



# C23 – Understanding & Evaluating Service Organization Control (SOC) Reports (formerly known as SAS 70s)

**Presented by:**  
**Steve Shofner, CISA, CGEIT**  
The Shofner Group, LLC  
[Steve@ShofnerGroup.com](mailto:Steve@ShofnerGroup.com)  
510-408-7004

[www.ShofnerGroup.com](http://www.ShofnerGroup.com)

**Back to Business**

# Learning Objectives

- Background & History
  - Outsourcing and the Need For Independent Audits
  - The Old, Familiar Standards
  - The New Standards
  - Who SOC Reports Are Designed For
  - Why You Want Them
- Understanding & Evaluating SOC Reports
  - How, When, And How Often To Ask For Them
  - Factors That Need To Be Considered When Evaluating Them
  - How To Evaluate Them

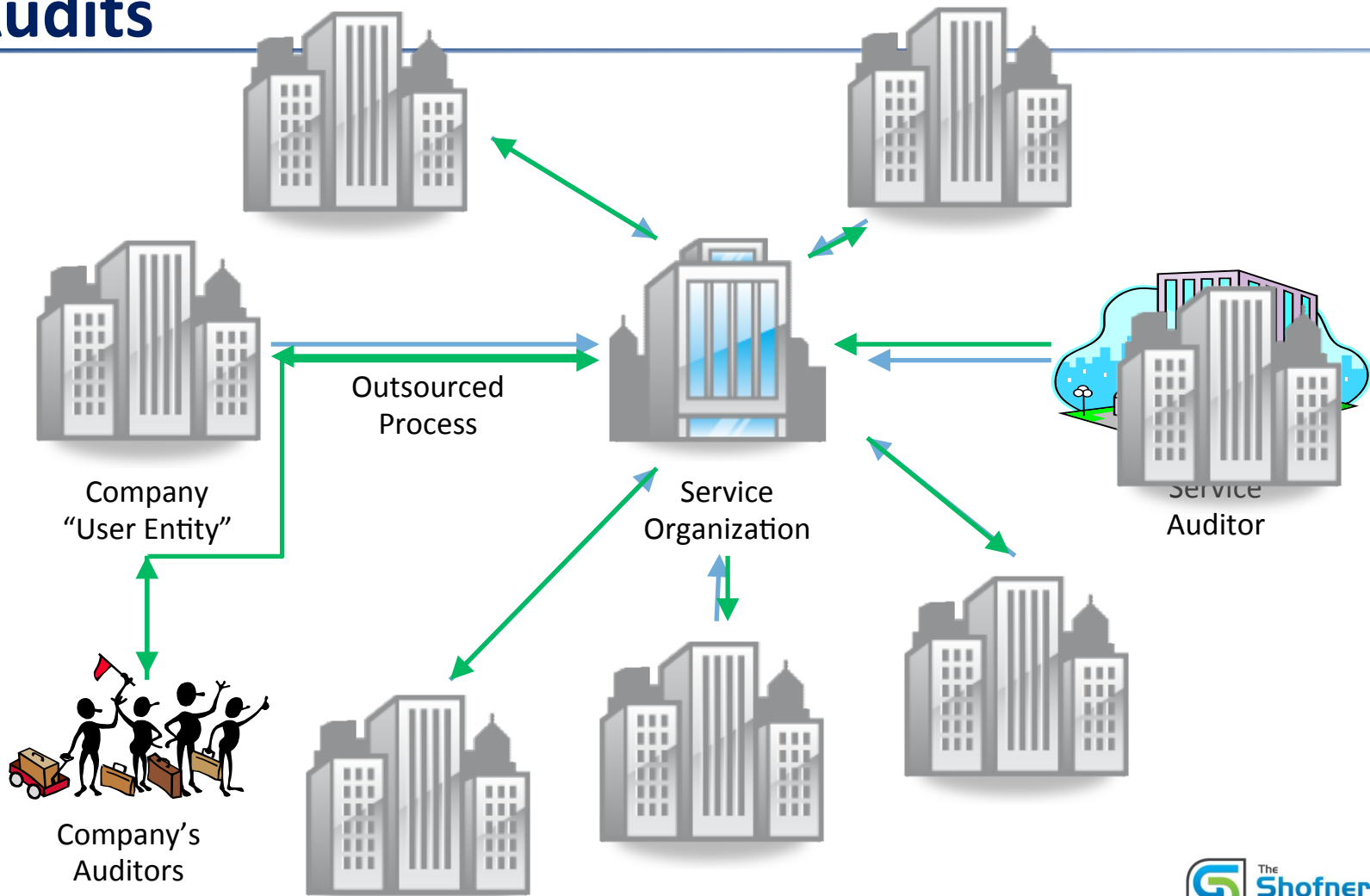


# Background & History



*Back to Business*

# Outsourcing and The Need For Independent Audits



# Old Standards

- SAS 70s: Statement of Auditing Standards #70
  - Published by the AICPA
  - Has been modified since, but “SAS 70” label stuck
- Addresses Financial Statement Processes & Controls
  - Follows COSO Framework
  - Focus on Processes and Controls
- Target Audience
  - User Entities and their Auditors, only
    - Confidential, with limited distribution
  - An “auditor-to-auditor” communication



# Old Standards

- SysTrust & WebTrust
  - Standards published by the AICPA
  - Addressed need presented primarily by Internet
- Addresses Non-Financial “Principles,” (that *could* be applied to financial systems):
  - Security
  - Availability
  - Processing Integrity
  - Confidentiality
  - Privacy
- Target Audience
  - Not limited to auditors
  - End-Users do not receive full report; A seal is issued for use on Service Organization’s website, and a ‘short-form’ report is provided (with less detail than a SAS 70)
  - These standards did not experience the same market acceptance as SAS 70s



# Changing Times

- SAS 70s Gained International Acceptance
- **The Gap:** The Market Wanted SAS 70-Level Of Detail for Non-Financial Systems, But That Wasn't Available
- **The Solution:** New Standards Took Effect 6/15/2011 (in United States):
  - ISAE 3402 Standard from the International Auditing & Assurance Standards Board
  - SSAE 16 (Statement on Standards for Attestation Engagements #16) in The United States



