Deloitte.

Service Organization Control (SOC) Reports

Transitioning from SAS 70 to SSAE 16

Deloitte & Touche LLP

Agenda

- Overview
- SAS 70/SSAE 16 Historical Perspective
- The New Framework Under SSAE 16 (SOC 1)
- Impact of Change
  - Risk Management / Internal Audit Groups
  - Users & Management
- Other Service Organization Control Reports
- Questions

SAS 70 / SSAE 16
Historical Perspective

Overview

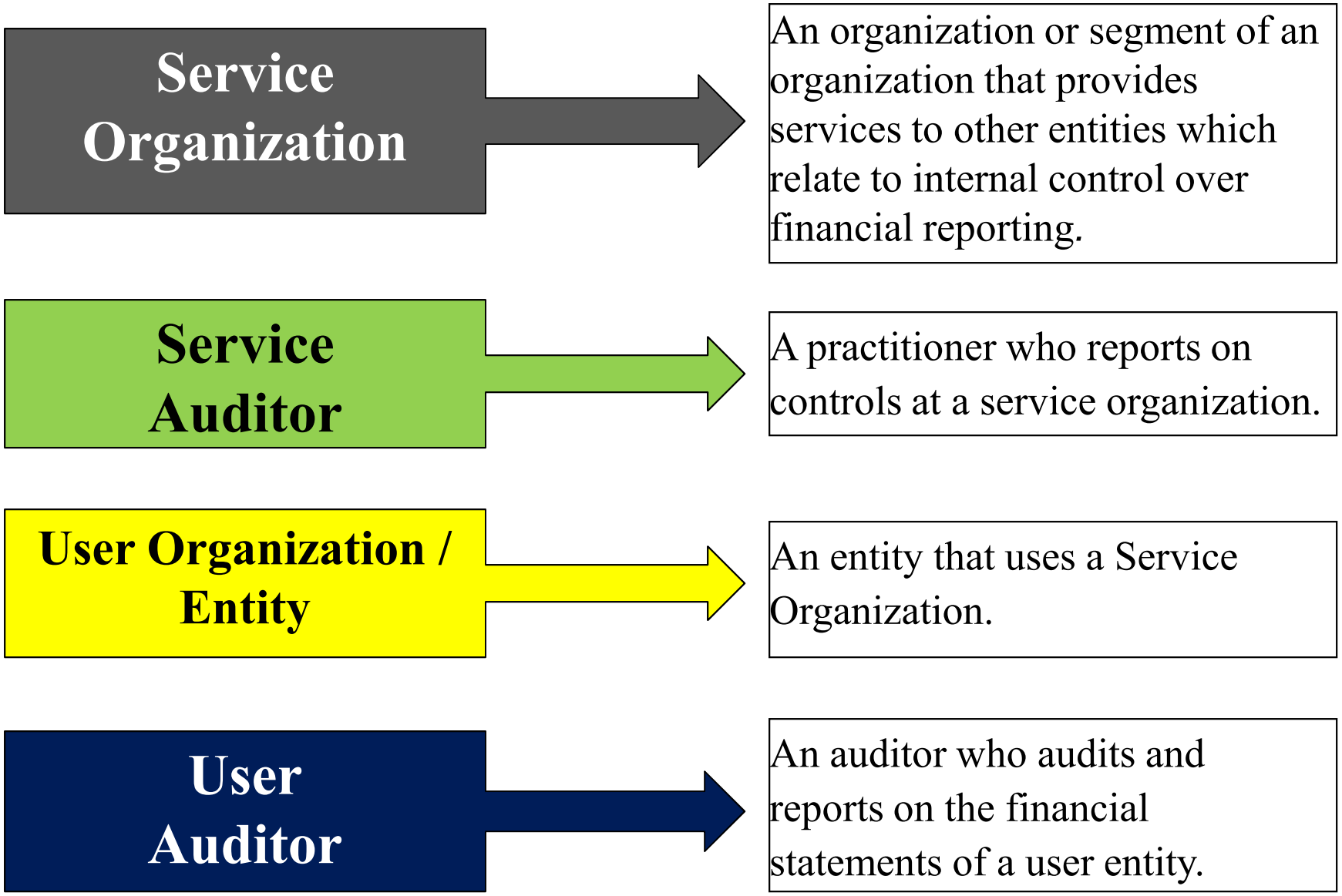
- What is a SAS 70/SSAE 16 report?

