



**PERKINS & CO**

**Risk Management Group** presents:

# **SSAE16 & SOC Reports**

**“Considerations for the Financial Executive”**

**Michael Hulet, CPA, CISA**  
**Principal at Perkins & Co**

# SAS No. 70, Service Organizations

**A standard for reporting on a service organization's controls affecting user entities' financial statements. Only for use by service organization management, existing user entities, and their auditors.**



# SAS No. 70, Service Organizations

## Misuse:

- “SAS 70 Certified” or “SAS 70 Compliant”
- Controls related to subject matter other than internal control over financial reporting
- Made report public






# Other Service Organization Control Reports (SOC)

**Marketplace demand for detailed report on controls on subject matter other than internal control over financial reporting includes:**

- ✓ Security
- ✓ Availability
- ✓ Processing integrity
- ✓ Confidentiality
- ✓ Privacy

# How the AICPA Addressed Issues



**Split SAS 70 into two standards: one for service auditors (SSAE 16), the other for user auditors (effective for 2012 year-end audits)**

**Recognized need for assessment of controls over security, availability, processing integrity, confidentiality or privacy**

**Brought together all options for reporting on controls at service orgs**

**Supported public interest by helping CPAs/service organizations correctly apply and use the standards**

# Service Organization Control Reports



**3 reports to help service organizations demonstrate reliability**

**CPA, client determine proper engagement for market need**

**SOC logo for service org's marketing, websites**

**Information on SOC reports:  
[aicpa.org/soc](http://aicpa.org/soc)**

# SOC Report Logos

For CPAs who provide the services that result in a SOC 1, SOC 2 or SOC 3 report

For service organizations that had a SOC 1, SOC 2 or SOC 3 engagement within the past year



# New Standards and Names



SERVICE ORG CONTROL 1 (SOC 1)	SERVICE ORG CONTROL 2 (SOC 2)	SERVICE ORG CONTROL 3 (SOC 3)
<b>SSAE16</b> - Service auditor guidance	<b>AT 101</b>	<b>AT 101</b>
Restricted Use Report (Type I or II report)	Generally a Restricted Use Report (Type I or II report)	General Use Report (with a public seal)
Purpose: Reports on controls for F/S audits	Purpose: Reports on controls related to compliance or operations	Purpose: Reports on controls related to compliance or operations

Trust Services Principles and Criteria



# SOC 1 Report (restricted use)

- **Report on controls at a service organization relevant to a user entity's internal control over financial reporting**





# SOC 1 Report (restricted use)

- **Engagement performed under:**
  - ✓ SSAE 16 (auditor obtains level of evidence and assurance as in SAS 70 service auditor engagement)
  - ✓ AICPA Guide, *Applying SSAE No. 16, Reporting on Controls at a Service Organization*
- **Contents of report package:**
  - ✓ Description of service organization system
  - ✓ CPA's opinion on fairness of description, suitability of design, operating effectiveness of controls





# SSAE 16: New Requirement for Written Assertion

- **Service auditor must obtain written assertion from service organization's management about the fairness of the presentation of the description of the service organization's system and about the suitability of the design**





# SSAE 16: New Requirement for Written Assertion

- **For type 2 engagements, operating effectiveness of the controls must be included in assertion**
- **Assertion will either accompany service auditor's report or be included in description of service organization's system**



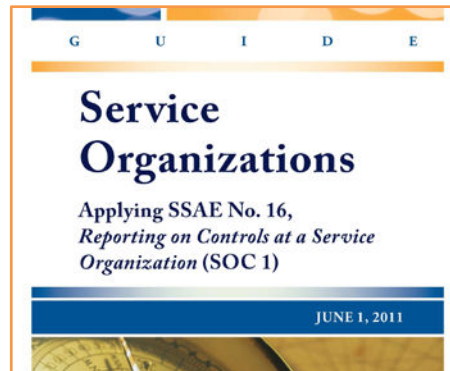
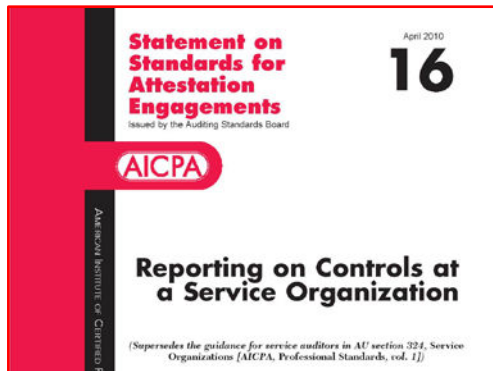
# SOC 1 Reports – Type 1 and Type 2

- **Both report on the fairness of the presentation of management's description of the service organization's system, and...**



# SOC 1 Reports – Type 1 and Type 2

- ✓ Type 1 also reports on the suitability of the design of the controls to achieve the related control objectives included in the description **as of a specified date**
- ✓ Type 2 also reports on the suitability of the design **and operating effectiveness** of the controls to achieve the related control objectives included in the description **throughout a specified period**



# SOC 2 Report (use determined by auditor)

- **Report on controls at a service organization relevant to security, availability, processing integrity, confidentiality or privacy**