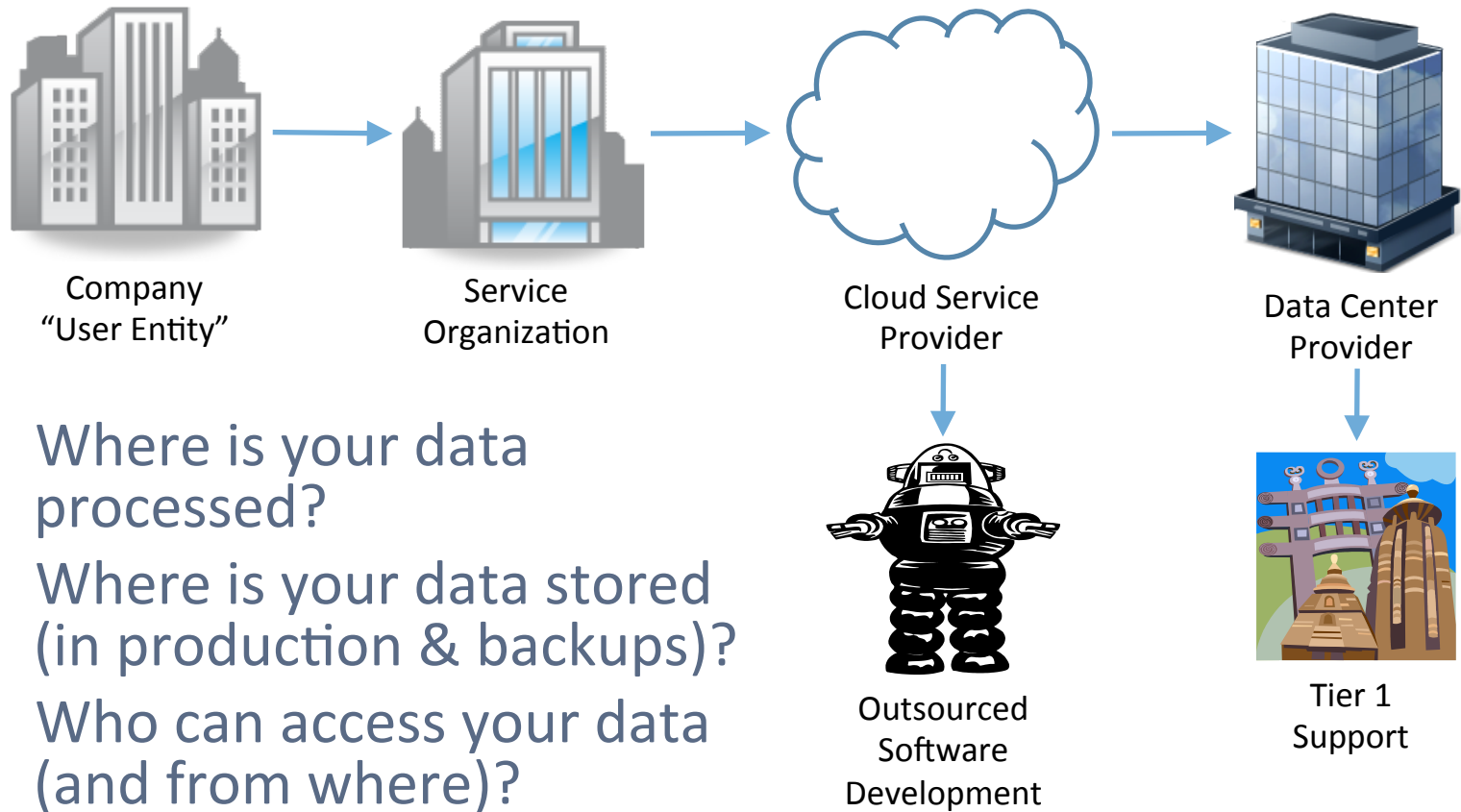
# New Reports

- Service Organization Control (SOC) Reports
  - Three Kinds Are Available:
    - **SOC 1:** “The New SAS 70”
      - Management’s Assertion
      - Design and Effectiveness Both Cover A Period Of Time
    - **SOC 2:** A “SAS 70-Style” Report Addressing One Or More Trust Principles
      - Security, Availability, Processing Integrity, Confidentiality, Privacy
    - **SOC 3:** “The New SysTrust / WebTrust”





# SOC 1/2s Needed More Than Ever Before



1. Where is your data processed?
2. Where is your data stored (in production & backups)?
3. Who can access your data (and from where)?

# Understanding & Evaluating SOC 1/2 Reports




*Back to Business*

# Dispelling Myths

- The Existence of a SOC or SAS 70 report does **not** mean you are “SOC Certified” or “SAS 70 Certified”
- SAS 70 and SSAE 16 are **Audit Standards** regarding how auditors do their work
  - How to audit
  - How to report results
- SOC reports are **audit reports** (not “certifications”), which could include bad results (poor controls, test exceptions, control failures, etc.) ...and many reports do
- It is incumbent upon User Entities to read the reports, make sure they address their needs, and determine if they identify any issues or problems



# Structure of SOC 1/2 Reports

- There are five sections:
  1. Service Auditor's Opinion Letter
  2. Management's Assertion Letter 
  3. Description of Controls
  4. Testing Results
  5. Other Information
- Critical information is spread throughout the report

# Evaluating SOC 1/2 Reports

- Determining Coverage:
  1. Does the report cover The Service you are purchasing?
    - The Specific Application(s)
    - Processing Centers / Data Centers
    - Cities / Countries

# Evaluating SOC 1/2 Reports

## Service Description Verbiage:

### CPA Firm's Logo

CPA Firm  
123 Main Street  
Hometown, USA 12345

To the Management of [*User Entity Vendor*]:

We have examined the accompanying description of controls related to the *PayAssure payroll processing and the TaxNation tax calculation and payment services processed in our Chicago, Dallas, and Los Angeles processing centers* . Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of XYZ Service Organization's controls that may be relevant to a user organization's internal control as it relates to an audit of financial statements, (2) the controls included in the description were suitably designed to achieve the control objectives....