  A report that a service organization (*investment adviser/prime broker*) can provide to its user organizations (*investors/funds*) that outlines its control environment and whether those controls were designed and operating effectively over a period of time.

- New Standards represent the **first significant modifications** since SAS 70 was issued nearly two decades ago.
  - The American Institute of Certified Public Accountants (AICPA) approved the Statement on Standards for Attestation Engagements (**SSAE 16**)
  - International Auditing and Assurance Standards Board (IAASB) issued the new International Standard on Assurance Engagements (**ISAE 3402)**, Assurance Reports on Controls at a Third Party Service Organization

  - The new standards became effective for Service Auditor's reports for periods ending on or after June 15, 2011.

SSAE16 Terminology



Purpose of SAS 70 / SSAE 16 Report

- Facilitated auditor to auditor to communication allowing User Auditors with a basis to reduce control risk
- Provided a structure for describing a service organization's controls around services provided
- Avoided redundant auditing of service organizations

Key Issue: SAS 70 was really an auditing standard and was intended to be an auditor-to-auditor communication vehicle – however, it became to be viewed more broadly

Reasons for Change

Reasons for Change

- Need for greater international consistency
- Misunderstandings, Misapplications, and Misuses of SAS 70
- Software as a Service (“SAAS”), Cloud Computing, etc.

Reasons for Change:
Common SAS 70 Misunderstandings

SAS 70 reports were used to:

→ Report on controls related to compliance requirements, such as HIPAA.

→ Report on operational matters, such as availability, confidentiality, privacy, and processing integrity.

Although contributing to some misunderstandings about SAS 70 reports, the AICPA has recognized the growing need for assurance in these areas.

Misapplications/misuses of SAS 70 not only contributed to the need for a change that more clearly reinforced the financial reporting purpose, but also . . .

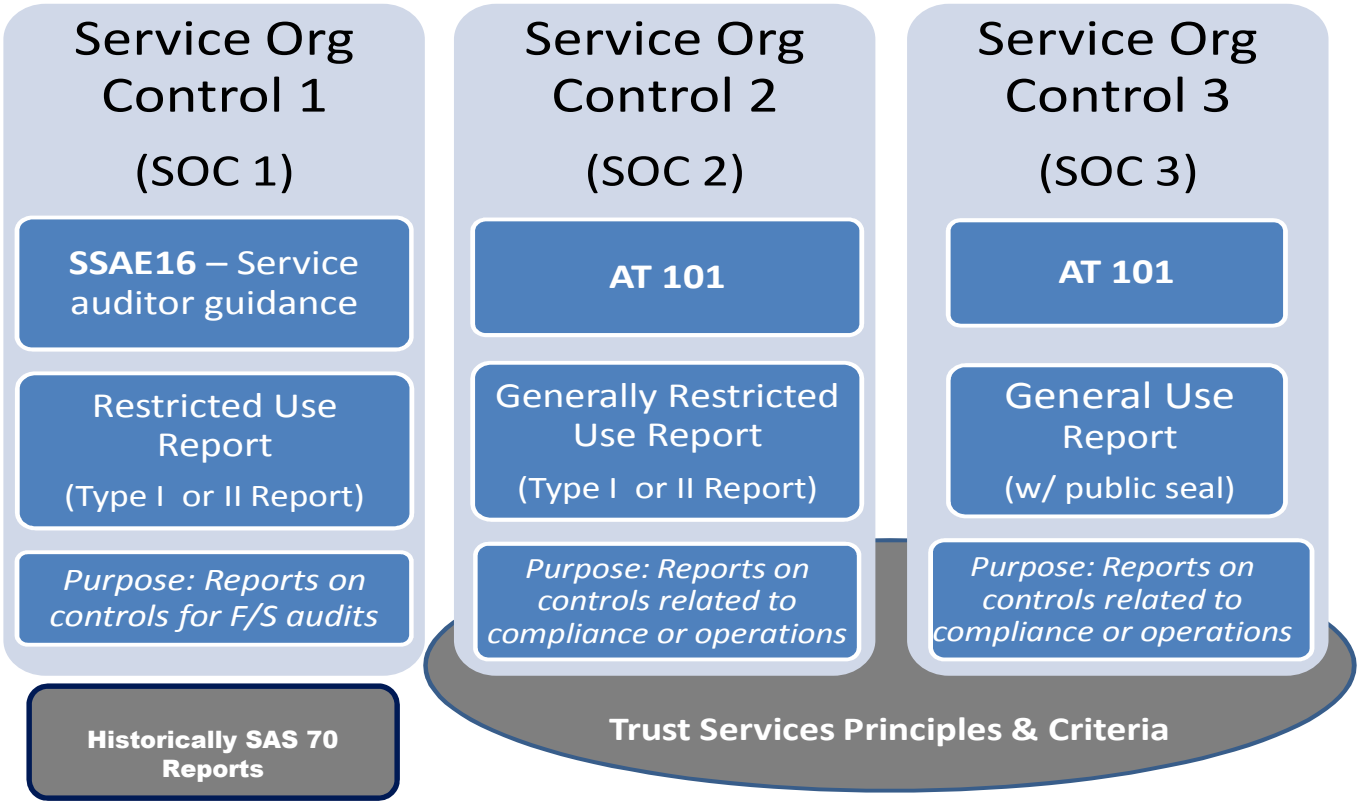
. . . Highlighted the need for more widely recognized and understood reporting options for CPAs to provide assurance regarding compliance and operational areas.

