

Bye-Bye SAS 70 ... Now What ?

David Hadley, CISA, CGEIT
CTO, Segmint, Inc.

Jeff Pershing, CISA, CISM, CISSP
Principal, Pershing Consulting, LLC

Overview / Agenda

- Introductions
- The Short Answer
- Why the change?
- History of the SAS 70
- SOC Reports (SAS70 rebooted)
- Trust Services Principals & GAPP
- Real-life examples
 - Segmint
 - Large Technology Service Provider
 - Third-party medical information provider to the US Government
- Questions/Discussion
- Wrap Up/Conclusion

SAS70

- In the beginning, the AICPA created the SAS70. The AICPA saw that the SAS70 was good and it was so. And then the AICPA rested . . .
 - For nearly 20 years
 - Okay, not quite . . . SAS78, SAS88, SAS94, . . .
 - Until . . .
- *“He’s dead, Jim . . . ”*
 - Leonard "Bones" McCoy

3

The Short Answer

- SAS70 is replaced by the SSAE16 (or SOC1)
 - Still only for ICFR
 - Still a limited distribution intended as a auditor to auditor communication
 - Except to the trained eye, it will be difficult to tell the difference
 - Still have Type I and Type II options
- SOC2 is a new option
 - Intended for subject matter “other” than ICFR
 - Intended for a wider audience, such as IT and Security Management (CIOs, CISOs, etc.)
 - Must use one or more of the Trust Services Principals as criteria (Security, Availability, Processing Integrity, Confidentiality, Privacy)
 - Also have Type I and Type II options
- SOC3 – Trust Services Report for Service Organization
 - General use report with very little detail (The “Good Housekeeping Seal of Approval”)
 - Must use one or more of the Trust Services Principals as criteria (Security, Availability, Processing Integrity, Confidentiality, Privacy)
 - SysTrust/WebTrust is now also a SOC3
- AT101 is another option (and it’s been around for quite a while)
 - SSAE16/SOC1, SOC2, and SOC3 are all performed in accordance with AT 101,

4

Let's back up . . . Why the need for a SAS70 anyway?

- Computers give rise to EDP – Electronic Data Processing
- Computers are very big and expensive (in the 60's, 70's, and 80's)
 - Okay, they're still expensive now . . .
- Let's share their use to be more efficient!
 - This sounds like a business opportunity!
 - Let's create a company to provide processing to several companies at once who can't afford their own
 - (Can anyone say, "cloud?")
- Auditor: How do I know my financial calculations are correct and you have good internal controls?
 - Service Provider: "Trust us!"
 - Auditor: "No, I will audit you. SAS55 says so. See you Monday. Here's my request list."
 - Service Provider: "Wait, I have hundreds of customers with auditors all saying the say thing!"

5

SAS70 – A brief history

- AICPA – American Institute of Certified Public Accountants
- SAS - Statement on Auditing Standards
- SAS 55 – Consideration of the Internal Control Structure in a Financial Statement Audit
 - Released in 1988
 - Created "death by auditing" for service providers
- SAS 70 – Service Organizations
 - Issues in 1992 as "Reports on the Processing of Transactions by Service Organizations", effective for reports issued March 31, 1993
 - One report to meet the needs of multiple user auditors
 - Amended by SAS 88 and renamed "Service Organizations"
- SAS70 amended several times by subsequent SAS
 - 1998 by SAS78 - "Consideration of Internal Control in a Financial Statement Audit: An Amendment to Statement on Auditing Standards No. 55"
 - 1999 by SAS88 – Title changed to "Service Organizations"
 - 2002 by SAS94 - The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit
 - 2002 by SAS98 - Omnibus Statement on Auditing Standards-2002
 - Other minor adjustments ("conforming changes") in 2006 by SAS105 & SAS106, and 2007 by SAS109 & SAS110

6

SAS70 – Abused!

- Sarbanes-Oxley Section 404
 - Required audit of ICFR, including ITGC
 - Specified COSO/CobIT as an acceptable frameworks
 - SAS 70, as amended by SAS 78, also used COSO
 - SAS 70 reports were provided a uniform format for third party reviews of Service Providers so that the description and disclosure of the service provider's processes and controls could be provided to customers and their auditors
 - *Bingo! We have a winner!*
- Intended for ICFR, but used for much more
 - To obtain assurance on controls regarding compliance and operations
 - E.g. Hosted Data Centers providing no financial reporting relevant services
 - SysTrust or AT 101 should have been used instead
 - SAS 70 grew in familiarity outside the auditing world (e.g. IT), but not necessarily well understood
 - *Are you "SAS70 Certified?"*

7

SOC Reports to the Rescue!

