Deloitte.

The Changing SAS 70 Landscape

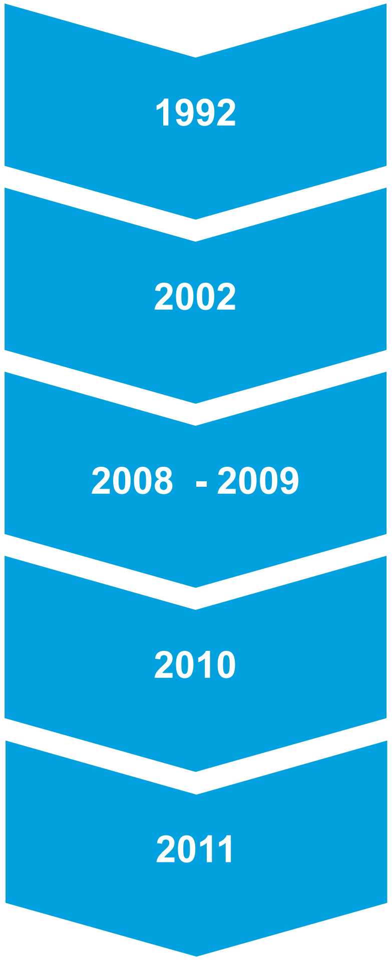
Dan Hirstein – Director
Rebecca Goodpasture – Senior Manager
Deloitte & Touche LLP
January 13, 2011

© 2010 Deloitte & Touche LLP

Table of Contents

© 2010 Deloitte & Touche LLP

A Short History of SAS 70



1992

Development of SAS 70 by the AICPA was originally designed as an **auditor to auditor communication** over specified control objectives related to specific business functions; however, SAS 70 (and it's successors) has evolved and reports are now being viewed more broadly.

2002

Passage of the Sarbanes-Oxley Act of 2002 leads to much **wider use of SAS 70**. SAS 70's have tended to migrate from their original intended use(financial controls) to a more pervasive view of the organization (operational controls).

2008 - 2009

Because there is no global standard, IAASB begins development of international standard on service organizations and the AICPA SAS 70 task force begins redrafting SAS 70.

2010

The IAASB issued ISAE 3402 as the global standard and the AICPA issued SSAE 16 to replace SAS 70.

2011

For examination periods ending on or after June 15, 2011, service auditors are required to comply with either ISAE 3402 or SSAE 16.

© 2010 Deloitte & Touche LLP

ISAE 3402 and SSAE 16 - Overview

- The new standards by the IAASB and AICPA are not aimed at overhauling how an engagement to report on controls at a service organization is performed. Rather, they have been drafted to meet the demands of the current market environment and to fit into the modern framework of assurance standards.
- While the standards drafted by the IAASB and AICPA are not significantly different from each other, nor from the present standard, they do present some changes from SAS 70 that may prove challenging for some service organizations.

- Effective Date – Periods ending on or after June 15, 2011. Early adoption allowed and expected for some organizations
- Criteria is specific to internal control over financial reporting (no operational controls)
- AICPA Practitioner Guide issued in 2010 is usable for both standards and for practitioners and service organizations alike
- Allows for the use of the framework/guidance to perform engagements under another standard (e.g., AT101)

Can combine both standards into one report – but have to then comply with the least common denominators of both

© 2010 Deloitte & Touche LLP

Changes from SAS 70

Management's Assertion: The most significant change to SAS 70 is the requirement in both ISAE 3402 and the SSAE that management of the service organization provide a written assertion attesting to the fair presentation, design, and operating effectiveness of controls (in a Type 2 report).

SAS 70	SSAE 16 / ISAE 3402
SAS 70 requires that management provide a letter that includes written representations that controls are suitably designed, or that they are suitably designed and operating effectively. However management was **not required to provide a written assertion** to the design and effectiveness of controls. .	Management will be required to **provide a written assertion** in addition to continuing to provide a representation letter, even though the service auditor will continue to report on the subject matter (i.e., whether controls are fairly presented, suitably designed and implemented, and (in a Type 2 report) operating effectively). If a service organization is using the inclusive method then the subservice organization also needs to provide a written assertion to be included as part of either the description of the system or as a separate document included within the report.

© 2010 Deloitte & Touche LLP

Changes from SAS70 – Management's Assertion

- In order to provide a written assertion, management will need to have a reasonable basis for making the assertion, which may include developing their own processes to support the assertion if such processes are not already in place.

- Management is required to:

  - Select suitable criteria, which will be used to prepare its description of the system as well as to evaluate whether controls were suitably designed (Type 1 report) or suitably designed and operating effectively (Type 2 report).

