
- 9. Quality.**
- 10. Monitoring and Enforcement.**

SOC 2: Report on controls at a service organization relevant to one or more:

- 1) Security**
- 2) Availability**
- 3) Processing Integrity**
- 4) Confidentiality**
- 5) Privacy**

SOC 2 Report Purpose

To provide management of a service organization, user entities and other specified parties with information and a CPA's opinion about controls at the service organization relevant to one or more of the Trust Services (TS) principles.

- Per AT 101
- SOC 2 Type 2 reporting for Privacy principle also includes the organization's compliance with commitments in its statement of privacy practices.

SOC 2 Report Content

- Auditor's Opinion Letter:
 - Fairness of Presentation
 - Suitability of Design
 - Operational Effectiveness of Controls (Type II only)
- Management Assertion
 - System Description (detailed)
 - Statement of privacy practices
 - Sub-Service organization functions – carve-out or inclusive
- Criteria related to the auditor's evaluation
- Test of Controls and Results
- Other Information from Service Organization (unaudited)

Management Assertion for SOC 2

- Management's description of the service organization's system **fairly presents the service organization's system**
- Controls stated in management's description of the service organization's system were **suitably designed**...
- Controls **operated effectively**...
- The service organization **complied with its privacy commitments**. (When scope covers GAPP)

System Description common requirements

- The types of services provided
- System components used to deliver the services (ISPPD)
- System boundaries
- Handling of significant events
- Reporting to User Entities

----- continued -----

System Description common requirements

- Sub-service org functions and
 - How info is exchanged
 - Controls the service org performs over the sub-service org
- Controls for applicable criteria including:
 - Complementary User Entity (CUE) controls, and
 - Controls at subservice org when inclusive method used.
- Other aspects of control environment, risk assessment, information and communication and monitoring.
- Relevant (material) changes to the system during the period.

SOC 2 Report Intended Users

Management of the service organization and other specified parties (a) who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria
- The applicable trust services criteria
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks

(a) SOC 2 reports also may be useful to a user entity's internal auditors or practitioners reporting on a user entity's security, availability, processing integrity, confidentiality, or privacy

User Entity Considerations when evaluating SOC 2 reporting (1/3)

- Confirm System Description aligns to agreements and service level agreements (SLAs)
- Does the Principle(s) being reported on align to the user entity control requirements and risk management needs?
- Do the controls defined by the service organization prevent or detect risks represented by the service organization related to compliance with laws and regulations, and the efficiency and effectiveness of operations?

User Entity Considerations when evaluating SOC 2 reporting (2/3)

- Do the controls provide sufficient information for users to understand how that control may affect the their entity?
 - Frequency
 - Responsible party
 - Nature of activity performed
 - Subject matter to which the control is applied
- Is timing, nature, extent of testing adequate to meet risk management needs.
- Is period of coverage of testing adequate.
- Do testing results indicate performance of controls is sufficient?

User Entity Considerations when evaluating SOC 2 reporting (3/3)

- Testing exceptions could indicate need to strengthen Complementary User Entity Controls (CUEs), make other process changes, increase degree of monitoring, etc.
- For any CUEs identified by the Service Organization:
 - Confirm relevancy, deploy and monitor
- Sub-service organizations
 - Are they sufficiently described and are control measures defined commensurate with the risk represented by the sub-service organization?
 - Inclusive vs. carve-out method appropriate?

SOC 3: Trust Services Report for Service Organizations



SOC 3 Report Overview

- Covers one or more Trust Services Principles
- Report prepared per AT 101 with criteria from one or more TS representing suitable criteria
- Summary assertion that criteria fulfilled for designated date or period
- Unrestricted distribution
- Current and prospective customers
- Supports marketing to demonstrate that the service organization has effective controls in place to mitigate risks related to security, availability, processing integrity, confidentiality, or privacy



