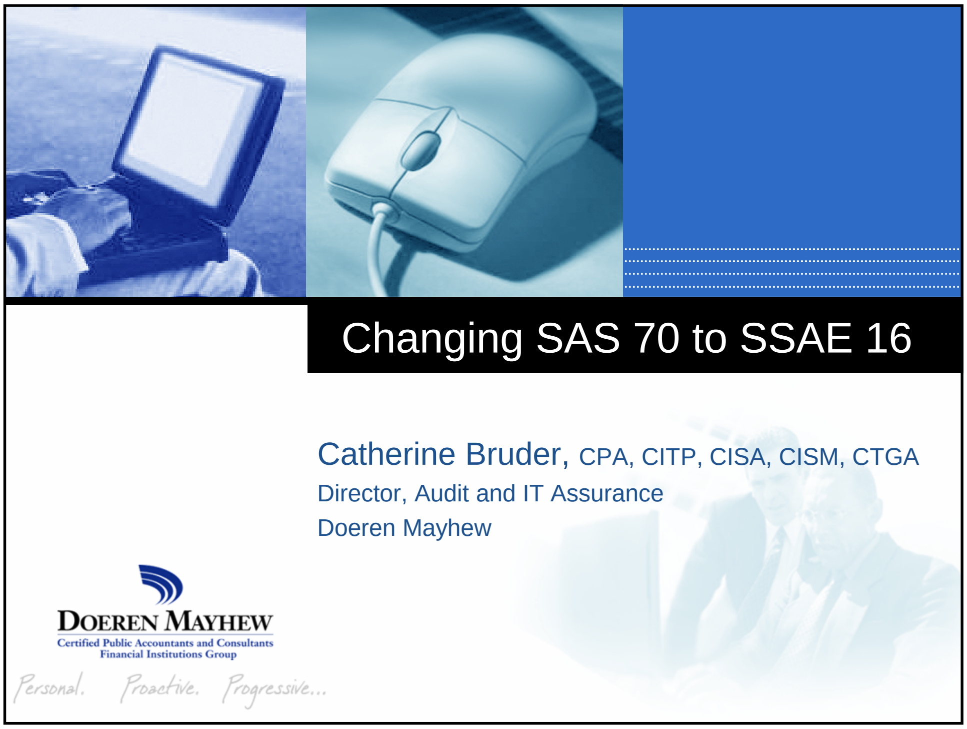


Changing SAS 70 to SSAE 16

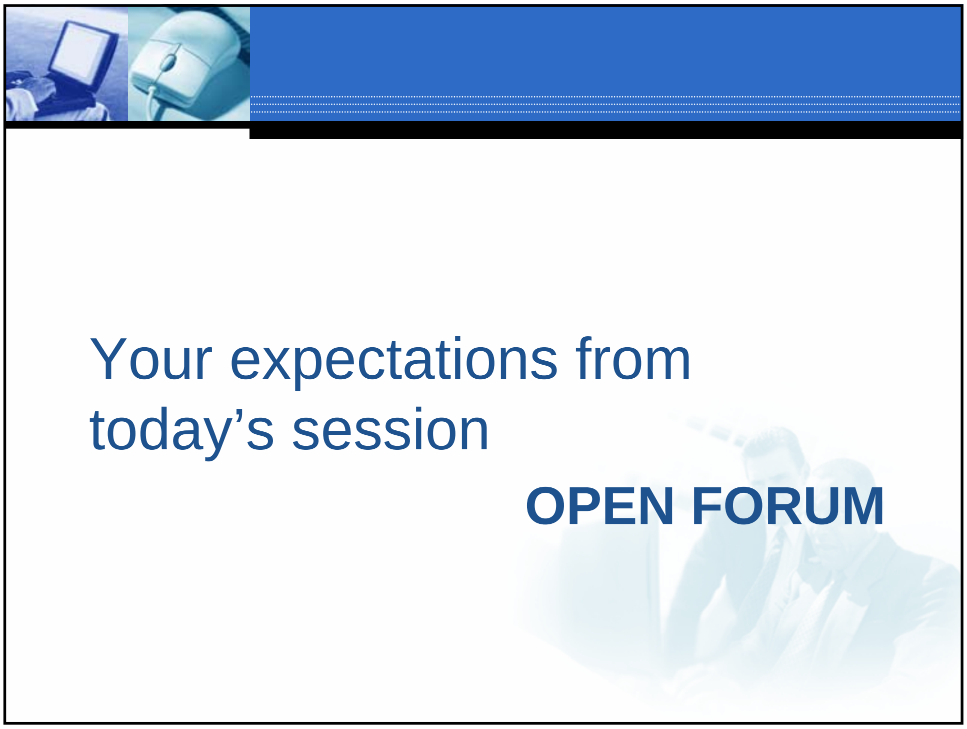
Catherine Bruder, CPA, CITP, CISA, CISM, CTGA
Director, Audit and IT Assurance
Doeren Mayhew

DOEREN MAYHEW
Certified Public Accountants and Consultants
Financial Institutions Group

Personal. Proactive. Progressive...