# Evaluating SOC 1/2 Reports

- Are there any Sub-Service Providers?
  - The report will either be “Inclusive” or “Carve Out” those sub-services provider’s processes and controls

# Evaluating SOC 1/2 Reports

- Inclusive language example

We have examined XYZ Service Organization's *and ABC Subservice Organization's* description of *their* [type or name of] system for processing user entities' transactions [or identification of the function performed by the system] throughout the period [date] to [date] (description) and the suitability of the design and operating effectiveness of XYZ Service Organization's *and ABC Subservice Organization's* controls to achieve the related control objectives stated in the description. *ABC Subservice Organization is an independent service organization that provides computer processing services to XYZ Service Organization. XYZ Service Organization's description includes a description of ABC Subservice Organization's [type or name of] system used by XYZ Service Organization to process transactions for its user entities, as well as relevant control objectives and controls of ABC Subservice Organization.*

### *XYZ Service Organization's responsibilities*

On page XX of the description, XYZ Service Organization *and ABC Subservice Organization* have provided *their* assertions about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. XYZ Service Organization *and ABC Subservice Organization* are responsible for preparing the description and assertions, including the completeness, accuracy, and method of presentation of the description and assertions, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria,





# Evaluating SOC 1/2 Reports

- Carve-Out language example

We have examined XYZ Service Organization's description of its system for processing user entities' transactions [*or identification of the function performed by the system*] throughout the period [date] to [date] (description) and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description.

