Meet the New SOCs

UHY LLP
Certified Public Accountants

David Barton
Principal, UHY LLP

UHY LLP Certified Public Accountants

Objectives

- History
- SAS 70 Dirty Little Secret
- Why SAS 70 was eliminated
- New SOCs
- Differences between SAS 70 and SOC 1
- Differences between SOC 1, 2, 3
- When to use each

UHY LLP Certified Public Accountants

A history lesson

SAS 70 – April 1992, AICPA issues SAS 70 in response to pressure from service organizations that were being overwhelmed by audits.

- allowed one internal control review to be performed on service organizations to examine all of the areas required to meet SAS 55 requirements.
- resulting service auditor's report (aka SAS 70 report) can be distributed and relied upon by all of the financial statement auditors of the service organizations clients.

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

Original intent of SAS 70

Applicability of SAS No. 70, as Amended I-06

SAS No. 70, as amended, is not applicable to every service provided by a service organization. It is applicable only if the service is part of the user organization's *information system*. A service organization's services are part of an entity's information system if they affect any of the following:

- The classes of transactions in the entity's operations that are significant to the financial statements.
- The procedures, both automated and manual, by which the entity's transactions are initiated, recorded, processed, and reported from their occurrence to their inclusion in the financial statements.
- The related accounting records, whether electronic or manual, supporting information, and specific accounts in the financial statements involved in initiating, recording, processing and reporting the entity's transactions.
- How the entity's information system captures other events and conditions that are significant to the financial statements.
- The financial reporting process used to prepare the entity's financial statements, including significant accounting estimates and disclosures.

AICPA Audit Guide: Service Organizations: Applying SAS 70 as Amended

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

Original intent of SAS 70

Applicability of SAS No. 70, as Amended I-06

SAS No. 70, as amended, is not applicable to every service provided by a service organization. It is applicable only if the service is part of the user organization's *information system*. A service organization's services are part of an entity's information system if they affect any of the following:

- The classes of transactions in the entity's operations that are significant to the financial statements.
- The procedures, both automated and manual, by which the entity's transactions are initiated, recorded, processed, and reported from their occurrence to their inclusion in the financial statements.
- The related accounting records, whether electronic or manual, supporting information, and specific accounts in the financial statements involved in initiating, recording, processing and reporting the entity's transactions.
- How the entity's information system captures other events and conditions that are significant to the financial statements.
- The financial reporting process used to prepare the entity's financial statements, including significant accounting estimates and disclosures.

AICPA Audit Guide: Service Organizations: Applying SAS 70 as Amended

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

Applicability of SAS 70

I-10 There is a direct relationship between an entity's objectives and the internal control components it implements to provide reasonable assurance about their achievement. Ordinarily, *controls that are relevant to an audit pertain to the entity's objective of preparing financial statements that are fairly presented* in conformity with generally accepted accounting principles or a comprehensive basis of accounting other than generally accepted accounting principles **fn 1** including the management of risk that may give rise to risks of material misstatement in those financial statements.

AICPA Audit Guide: Service Organizations: Applying SAS 70 as Amended

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

Applicability of SAS 70

- Third party administrators
- Data Centers and co-location providers
- Payroll processors
- Pest control companies
- Print and Ship services
- A/P processing services
- Trust agencies
- Mortgage Servicers
- ASP and SaaS providers
- ISPs and Web Hosting companies
- Property management companies

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

Impact of Sarbanes-Oxley

- Fundamentally changed the way financial statement audits were conducted
  - Required auditor to have an understanding of ICFR
  - Could no longer overlook service organizations
- Increased demand for SAS 70 reports
  - Financial statement auditors requested
  - Became a checklist item for all service organizations

UHY LLP Certified Public Accountants

The Customer is always Right

- Largest publicly held companies must comply with SOX
- Auditors must have understanding of controls – SAS 70 = checklist item
- Procurement began qualifying service organizations based on availability of SAS 70

UHY LLP Certified Public Accountants

Additional Demand Increase

- Greater awareness of risk management and internal controls
- Heightened Regulatory environment
  - PCI
  - HIPAA
  - Gramm, Leach, Bliley
- Increase in outsourcing
- Board/Audit Committee
- Business requirement

UHY LLP
Certified Public Accountants

"SAS 70 Certified"

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

"SAS 70 Certified"

certified *Adjective*

1. holding or guaranteed by a certificate
2. To guarantee as meeting a standard[1]

- Certification implies a standard
- What standard?
- Who grants the certificate?