- ISAE 3402/SSAE16 (SOC1) for ICFR
 - International Standard on Assurance Engagements (ISAE) 3402 issued in December of 2009
 - AICPA issued SSAE No. 16 shortly afterwards as a US Standard in alignment with ISAE 3402
 - Drafted to help correct misuses of the SAS70
 - Minor differences between the two
- SOC2 for matters other than ICFR
 - Specifically, for Security, Availability, Processing Integrity, Confidentiality, and Privacy
- SOC3, similar to SOC2, but with a general use report
- All three based on AT101 (SSAE 16 becomes AT801)

8

SOC – What’s the same as SAS70?

- For the SOC1 - A lot! – Will look and feel familiar
- SOC1/SSAE16 and SOC2
 - Type I – Design only
 - Type II – Design and operating effectiveness

9

SOC - What’s different from SAS70?

- Attestation Standard vs. Auditing Standard
- Management Assertion
- Description of “System” vs. Controls
- Use of suitable criteria
- Suitability of design opinion
 - SAS70: point in time
 - SSAE16(SOC1)/SOC2: entire period
- Materiality
 - “deviations” (not exceptions)
- Use of Internal Audit
 - Must identify testing by IA in the report
- Opinion Format

10

BREAK

11

What is a “System”?

- TSP100 defines a “system” in footnote 1 as follows:
- A **system** consists of five key components organized to achieve a specified objective. The five components are 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 programmed and manual procedures involved in the operation of a system (automated and manual)
 - **Data**. The information used and supported by a system (transaction streams, files, databases, and tables)

12

Suitability of Criteria – AT101

- .24 Criteria are the standards or benchmarks used to measure and present the subject matter and against which the practitioner evaluates the subject matter.* Suitable criteria must have each of the following attributes:
 - *Objectivity* - Criteria should be free from bias.
 - *Measurability* - Criteria should permit reasonably consistent measurements, qualitative or quantitative, of subject matter.
 - *Completeness* - Criteria should be sufficiently complete so that those relevant factors that would alter a conclusion about subject matter are not omitted.
 - *Relevance* - Criteria should be relevant to the subject matter.
- .25 Criteria that are established or developed by groups composed of experts that follow due process procedures, including exposure of the proposed criteria for public comment, ordinarily should be considered suitable. Criteria promulgated by a body designated by the AICPA Governing Council under the AICPA Code of Professional Conduct are, by definition, considered to be suitable.
 - (I.e. Trust Services Principles)

13

SOC1 / SSAE16 Reports

- Designated to be used for “reporting on controls relevant to internal control over financial reporting (ICFR)”
- To be completed in accordance with Statement on Standards for Attestation Engagements (SSAE) No. 16
- SSAE 16 Audit Guide released early 2011
- Two report types:
 - SOC 1 Type I = SSAE 16 Type I Report
 - SOC1 Type II = SSAE 16 Type II Report
- Suitable Criteria
 - What is it??? (i.e. control objectives)
 - Where does it come from? (previous SAS70, App D. of guide, etc.)

14

SOC2 Reports

- Reports on Controls at a Service Organization over Security, Availability, Processing Integrity, Confidentiality, or Privacy
- Guide release in May 2011
- Report format designed to match the SSAE16
- Criteria is prescribed: Must use TSP 100 - Trust Services Principles

15

SOC3 Reports

- Similar to a SOC2
- Uses TSP100 – Trust Service Principles
- Primary Differences
 - Does not contain a description of the practitioner’s tests of controls and results of those tests
 - Is a general use report rather than a restricted use report

16

Attestation Standards Section 101

- Section provides a framework for attestation engagements that are completed by practitioners
- SOC 1, SOC2 and SOC3 reports completed in accordance with AT Section 101
- AT101 reports can align with regulatory constraints
 - AT601 Compliance Attestation