The New Framework

The New Framework

AICPA Service Organization Control (SOC) Reports

New Standards & Options



SOC 1 vs. SAS 70 Key Changes

Change	Result of the Change
1. Form of Standard	- Auditing Standard to an Attest Standard
2. Applicability of Report	- Specific to internal control over financial reporting
3. Management is required to provide a written assertion	- Management needs to have a basis to support their assertion
4. Identify risks that threaten the achievement of control objectives	- Management's responsibility to identify risks and include them in the evaluation of the design of controls and development of control objectives.
5. Service Auditor required to assess suitability of criteria	- Management needs to select suitable criteria to prepare description of systems and to evaluate whether controls have been designed, implemented and operating effectively.
6. Type 2 Report to cover a period for D&I, rather than point in time	- The opinion will now include coverage throughout the period for design (new), implementation (new), and operating effectiveness.

SOC 1 vs. SAS 70 Key Changes

Change	Result of the Change
7. Cannot use prior-year evidence to conclude on operating effectiveness of controls	- Auditor may not reduce tests of controls below the minimum standards (AU350) based on the results from the prior year.
8. Clearly identify work performed by Internal Audit function in description of tests of controls	- Description of tests of operating effectiveness needs to include description of Internal Audit's work and Service Auditor's procedures over Internal Audit's work (not applicable for direct assistance)
9. Service Auditor to investigate the nature and cause of any deviations and whether these were caused by intentional acts. Cannot disclaim deviation as isolated.	- Previous standard allowed disclaiming of deviations as isolated incidents. - New consideration of intentional acts
10. Subservice organizations are required to provide a similar assertion when the inclusive method is used	- Assertion will be included in the report - Inclusive method only - Continues to require a management representation letter as well

Frequently Asked Questions

Management's written assertion

- The Management Assertion can be included as a separate section of the report, or part of the description of the system (narrative section). It is not included with the Auditor's opinion.

- There is no requirement for the assertion to be signed
  - If signed, it **may be signed** by a member of management (e.g. CFO),
  - signed as the service organization

The majority of assertions issued to date have been signed by a member of management which have been included within a new section.

- Typically on client's letterhead

Sample of Management Assertion (Excerpt)

We have prepared the description of XYZ Service Organization's [*type or name of] system* (description) for user entities of the system during some or all of the period [*date] to [date], and their* user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements. **We confirm, to the best of our knowledge and belief, that**

a. *the description fairly presents the [type or name of] system made available to user entities of the* system during some or all of the period [*date] to [date] for processing their transactions [or identification of the function performed by the system]. The criteria we used in making this assertion* were that the description

b. *the description includes relevant details of changes to the service organization's system during the period covered by the description when the description covers a period of time.*

c. *the controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period [date] to [date] to achieve those control objectives. The criteria we used in making this assertion were that …*

Page 157 (.A71) of AICPA SSAE 16 Guide

How can Risk Management / Internal Audit Help?