  - Identify the risks that threaten the achievement of the control objectives stated in the description.

© 2010 Deloitte & Touche LLP

Changes from SAS70 – Management’s Assertion (con’t)

- Service organizations that do not already have extensive processes to monitor and evaluate their controls may face significant challenges:
  - For example, if the service organization relies on controls at a subservice organization and management elects to use the inclusive method (that is, management’s description of the service organization’s system includes controls at the subservice organization), management will also need to determine whether controls at the subservice organization are suitably designed or suitably designed and operating effectively.
  - In order to make this determination and to support their own assertion, management of the service organization would need to obtain a written assertion from management of the subservice organization. Service organizations should initiate discussions with their subservice organizations soon in order to avoid difficulties in obtaining these assertions when the new standards become effective.

© 2010 Deloitte & Touche LLP

Changes from SAS 70

One to One Reporting

SAS 70	SSAE 16 / ISAE 3402
One to One Reporting is accepted under the existing standard.	One-to-one reporting, where the service organization did not design the controls, is **not applicable** under the new standard. If the service organization did not design the controls there is no ability for them to provide an assertion, therefore one-to-one reporting in this scenario would not be appropriate.

© 2010 Deloitte & Touche LLP

Changes from SAS 70

Restriction of Report Use

SAS 70 / SSAE 16	ISAE 3402
The service auditor report includes a statement restricting use of the report to management of the service organization, user entities of the service organization's system, and user auditors.	Report required to state that it is only intended for user entities and their auditors, **but may also include restrictive use language**.

Changes from SAS 70

Exceptions - Both the SSAE and ISAE 3402 require the service auditor to investigate the nature and cause of any deviations identified. However, the SSAE indicates that if the service Auditor becomes aware that the deviations resulted from intentional acts by service organization personnel, the service auditor should assess the risk that the description of the service organization's system is not fairly presented and that the controls are not suitably designed or operating effectively. The ISAE is silent on this requirement, but Deloitte does not believe this means that an intentional act would be ignored.

SAS 70 / SSAE 16	ISAE 3402
Does not enable a service auditor to conclude that a deviation identified when performing tests of controls involving sampling is not representative of the population from which the sample was drawn — all exceptions are disclosed in the report. .	Enables a service auditor to conclude that a deviation identified when performing tests of controls involving sampling is **isolated**.

© 2010 Deloitte & Touche LLP

Changes from SAS 70

Subsequent Events

SAS 70 / SSAE 16	ISAE 3402
Service auditor to consider disclosing subsequent events in the opinion, if not included in the description of the system, so users are not misled in addition to disclosure of events that could impact their opinion. .	Limits the service auditor’s disclosure to those events that could impact their opinion.

© 2010 Deloitte & Touche LLP

Changes from SAS 70

Use of Internal Audit

SAS 70	SSAE 16	ISAE 3402
Use of internal audit is allowed, however, no disclosure of tests performed by internal audit.	Continues to allow for use of internal audit, however, when using the internal audit function tests performed by internal audit are disclosed as well as service auditor tests of internal audit work.	**No provision for use of IA for direct assistance – however, likely to be adopted.**

© 2010 Deloitte & Touche LLP

Changes from SAS 70

Evidence Obtained in Prior Audits

SAS 70	SSAE 16 / ISAE 3402
A service auditor may use evidence from prior service auditor’s engagements to reduce the nature, timing, and extent of the tests of operating effectiveness.	Evidence obtained in prior engagements about the satisfactory operation of controls in prior periods does **not provide** a basis for a reduction in testing, even if it is supplemented with evidence obtained during the current period. In instances where prior deviations existed, it may, however, increase the extent of testing performed in the current period.

© 2010 Deloitte & Touche LLP

Notable Similarities with SAS 70

Consideration	Similarity
Control Objectives	Management to specify control objectives
Control Design	Requirement for management to design and implement controls that achieve the control objectives
User Control Considerations	Complete disclosure of complementary user entity controls (formerly UCCs).
Sub-Servicer Approach	Carve out and Inclusive method of reporting options for subservice organizations
Representations	Management to provide representation letter
Report Restrictions	Reports are for restricted use only
Additional Information	Additional information may be included (Section 4 of reports)

© 2010 Deloitte & Touche LLP

Notable Differences (Between ISAE 3402 and SSAE 16)

SSAE 16	ISAE 3402
Use of Report: Report required to specifically state that it is restricted to the intended users	Report required to state that it is only intended for user entities and their auditors, but may also include restrictive use language
Intentional Acts: Service auditor considers impact of intentional acts on the report	Silent on this requirement, but does not mean service auditor would do nothing
Use of Internal Audit: Provides for use of Internal Audit in direct assistance and using the Internal Audit (IA) function's tests	No provision for use of IA for direct assistance – however, likely to be adopted
Subsequent Events: Service auditor to consider Type 2 subsequent events after the report date	Does not require auditor to consider events after the report date that do not impact the examination period
Reporting: All deviations are reported	Enables a service auditor to conclude a deviation is an anomaly

Which Standard (SSAE 16 or ISAE 3402) should you follow?