17

Reports Comparison

	SSAE16 (SOC 1)	SOC 2	SOC 3	Other Reports
GUIDANCE	AICPA Attest Standards (SSAE 16)	AICPA Attest Standards (AT101) Trust Services Principles	AICPA Attest Standards (AT101) Trust Services Principles	AICPA Attest Standards (AT101)
EXAMPLE PROJECTS	<ul style="list-style-type: none"> • Auditor to auditor opinion report for financial reporting controls • Audit entity meets definition of service organization • CPA firm responsible for the adequacy of the procedures 	<ul style="list-style-type: none"> • Opinion report on system security, availability, processing integrity and confidentiality/or privacy • Detailed like SOC1 • CPA firm responsible for the adequacy of the procedures 	<ul style="list-style-type: none"> • Opinion report on system security, availability, processing integrity and confidentiality/or privacy • Client description is not audited • CPA firm responsible for the adequacy of the procedures 	<ul style="list-style-type: none"> • Doesn't fall under SSAE 16 or Trust Services Principles • Reporting on the design of internal controls • CPA firm responsible for the adequacy of the procedures
REPORT DISTRIBUTION	<ul style="list-style-type: none"> • Report distribution to service organization users • Issued by licensed CPA 	<ul style="list-style-type: none"> • Intended for non-auditor audience (e.g., CIO) • Issued by licensed CPA 	<ul style="list-style-type: none"> • Intended for non-auditor audience (e.g., CIO) • General use report • Issued by licensed CPA 	<ul style="list-style-type: none"> • May be issued for general or restricted use • Issued by licensed CPA

Source: McGladrey & Pullen, LLP

18

The Trust Services Principals

- Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy (punts to GAPP)

19

Principles & Criteria

- Criteria organized around
 - Policies
 - Communications
 - Procedures
 - Monitoring
- Lots of redundancy
 - Security: The entity's security policies are established and periodically reviewed and approved by a designated individual or group.
 - Availability: The entity's system availability and related security policies are established and periodically reviewed and approved by a designated individual or group.
 - Processing Integrity: The entity's processing integrity and related security policies are established and periodically reviewed and approved by a designated individual or group.
 - Confidentiality: The entity's system confidentiality and related security policies are established and periodically reviewed and approved by a designated individual or group.
- Privacy is different – TSP100 defers to Generally Accepted Privacy Principles (GAPP)

20

Demonstration

- Trust Services Principles
- Comparison Matrix
- GAPP

21

Real-world Examples

22

Segmint & the AT101 Report

- Segmint Background
- Policies >> Programs >> Control Objectives >> Control Statements
 - Audit
 - Business Continuity
 - Software Development and Acquisition
 - Information Security
 - IT Operations
 - IT Risk Management
 - Vendor Management
- Why the AT101 over the SOC2?

23

Large Financial Services Integrated Technology Solutions Company

- Background
 - Technology Service Provider (TSP)
 - Clients include very small to very large FIs
 - Provides Services that provided access to FI data
 - Cash Management
 - Campaign
 - Status and Monitoring
 - No previous SAS70
- SSAE16? SOC2? Or something else?

24

Medical Information Provider to the DoD

- DoD Information Assurance Certification and Accreditation Process (DIACAP)
- Previously had SAS70
- Only one client – the DoD
- Why is an attestation report needed?
- Which one? SSAE16? SOC2? Something else?

25

Wrap Up

26

Questions ???

27

References and Sources:

- AICPA.org – Links to all current SAS and SSAEs, including AT101 and AT801(SSAE16)
 - <http://www.aicpa.org/Research/Standards/AuditAttest/Pages/SAS.aspx>
 - <http://www.aicpa.org/Research/Standards/AuditAttest/Pages/SSAE.aspx>
- AICPA Guides (available in a variety of formats for purchase)
 - SOC1: http://www.cpa2biz.com/AST/Main/CPA2BIZ_Primary/AuditAttest/IndustryspecificGuidance/PRDOVR~PC-0127910/PC-0127910.isp
 - SOC2: http://www.cpa2biz.com/AST/Main/CPA2BIZ_Primary/AuditAttest/IndustryspecificGuidance/PRDOVR~PC-0128210/PC-0128210.isp
- Brief History of all SAS with links to full text for many
 - [http://en.wikipedia.org/wiki/Statements_on_Auditing_Standards_\(USA\)](http://en.wikipedia.org/wiki/Statements_on_Auditing_Standards_(USA))
- Downloadable copy of Trust Services Principal , Criteria, and Illustrations (TSP sec. 100)
 - <http://www.webtrust.org/item27806.doc>
- Generally Accepted Privacy Principles (GAPP) – Site has many GAPP resources available for free download
 - <http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/Pages/default.aspx>

28

Thank You!!!

29

Extra Slide - Review vs. Examination

- Examination
 - provide a high level of assurance
 - the practitioner's objective is to accumulate sufficient evidence to restrict attestation risk to a level that is appropriately low
 - Practitioner's conclusion expressed in the form of an *opinion*
- Review
 - provide a moderate level of assurance
 - objective is to accumulate sufficient evidence to restrict attestation risk to a moderate level
 - Practitioner's conclusion expressed in the form of *negative assurance*
- Agreed-upon procedures engagements (AT201)
 - Procedures performed as agreed
 - Report results as “findings”
- SOC1/2/3 are Examinations

30