*XYZ Service Organization uses a computer processing service organization for all of its computerized application processing. The description on pages [bb–cc] includes only the controls and related control objectives of XYZ Service Organization and excludes the control objectives and related controls of the computer processing service organization. Our examination did not extend to controls of the computer processing service organization.*

# Evaluating SOC 1/2 Reports

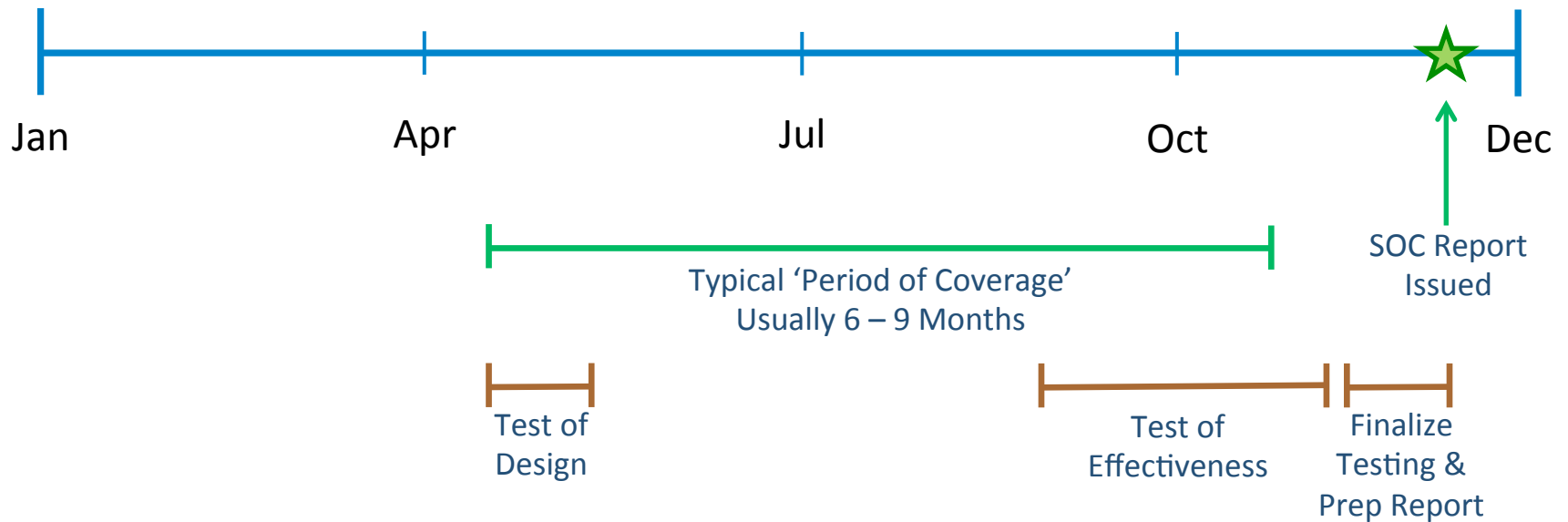
- Is the report the right Type?

	Type I	Type II
<b>Period of Coverage</b>	Point In Time Only	Period of time. Typically a minimum of six months
<b>Testing Performed</b>	No	Yes
<b>Value of the Report</b>	Provides a description of controls that have been evaluated by the Service Organization, and an opinion regarding the <u>design of controls</u> only.	Has all the information noted in a Type I, and it includes testing of the controls for the period of time specified. The opinion is regarding the <u>design of controls</u> <i>and</i> the <u>operational effectiveness of controls</u> for that period of time.

# Evaluating SOC 1/2 Reports

- Does the Period of Time meet your needs?
  - Point in time (Type I)
  - Period of time (Type II)
- SOC Reports are typically used to support User Entity audits (including their external audits). If so, does the report provide sufficient coverage to meet the audit's needs?