1 Collins Essential English Dictionary 2nd Edition 2006 © HarperCollins Publishers 2004, 2006

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

SAS 70's Dirty Little Secret

- What is the criteria for a SAS 70 audit?
- Who is responsible for description of controls?
  - the *service organization* is responsible for identifying and describing the controls that the auditor will render an opinion on.
  - the *service organization* writes the test!

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

SAS 70's Dirty Little Secret

Overall opinion for a SAS 70 Type II audit: accuracy, completeness, design, and operating effectiveness of the controls that are described *by the service organization*

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

SAS 70's Other Dirty Little Secret

Carve Out

"Acme, Inc. uses XYZ's Administration System for plan and participant recordkeeping and Anywhere Telecom to provide various information technology supports such as Internet Service Provider and firewall services. The accompanying description includes only those controls and related control objectives of Acme, Inc. and does not include the controls and related control objectives of XYZ's Administration System or Anywhere Telecom."

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

What was Wrong with SAS 70?

- Incorrectly applied
  - Data Centers
  - Colocation providers
  - Software providers
  - Pest Control Companies
- No standard criteria for ITGC
- Inconsistent quality
- Not consistent with International Standards

UHY LLP Certified Public Accountants

What was Wrong with SAS 70?

Inconsistent Quality:

- *CONTROL OBJECTIVE #6*
- Controls provide reasonable assurance that data integrity is maintained through various stages of processing in accordance with user specifications.

Controls Specified by ACME	Tests Performed by Big 4, LLP
The IT Director is solely responsible for maintaining all archive and backup systems. Reports are generated detailing job statistics and exceptions, if any, for daily backup procedures for each server. Media tapes are used to execute the backup procedures. Offsite storage is provided by Iron Mountain Data Services, Inc.	Inquired and reviewed EMCAS' archive and backup policies and procedures with the IT Director. Examined a sample of backup reports for successful completion of backup jobs. Verified the condition of the on-site media tapes. Examined acknowledgment receipts from the offsite storage provider.
Conclusion: No exception noted.	

UHY LLP Certified Public Accountants

RIP SAS 70

- SAS 70 was officially eliminated on June 15, 2011
- All Service Organization audits completed after June 15, 2011 must be performed using one of the new standards.

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

New SOCs – not SOX

- SOC 1 - Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting (SSAE 16)
- SOC 2 - Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy
- SOC 3 - Trust Services Report for Service Organizations

UHY LLP Certified Public Accountants

New standards for third party audits

- SOC 1 – SSAE 16 – intended for ICFR
- SOC 2 – based on pre-defined controls “principles”:
  - Security
  - Availability
  - Processing Integrity
  - Confidentiality
  - Privacy
- SOC 3 – Condensed and abbreviated SOC 2 report
  - Includes auditor opinion and Management’s assertion
  - AICPA seal can be displayed
  - General availability

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

SAS 70 vs. SOC 1

- Audit vs. Attestation
- No assertion vs. Management assertion
- Description of controls vs. System description
- No criteria vs. Suitable criteria

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

SAS 70 vs. SOC 1

- Management provides “system description”
- Still no standard criteria
- Procurement is in the process of re-writing policies to require SSAE 16 “certification”

UHY LLP Certified Public Accountants

"SSAE 16 Certified"

Google Apps and Google App Engine Get **SSAE-16** Certification **...**
With security as its main priority, Google has received a **SSAE 16** certification for both the Google Apps cloud productivity and collaboration suite and the **...**
siliconangle.com/.../google-apps-and-google-app-engine-get-s...

Fibernet Receives Type II SAS 70 Certification
Utah Business
"Recently, a new standard, **SSAE 16**, has emerged as an enhancement to the SAS **...** "We're already in preparations to receive certifications through **SSAE 16** in **...**

C7 Data Centers Completes **SSAE 16** Certification
Utah Business
by PR or News Wire Colocation and IT infrastructure provider C7 Data Centers, Inc. (C7) announced the completion of the **SSAE 16** audit certification for its **...**

THE NEXT LEVEL OF SERVICE

UHY LLP
Certified Public Accountants

New Standards

SOC Report Comparison

	Who Are the Users	Why	What
SOC 1℠	Users' controller's office and user auditors	Audits of f/s	Controls relevant to user financial reporting
SOC 2℠	Management Regulators Others	GRC programs Oversight Due diligence	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