- In many cases, the determination of whether to follow the standards of ISAE 3402 or the SSAE will be clear. For example, service auditors that are engaged to report on controls of a service organization located in the U.S. will need to apply the standards of the SSAE.

- However, with the continuing globalization of business, many service organizations have operations and/or customers within as well as outside the U.S. In these cases, the determination of which standard to use may not be as clear. Many may wish to consult with their auditor to assist in the decision. Due to the efforts of the AICPA to converge the SSAE with ISAE 3402, the two standards are fairly similar. Still, a global service organization that has a widespread customer base may wish to have an examination performed under both sets of standards.

© 2010 Deloitte & Touche LLP

Questions for Service Organizations

- Which standard, SSAE or ISAE 3402, should be used by the service auditor to meet the needs of my customers?
- Should we early adopt the new standards or wait until they are required?
- What additional testing and/or monitoring processes will we need to implement so that we can support our assertion?
- Which members of management will be responsible for providing the assertion?
- How will the new standards affect our service organization and our service auditor?
- How should we educate our user organizations (and subservice organizations) about the changes and our approach to meeting them?
- Is the carve-out method or inclusive method of reporting of our subservice organizations the best method for us? Would we be able to obtain an assertion from them if we choose to use the inclusive method?
- Will we need to refine user contracts to accommodate adoption of the new standard?

© 2010 Deloitte & Touche LLP

USING SSAE 16 AS A MODEL TO REPORT ON NON-ICFR (SOC 1, SOC 2, SOC 3)

Copyright © 2010 Deloitte & Touche LLP. All rights reserved.

Using SSAE 16 as a Model to Report on non-ICFR

- The focus of SSAE 16 is on controls at service organizations that are relevant to **the user entities' internal control over financial reporting**
  - Paragraph 2 states that "*The **guidance herein also may be helpful** to a practitioner performing an engagement under AT section 101, Attest Engagements (AICPA, Professional Standards, vol. 1), to report on controls at a service organization… **other than those that are likely to be relevant to user entities' internal control over financial reporting** …….*"

- Currently, management of a user entity has limited options for obtaining detailed information about the effectiveness of controls at the service provider
  - Perform tests at the service provider using its internal auditors or others
  - Rely on the work performed by the service provider's internal audit function by inspecting the internal audit department's working papers
  - Engage a firm to perform procedures to evaluate the controls
  - Obtain the service provider's SAS 70 report, if available, and project the results of test of controls over ICFR to other objectives of internal control

© 2010 Deloitte & Touche LLP

Background

To provide the framework for CPAs to examine controls and to help management understand the related risks, the AICPA is establishing three **Service Organization Control (SOC) reporting options (SOC 1, SOC 2 and SOC 3 reports).**