SOC 3 Report Content

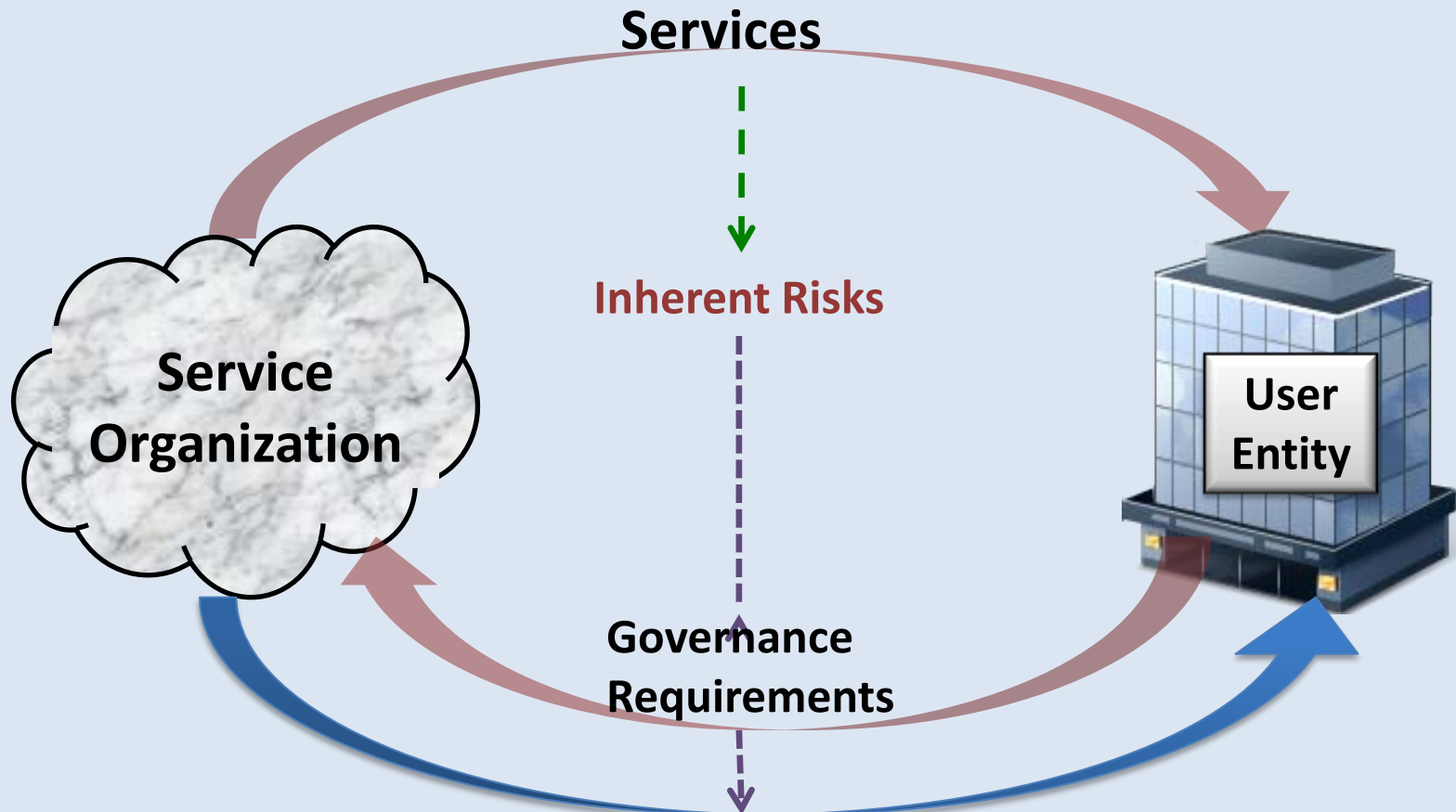
- Auditors Opinion Letter regarding fairness of Management Assertion relative to criteria for point-in-time, or period of time.
- Management Assertion
- System Description (summary)
- Criteria and Controls to fulfill the criteria
- Other Information from Service Organization (unaudited)

How User Entities can leverage the new SOC framework for governance of their Service Organizations

User Entity: Steps in Service Organization Governance

1. Understand services and the service organization's "system"
2. Assess Inherent Risks
3. Define governance requirements to mitigate risks (e.g., controls, assurance reporting, contract terms, insurance, etc.)
 - a) Identify appropriate SOC reporting approach when applicable and frequency of reporting
 - b) **Customize SOC 2 reports to address specific requirements:**
 - Compliance (e.g., PCI, HIPAA)
 - Recognized control frameworks (e.g., ISO 27002, NIST)
 - Service Level agreement criteria
4. Monitor reporting (SLA, attest)
 - a) Enact other risk mitigation procedures as needed.
5. Integrate/link service organization control reporting to IA/ERM program.