THE NEXT LEVEL OF SERVICE

UHY LLP
Certified Public Accountants

When to use SOC 1, 2, 3

Will report be used by your customers and their auditors to plan/perform an audit of their financial statements?	Yes	SOC 1℠ Report
Will report be used by customers/stakeholders to gain confidence and place trust in a service organization's system?	Yes	SOC 2℠ or SOC 3℠ Report
Do you need to make report generally available or seal?	Yes	SOC 3℠ Report

UHY LLP
Certified Public Accountants

Differences between SOC 2 and 3

Do your customers 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

THE NEXT LEVEL OF SERVICE

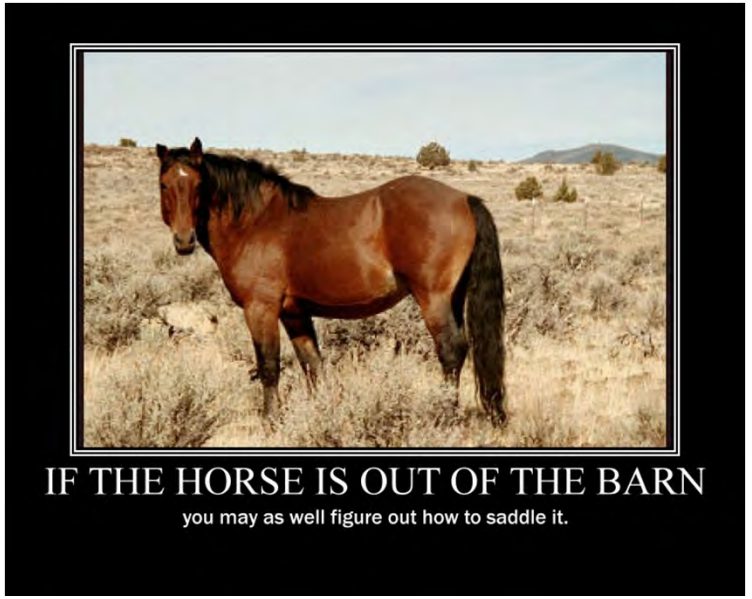
UHY LLP Certified Public Accountants

SOC 2 and 3 Criteria

- Over 120 individual controls criteria
- Focused on 4 key areas:
  - Policies
  - Communication
  - Procedures
  - Monitoring

THE NEXT LEVEL OF SERVICE

Why New Standards Won't Help



- SAS 70 "Brand"
- "SSAE 16 replaces SAS 70"
- SSAE 16 Certified
- Service Organization still specifies controls
- Quality is still questionable
- The Customer is Always Right

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

SSAE 16 Dirty Little Secret

Overall opinion for SSAE 16 Type II attestation:

accuracy, completeness, design, and operating effectiveness of the controls that are described *by the service organization* in the system description

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

Pop Quiz

- Your organization is publicly traded or has public debt
- You utilize a third party colocation facility for financial systems
- Which SOC report should you request?

(you may ask additional questions to get additional information)

UHY LLP Certified Public Accountants

Pop Quiz

- Your organization is publicly traded or has public debt
- You utilize a third party colocation facility for financial systems
- Which SOC report should you request?

- SOC 2 or SOC 3

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

Pop Quiz

- Your organization is publicly traded or has public debt
- They utilize a third party SaaS provider for financial systems
- Which SOC report should you request?

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

Pop Quiz

- Your organization is publicly traded or has public debt
- They utilize a third party SaaS provider for financial systems
- Which SOC report should you request?

- SOC 1 (SSAE 16)

UHY LLP Certified Public Accountants

Pop Quiz

- Your organization is publicly traded or has public debt
- They utilize a public cloud provider for development and testing of financial systems
- Which SOC report should you request?

UHY LLP Certified Public Accountants

Pop Quiz

- Your organization is publicly traded or has public debt
- They utilize a public cloud provider for development and testing of financial systems
- Which SOC report should you request?

- SOC 2 or N/A

THE NEXT LEVEL OF SERVICE

UHY LLP Certified Public Accountants

Additional Resources

- https://cloudsecurityalliance.org/
- http://www.aicpa.org/SOC/
- http://www.isaca.org

Questions?

David Barton, Principal
UHY LLP

Five Concourse Parkway
Suite 2430
Atlanta, GA 30328

678-602-4490

THE NEXT LEVEL OF SERVICE