# A Word About Trust Principles and Criteria

- **Each principle and criteria (except Privacy) is organized into four broad areas**
  1. Policies
  2. Communications
  3. Procedures
  4. Monitoring
- **Privacy criteria based on Generally Accepted Privacy Principles (GAPP) comprising of 10 principles**



# SOC 2 Report (use determined by auditor)

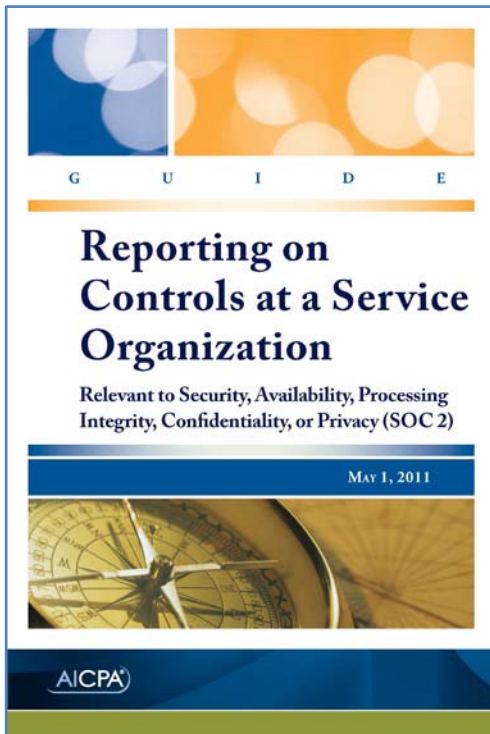
- **Engagement performed under:**
  - ✓ *AT 101, Attestation Engagements*
  - ✓ *AICPA Guide, Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy*
- **Contents of report package same as SOC 1**



# SOC 2 Reports – Type 1 and Type 2

- **Both report on management’s description of a service organization’s system, and...**

- ✓ Type 1 also reports on suitability of design of controls
- ✓ Type 2 also reports on suitability of design **and operating effectiveness** of controls



# SOC 3 Report (general use)

- **Trust Services Report for Service Organizations**
- **Engagement performed under:**
  - ✓ *AT 101, Attestation Engagements*
  - ✓ *AICPA TPA, Trust Services Principles, Criteria and Illustrations*



# SOC 3 Report (general use)

- **Contents of report package:**
  - ✓ CPA's opinion on whether entity maintained effective controls over its system
  - ✓ A seal can be issued on service organization's website (if CPA is so licensed by CICA)



# Report Comparison



	Who the users are	Why	What
SOC 1	Users' controller's office and user auditors	Audits of Financial Statements	Controls relevant to user financial reporting
SOC 2	Management Regulators Customers Other	Customer Demand Due diligence GRC programs Oversight	Concerns regarding security, availability, processing integrity, confidentiality or privacy
SOC 3	Any users with need for confidence in service organization's controls	Marketing purposes; detail not needed	Seal and easy to read report on controls

# Which SOC Report Should Be Used?



Will report be used by service users and their auditors to plan/perform an audit of their financial statements?	Yes	SOC 1 Report
Will report be used by service users and/or stakeholders to gain confidence and place trust in a service organization's system?	Yes	SOC 2 or SOC 3 Report
Does the report need to be made generally available or is a seal needed?	Yes	SOC 3 Report

# Deciding Between SOC 2 and SOC 3 Reports



Do the service users have the need for/ability to understand the details of processing and controls at a service organization, the tests performed by the service auditor and results of those tests?

Yes

SOC 2 Report

No

SOC 3 Report



# Company Responsibilities

- **Although a process has been outsourced, the user organization is responsible for the accuracy and integrity of the financial data associated with the outsourced process.**





# Company Responsibilities

- **The User Organization must understand the design and operating effectiveness of internal controls at the Service Provider and how those controls interact with their own.**



# Company Responsibilities

- **A SOC report can be used to help reduce but not eliminate management's need to perform independent evaluation procedures of Service Provider's internal controls.**



# Assessing Usefulness of a SOC Report

## ● Consider:

- ✓ Service Auditor's Professional Reputation / Competency
- ✓ Scope of Report Relevancy
- ✓ Opinion and Exceptions
- ✓ User Control Considerations
- ✓ Gap Period





# Should I Request a SOC Report?

- **Consider requesting/producing a report if the vendor/your company:**
  - ✓ Processes financial transactions
  - ✓ Has physical or logical possession of systems
  - ✓ Has access to customer or employee personally identifiable information
  - ✓ Has access to confidential information
  - ✓ Controls availability of systems or data
  - ✓ Is regularly audited by customers



# Conclusion

- ✓ “SAS 70” reports were misused – AICPA created “SOC” reports to address market demands
- ✓ SOC 1= Internal Controls over Financial Reporting
- ✓ SOC 2 = security, availability, processing integrity, confidentiality or privacy
- ✓ SOC 3 = less detailed report + seal
- ✓ Consider requesting or producing a SOC report for outsourced functions

# Questions?



**Michael Hulet, CPA, CISA**

Principal at Perkins & Co

503-221-7533

[mhulet@perkinsaccounting.com](mailto:mhulet@perkinsaccounting.com)

Twitter: @PerkinsCo