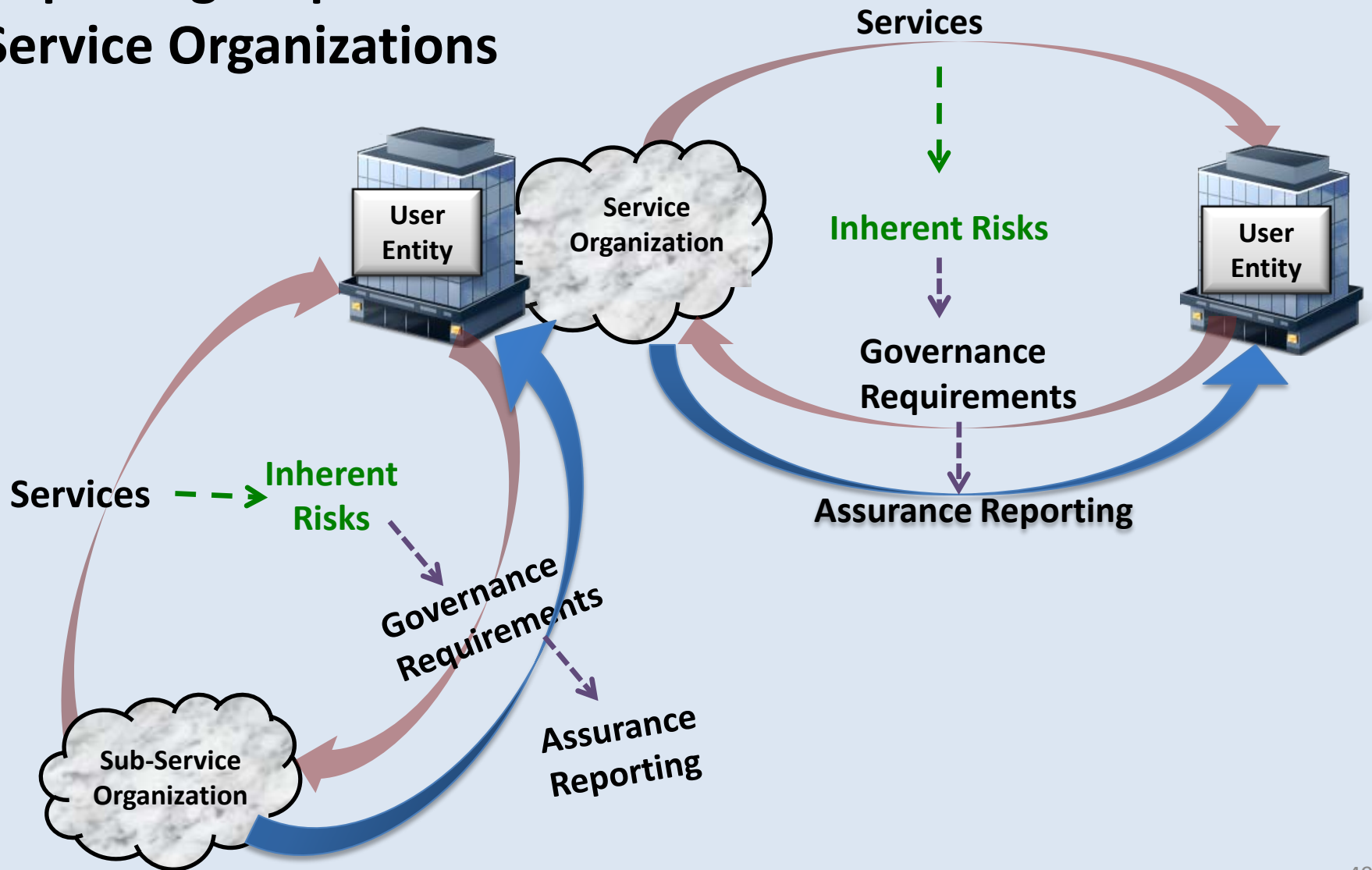
Identify SOC Reporting Approach that fulfills Risk Based Governance Requirements



Attestation / Assurance Reporting:

- SOC 1 / SOC 2 / SOC 3
- Other Attest (e.g., AT 101, 201, AT 601)
- SLA Reporting

Extending Governance and SOC Reporting Requirements to Sub-Service Organizations



Extending/Customizing SOC 2 Reporting

- User Entities can request Service Organizations extend SOC criteria to address additional criteria not covered within Trust Services criteria for principle being reported related to regulatory requirements, service level agreements, etc
- Trust Services criteria are often written at a high level and therefore, often can be mapped to specific regulatory requirements and recognized control frameworks; for example:
 - HIPAA Privacy and Security Rules map very well to GAPP.
 - PCI DSS Requirements map very well to Security principle.

Extending/Customizing SOC 2 Reporting

Illustration of HIPAA Mapping to GAPP

| HIPAA Security Standards: Administrative Safeguards | | | Mapping to GAPP Criteria |
|---|--|--|--------------------------|
| Section / Standards | Implementation Specs | Definition | |
| 164.308(a)(4) Information Access Management: Implement policies and procedures for authorizing access to electronic protected health information | Isolating Health care Clearinghouse Function (R) | If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | 7.2 |
| | Access Authorization (A) | Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. | 8.2.2-8.2.3 |
| | Access Establishment and Modification (A) | Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | 8.2.2-8.2.3 |