Performing a Risk Assessment: Identifying the risks that threaten the achievement of the control objectives stated in the description.

Supporting the Assertion: Link Risk Management / Internal Audit's testing, reports, and results to the risk assessment; this documentation can be leveraged by Management.

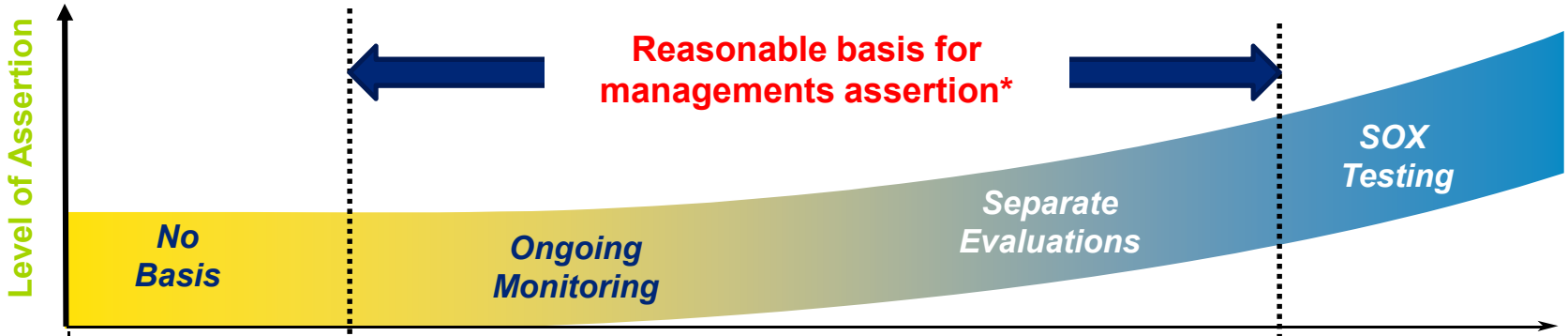
Reconfirming the Control Objectives: Confirm that control objectives are specific to internal control over financial reporting.

Monitoring of Third Parties: Assist management with identifying and including oversight controls within the SSAE 16 report for those subservice organizations "carved out" of the SSAE 16 report.

Engagement Execution: Provide the external auditor with risk management / internal audit reports and/or test plans to help identifiy areas of leveage; assist with retreiving updates to the report and/or testing documentation

Support for the *Assertion*

Examples of activities to support management's assertion



Example Procedures	• Service auditor performs testing and issues report	• Management reporting and other oversight activities • Management risk assessment • Review of exception reports • Oversight of subservice orgs	• Internal Audit testing/monitoring • Independent regulatory exams • Independent risk/compliance assessments	• Management or independent assessment of operating effectiveness
Supporting Documentation	• None	• Management monitoring documentation • Management risk assessment documentation • Sub-certifications	• Regulatory reporting • Internal Audit reporting • Independent risk assessment results	• Testing evidence for the operating effectiveness

* A combination of ongoing monitoring and separate evaluations will usually help ensure that internal control maintains its effectiveness over time.

Sample Template - Management's Risk Assessment

This is an example template for documenting management's risk assessment using a sample control objective:

User Entities financial statements assertion	Control Objective	Financial reporting related?	Risk Statements that threaten the achievement of the control objective	Control activity in place to mitigate identified risk	Assertion satisfied by the control activity	Design and operating effectiveness assessment
Investments - accuracy, completeness and timeliness	**Trade Capture** Controls provide reasonable assurance that transactions are received from an authorized source and recorded accurately, completely and in a timely manner.	Yes (Should be included in the SSAE 16 report)	Transactions may not be recorded accurately, completely and in a timely manner.	Position and trade files are provided by custodians. A position reconciliation is performed within the system comparing system calculated position balances to position balances provided by custodians. Inconsistencies found during position reconciliations are researched and resolved.	Accuracy, Complete-ness, Timeliness	Determine approach to design and operating effectiveness assessment using existing processes and/or identify new processes to support management's assertion. (e.g., Internal audit procedures, monitoring controls, risk management oversight, etc.)