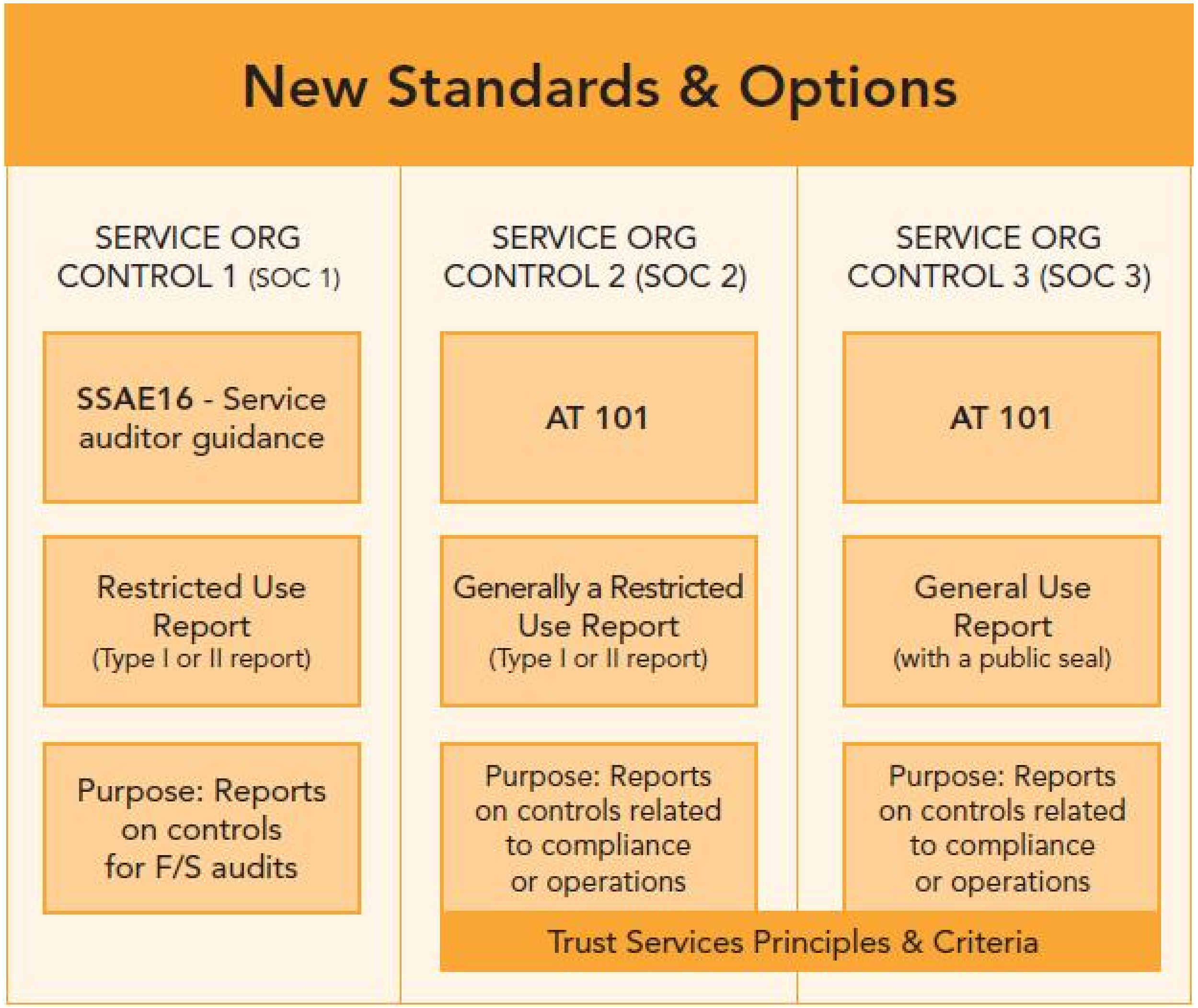
- **SOC 1 engagements are performed in accordance with Statement on Standards for Attestation Engagements (SSAE) 16, Reporting on Controls at a Service Organization. SOC 1 reports focus solely on controls at a service organization that are likely to be relevant to an audit of a user entity's financial statements.**

- **SOC 2 and SOC 3** engagements address controls at the service organization that relate to operations and compliance and specifically address one or more of the following five key system attributes:

- **Security -** The system is protected against unauthorized access (physical and logical).
- **Availability -** The system is available for operation and use as committed or agreed.
- **Processing integrity -** System processing is complete, accurate, timely and authorized.
- **Confidentiality –** Info designated as confidential is protected as committed or agreed.
- **Privacy -** Personal information is collected, used, retained, disclosed and disposed of in conformity with the commitments in the entity's privacy notice, and with criteria set forth in (GAPP).

© 2010 Deloitte & Touche LLP

Overview



New Standards & Options

SERVICE ORG CONTROL 1 (SOC 1)	SERVICE ORG CONTROL 2 (SOC 2)	SERVICE ORG CONTROL 3 (SOC 3)
SSAE16 - Service auditor guidance	AT 101	AT 101
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 & Criteria	Trust Services Principles & Criteria

Image Source: AICPA: Service Organization Controls Managing Risks by Obtaining a Service Auditor's Report

© 2010 Deloitte & Touche LLP

SOC 2 vs SOC 3

- The key difference between a SOC 2 report and a SOC 3 report is that a SOC 2 report, which is generally a restricted-use report, contains a detailed description of the service auditor’s tests of controls and results of those tests as well as the service auditor’s opinion on the description of the service organization’s system.

- A SOC 3 report is a general-use report that provides only the auditor’s report on whether the system achieved the trust services criteria **(no description of tests and results or opinion on the description of the system**). It also permits the service organization to use the SOC 3 seal on its website.