Example SOC 2 and SOC 3 Scenarios

| Service Provider Scenario | Key Risks | Principles Reported |
|--|--|---|
| Healthcare – advisory and processing of claims | <ul style="list-style-type: none"> • Privacy, security • HIPAA compliance | <ul style="list-style-type: none"> • Privacy |
| Provider of Targeted Marketing Campaigns | <ul style="list-style-type: none"> • Timeliness and accuracy in execution of marketing campaigns | <ul style="list-style-type: none"> • Processing Integrity • Security • Confidentiality |
| Financial services: SaaS for Equity Trading | <ul style="list-style-type: none"> • Timely, accurate quote and trade execution • Data breach | <ul style="list-style-type: none"> • Processing Integrity • Availability |
| Communications gateway bridging user entity back office and mobile comm carriers | <ul style="list-style-type: none"> • Exposure of sensitive data being processed and translated • System downtime | <ul style="list-style-type: none"> • Availability • Security • Confidentiality |
| Document Management | <ul style="list-style-type: none"> • Exposure of sensitive case data • Incorrect indexing, cataloging, storage | <ul style="list-style-type: none"> • Processing Integrity |
| Data Center hosting numerous companies IT environments | <ul style="list-style-type: none"> • Continuity of processing and internet connectivity, environmental safeguards to restrict access and protect the equip. | <ul style="list-style-type: none"> • Availability |

Linking Service Organization Risks to User Entity IA / ERM Program

2. Identify mitigating controls and who performs the control

3. Map to SOC reporting when possible

| | | Mitigating Controls | | | |
|-----------------|---------|-------------------------|---------|---------|---------|
| | | Control # / Definition: | 1. | 2. | 3. |
| Source of Risk: | | Control performed by: | UE | Svc Org | UE |
| Inherent Risks | Risk: | SOC Report X-Ref | n/a | CA 7.3 | UCC 4.5 |
| 1. | UE | | Primary | | |
| 2. | Svc Org | | | Primary | |
| 3. | Svc Org | | | | Primary |

1. Identify Service Organization risks affecting control objective or function, or F/S assertion

IN SUMMARY...

Key Take-Aways for User Entities (1/2)

- Leverage this opportunity to improve efficacy of reporting for governance purposes
- Understand and prioritize risks represented by service organizations
- Collaborate with service organization to arrive at reporting/governance approach that meets both parties needs
 - Establish reporting and monitoring approach that is commensurate with risks.
 - Map to risk/controls for the process supported
- Establish control structure and standards that align to risk and compliance needs

Key Take-Aways for User Entities (2/2)

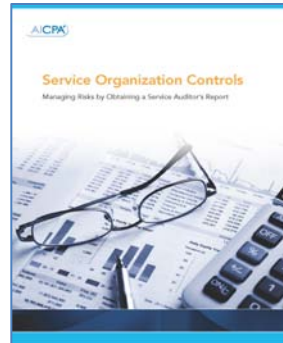
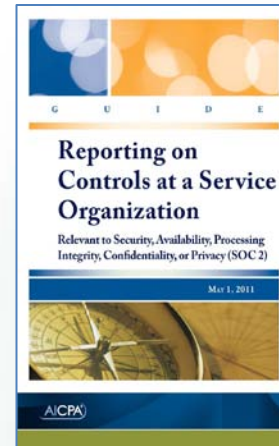
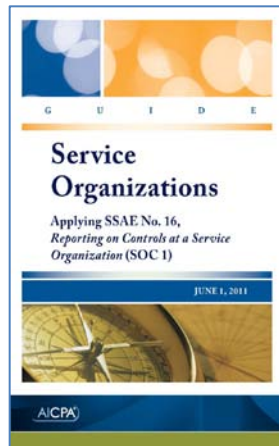
- Map compliance control requirements (e.g., HIPAA) and recognized control frameworks (e.g., ISO 27002, NIST) to Trust Services principles and criteria
 - Extend criteria when necessary
- Do not assume that legacy SAS 70 reports naturally convert to SSAE 16/SOC 1
 - SOC 2 may be more appropriate
 - SOC 1 and SOC 2 may be more appropriate
- Contracts:
 - Write reporting requirements into contract before closing deal.
 - Revise existing contracts to reflect change represented by SOC
- Vendor management: leverage SOC reporting to minimize questionnaires

Summary of Change in User Entity Approach

| Old Way | | New Way |
|--|------------------------------------|---|
| Service Org | Who determines report type? | User Entity |
| SAS 70 – what else? | Report generated? | SOC Report(s) to reflect governance needs |
| After the agreement, or SAS 70 standard contract provision | When reporting defined? | Part of the agreement |
| Annually | Frequency of report | Frequency driven by risk based monitoring needs |
| None | Linkage to IA / ERM | Integrated |
| Complete the checkmark | Why report needed? | Fulfill Governance needs |

AICPA Resources

www.aicpa.org/soc



Thank You!

For more information....

dan.schroeder@hawcpa.com

<http://www.linkedin.com/in/danschroeder>

404-862-9924

www.aicpa.org/soc

http://www.hawcpa.com/home/it_audit.asp