# Typical Timeline



- Does this provide enough coverage for your organization (consider your fiscal year)?

# Evaluating SOC 1/2 Reports

- Determining Type:
  - Type I Verbiage:

*We did not perform procedures to determine the operating effectiveness* of controls for any period. Accordingly, we express no opinion on the operating effectiveness of any aspects of XYZ Service Organization's controls, individually or in the aggregate.

- Type II Verbiage:

The description of controls at XYZ Service Organization is as of [*Point In Time Date*], and information about *tests of the operating effectiveness of specific controls covers the period from [Start Date] to [End Date]*.

# Evaluating SOC 1/2 Reports

- Is there a “Qualified” opinion?
  - Basically says “These processes and controls are good...well, let me qualify that. They are good, *except for...*”
  - You want an “Unqualified” opinion

The accompanying description states that XYZ Service Organization uses operator identification numbers and passwords to prevent unauthorized access to the system. Based on inquiries of staff personnel and inspection of activities, we determined that such procedures are employed in Applications A and B *but are not required to access the system in Applications C and D*.

In our opinion, *except for the matter referred to in the preceding paragraph*, the accompanying description of the aforementioned application presents fairly, in all material respects, the relevant aspects of XYZ Service Organization's controls that had been placed in operation as of [*Point In Time Date*].

# Evaluating SOC 1/2 Reports

- Are there any Significant Deficiencies?

As discussed in the accompanying description, from time to time the Service Organization makes changes in application programs to correct deficiencies or to enhance capabilities. The procedures followed in determining whether to make changes, in designing the changes, and in implementing them *do not include review and approval by authorized individuals who are independent from those involved in making the changes. There are also no specified requirements to test such changes or provide test results to an authorized reviewer prior to implementing the changes.*

Also in our opinion, except *for the deficiency referred to in the preceding paragraph*, the controls, as described, are suitably designed to provide reasonable assurance that the related control objectives would be achieved if the described controls were complied with satisfactorily.

# Evaluating SOC 1/2 Reports

- Are Any Controls Missing?
  - Depending on *your* organization's control strategy, you may *require* certain controls, but the Service Organization may not have them
  - Remember SOC reports are not “certifications.” There are no ‘required’ controls.



# Evaluating SOC 1/2 Reports

- Are there Client Control Considerations?
  - These are controls that the Service Organization tells *you* to have for the overall control environment to be effective
  - Usually at the end of Section 3, but could be peppered throughout the report

# Evaluating SOC 1/2 Reports

- Were there any Exceptions noted during testing?

# Evaluating SOC 1/2 Reports

- For any Missing Controls, Client Control Considerations, or Testing Exceptions, you need to determine how to address the related risks:
  - Implement controls at the User Entity (your organization)
  - Convince the Service Organization to implement new controls
  - Switch to another Service Organization

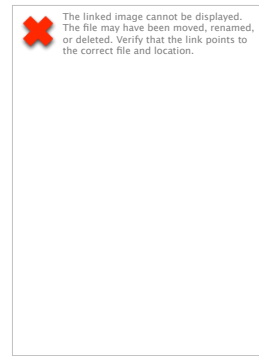
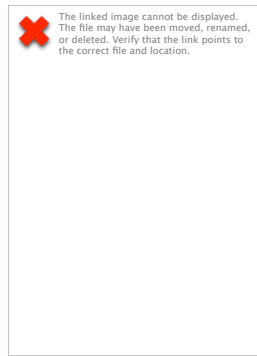


# Summary:

- Determine Scope & Coverage
  - The Specific Application(s)
  - Processing Centers / Data Centers
  - Cities / Countries
  - Type I or II
  - Date Coverage
  - Use of Sub-Service Providers (inclusive or carve-out)
- Check for Control Issues:
  - Significant Deficiencies
  - Missing Controls
  - Client Control Considerations
  - Testing Exceptions
- Evaluate & address impact to your organization

# Resources

- AICPA:
  - Books:



- Website:

- SSAE 16:  
<http://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AT-00801.pdf>
- SOC Report Info & Guidance: <http://www.aicpa.org/soc>

- Shofner Group Whitepaper (coming soon)



# Thank You! & Questions

---

Steve Shofner, CISA, CGEIT

CEO, The Shofner Group, LLC

[www.ShofnerGroup.com](http://www.ShofnerGroup.com)

[Steve@ShofnerGroup.com](mailto:Steve@ShofnerGroup.com)

510-408-7004



*Back to Business*