What are the Key Changes for Management?

Key Change for Management

- Management is now including an assertion within the SSAE 16 report
    - Expectation of support from the process owners; assisting with the basis for assertion
- Exceptions identified within report may potentially increase; questions may arise from clients. Excerpt from Assertion:

    The controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period December 1, 20X0, to November 30, 20X1, to achieve those control objectives.

What is the Impact to User & their Auditors?

Appearance of the Report

The Appearance and the use of the Report is mostly unchanged

Confirmation of Scope

The AICPA has provided suggested areas and control objectives for certain organizations, for example:

- Investment Manager
- Transfer Agent
- Payroll

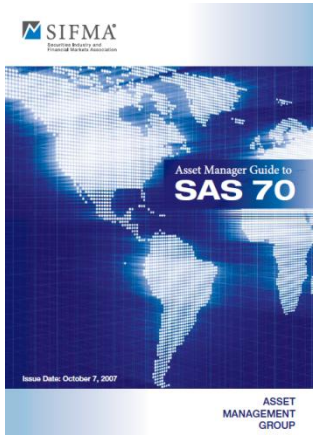
Potential Increase to the number of Reported Exceptions –

Exceptions to be reported as “No Exceptions Noted” as opposed to be previously to “No *Relevant* Exceptions Noted”. Materiality is not applied when reporting the results of tests of controls for which deviations have been identified.

Industry View on Scope

Securities Industry and Financial Markets Association's *("SIFMA")* Asset Manager's Guide to SAS 70

Investment advisers	• New account set-up and maintenance • Security set-up and maintenance • Contributions/distributions • Trading (Order Capture, Compliance, Confirmation/Affirmation/Settlement) • Pricing • Investment income • Corporate actions • Custodial reconciliations • Client reporting



SEC's Custody Rule for Advisers

SEC Custody Rule for Advisers w/ Custody	• Client account setup and maintenance, • Authorization and processing of client transactions, • Security maintenance and setup, • Processing of income and corporate action transactions, • Reconciliation of funds and securities to depositories and other unaffiliated custodians, • Client reporting.

Industry View – Broker/Dealer

Change to Rule 17a-5, “Reports to Be Made by Certain Brokers and Dealers,” of the Securities Exchange Act of 1934

Rule 17a-5

(Excerpt)

• Proposed amendments would require carrying broker-dealers to file, on an annual basis, a compliance report that asserts compliance, and effective internal control over compliance, with the SEC’s financial responsibility rules (FRRs).

• Broker-dealers would also have to file a form, known as “form custody,” on a quarterly basis. The form custody would require broker-dealers to disclose various information about their custodial activities.

• The PCAOB also issued two proposed attestation standards on engagements related to broker-dealer compliance and exemption reports required by the SEC’s proposed amendments to Rule 17a-5.