© 2010 Deloitte & Touche LLP

Comparison of Reports

	SOC 1	SOC 2	SOC 3
Under what professional standard is the engagement performed?	SSAE No. 16, *Reporting on Controls at a Service Organization*	AT 101, *Attestation Engagements*	AT 101, *Attestation Engagements*
What is the subject matter of the engagement?	Controls at a service organization relevant to user entities internal control over financial reporting.	Controls at a service organization relevant to security, availability, processing integrity confidentiality, or privacy. If the report addresses the privacy principle, the service organization's compliance with the commitments in its statement of privacy practices.	Controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy If the report addresses the privacy principle, the service organization's compliance with the commitments in its statement of privacy practices.
Who are the intended users of the report?	Auditor's of the user entity's financial statements, management of the user entities, and management of the service organization.	Parties that are knowledgeable about the service organization.	Anyone

© 2010 Deloitte & Touche LLP

Comparison of Reports (continued)

	SOC 1	SOC 2	SOC 3
What is the purpose of the report?	To provide information to the **auditor** of a user entity's financial statements about controls at a service organization that may be relevant to a user entity's **internal control over financial reporting.** It enables the user auditor to perform risk assessment procedures, and if a type 2 report is provided, to assess the risk of material misstatement of financial statement assertions affected by the service organization's processing.	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 that may affect user entities' **security, availability, processing integrity, confidentiality or privacy.** A type 2 report that addresses the privacy principle, also provides a CPA's opinion about the service organization's compliance with the commitments in its statement of privacy practices.	To provide **interested parties** with a CPA's opinion about controls at the service organization that may affect user entities' **security, availability, processing integrity, confidentiality, or privacy.** A report that addresses the privacy principle, also provides a CPA's opinion about the service organization's compliance with the commitments in its privacy notice.

© 2010 Deloitte & Touche LLP

Comparison of Reports (continued)

	SOC 1	SOC 2	SOC 3
What are the components of the report?	A description of the service organization’s system. A service auditor’s report that contains an opinion on the fairness of the presentation of the description of the service organization’s system, the suitability of the design of the controls, and in a type 2 report, the operating effectiveness of the controls. In a type 2 report, a description of the service auditor’s tests of the controls and the results of the tests.	A description of the service organization’s system. A service auditor’s report that contains an opinion on the fairness of the presentation of the description of the service organization’s system, the suitability of the design of the controls, and in a type 2 report, the operating effectiveness of the controls. In a type 2 report, a description of the service auditor’s tests of controls and the results of the tests. If the report addresses the privacy principle, the service auditor’s opinion on whether the service organization complied with the commitments in its statement of privacy practices. In a type 2 report that addresses the privacy principle, a description of the service auditor’s tests of the service organization’s compliance with the commitments in its statement of privacy practices and the results of those tests.	A service auditor’s report on whether the entity maintained effective controls over its system as it relates to the principle being reported on i.e., security, availability, processing integrity, confidentiality, or privacy, based on the applicable trust services criteria. If the report addresses the privacy principle the service auditor’s opinion on whether the service organization complied with the commitments in its statement of privacy practices.

© 2010 Deloitte & Touche LLP

Potential Uses

- Cloud computing - On-demand network access to a shared pool of configuarable computing resources, for example, networks, servers, storage, applications, and services

- Logical security management - Managing access to networks and computing systems for user entities

- Financial services customer accounting - Processing financial transactions on behalf of customers of a bank or investment company

- Contact center for customer service - Providing customers of user entities with on-line or telephonic post sales support and service management

- Sales force automation - Providing and maintaining software to automate business tasks for user entities that have a sales force

- Health care claims management and processing. - Providing medical providers, employers, and insured parties of employers with systems that securely and confidentially support the processing of medical records and related health insurance claims

© 2010 Deloitte & Touche LLP

Making the Right Choice

In summary, to determine the most appropriate SOC report for your purposes, a service organization should:

Understand the needs of user entities:

- Are they focused on internal control over financial reporting? Then a SOC 1 report is most appropriate.
- Are key compliance and operational controls (such as those related to security, availability, processing integrity, confidentiality or privacy) of primary interest? Then a SOC 2 or SOC 3 report may be most appropriate.

Understand the best communication mechanism for your users:

- Are they in need of detail about your systems and processes? Then a SOC 1 or SOC 2 report may be most appropriate.
- Will the posting of a summary report/seal suffice? Then a SOC 3 report may be most appropriate.

© 2010 Deloitte & Touche LLP

SOC Reporting Summary

- By helping to increase customer trust and helping customers to address their risk and governance concerns, these reports provide value to service organizations — but it’s important to understand the unique aspects of what the SOC report offers and match those aspects to user needs.

© 2010 Deloitte & Touche LLP

QUESTIONS

© 2010 Deloitte & Touche LLP

Deloitte.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

Member of
Deloitte Touche Tohmatsu

© 2010 Deloitte & Touche LLP