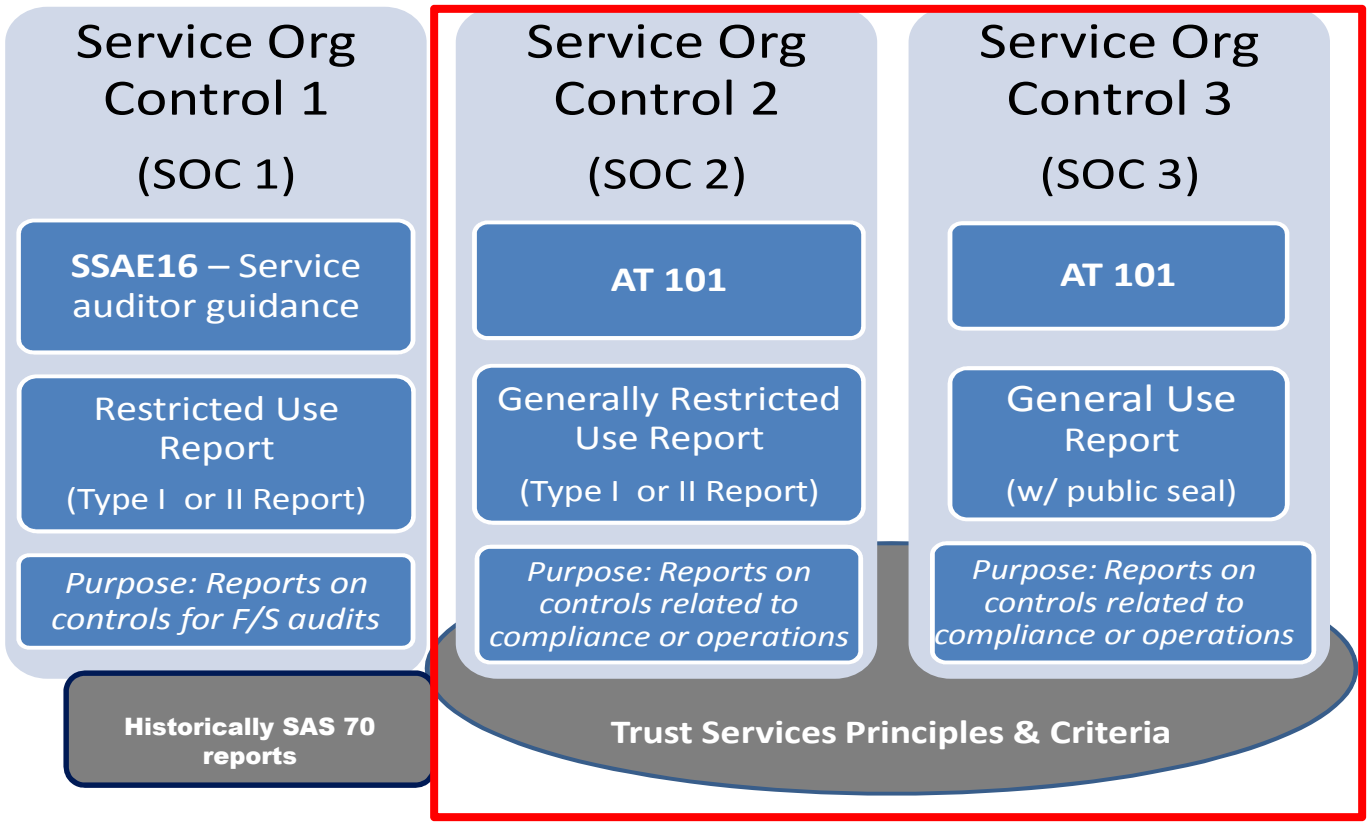
- The proposed attestation standard on compliance reports would require the assertions made by the broker-dealer regarding the FRRs as well as the existence of assets, risk of fraud, and any risks of material misstatement.
- The proposed attestation standard on exemption reports would require independent auditors to apply a risk-based approach in reviewing the assertions made by the broker-dealer.

• Timing of Implementation has not been confirmed

THE NEW FRAMEWORK: *SOC 2 AND SOC 3*

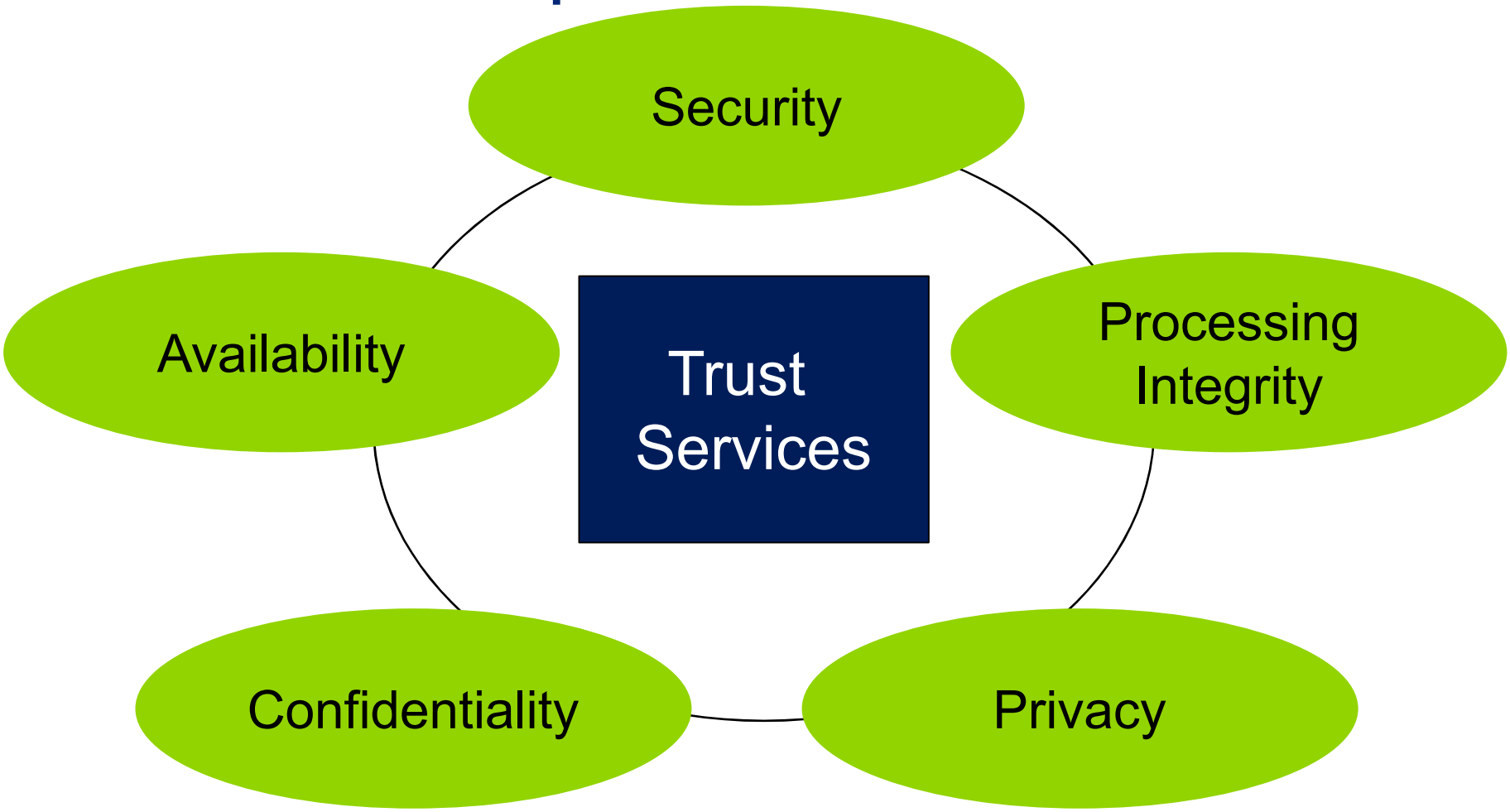
AICPA Service Organization Control (SOC) Reports:

New Standards & Options



THE NEW FRAMEWORK: *SOC 2 AND SOC 3*

Trust Services Principles & Criteria



SOC 2 – What is it?

- An AICPA report that allows service auditor to provide an opinion on the security, availability, processing integrity, confidentiality or privacy of a service organization's controls.
  - Can include one or more of the above Trust Services principles

- Similar in structure and general approach to SAS 70 (SSAE 16):
  - An option for a Type 1 or Type 2 report.
  - An opinion
  - A section describing the processing environment
  - Description of the system, including trust principles, control activities, and tests

SOC 2 – Differences from SAS 70 / SSAE 16

- A SOC 2 report does not cover processing related to financial reporting, nor is it intended to support financial reporting for your users.

- It can potentially be supplied to a wider audience. Intended users are management of the service organization, user entities, and other "specified parties." Specified parties can be anyone who understands the nature of the services being provided by the service organization, how the service organization operates, and internal control.

SOC 3 – What is it?

Controls addressed by SOC 3 are similar to those of SOC 2 Reports

- Controls over the security, availability and processing integrity of a system, and the confidentiality and privacy of information processed by the system

Key Differences between SOC 2 and SOC 3 –

- A SOC 3 report is a general use report (no restrictions)
- Provides only the auditor's report on whether the system achieved the specified Trust Services criteria. There is no description of the tests performed or the results achieved.
- The Service Organization can not receive a non-qualified opinion if:
  - UCC are significant – and the threshold for significance is relatively low
  - Any significant subservice providers are carved out

Questions?

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this presentation.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, 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 Limited 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. Certain services may not be available to attest clients under the rules and regulations of public accounting.