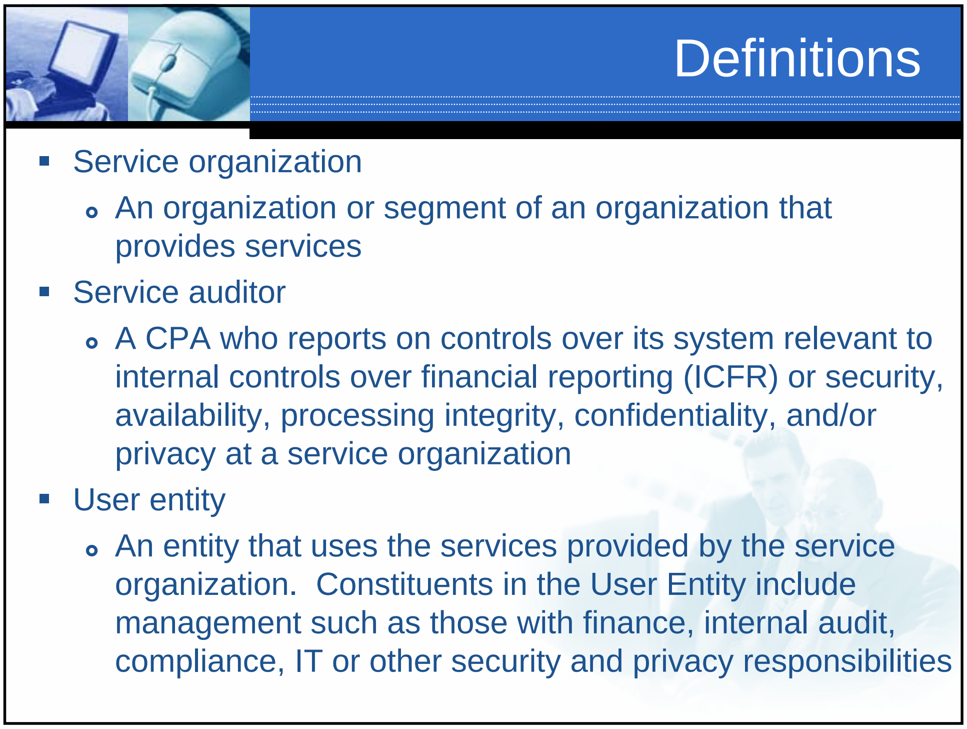
Agenda

1. History
2. Why Change
3. Key Elements of the New Reports
4. Determining Which Report
5. Outsourcing and User Entities



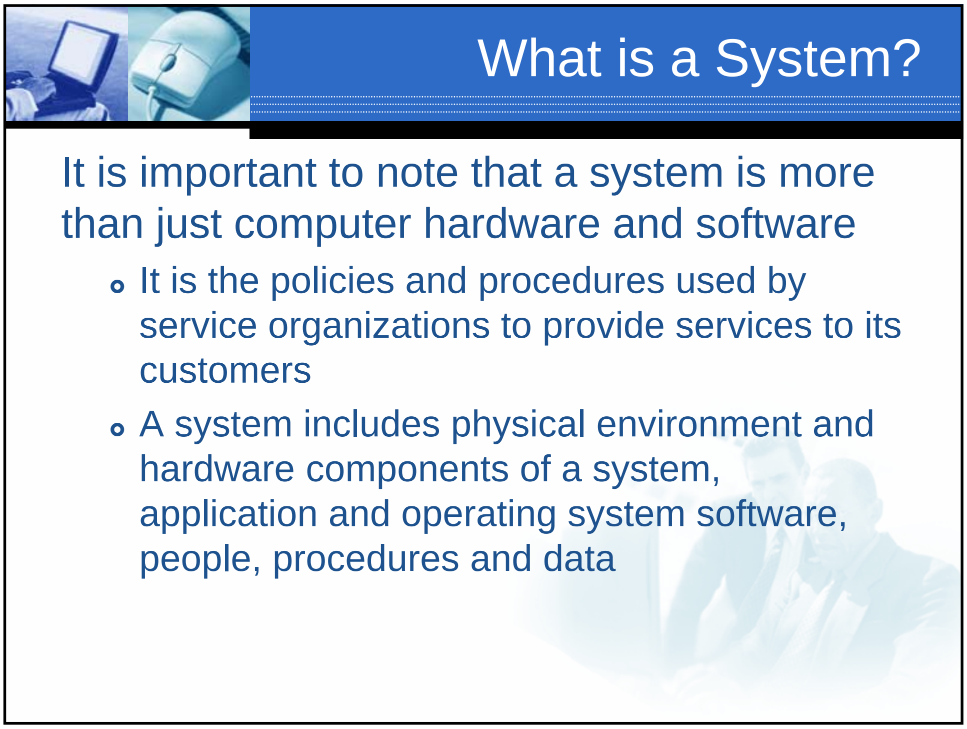
Your expectations from today's session

OPEN FORUM



Definitions

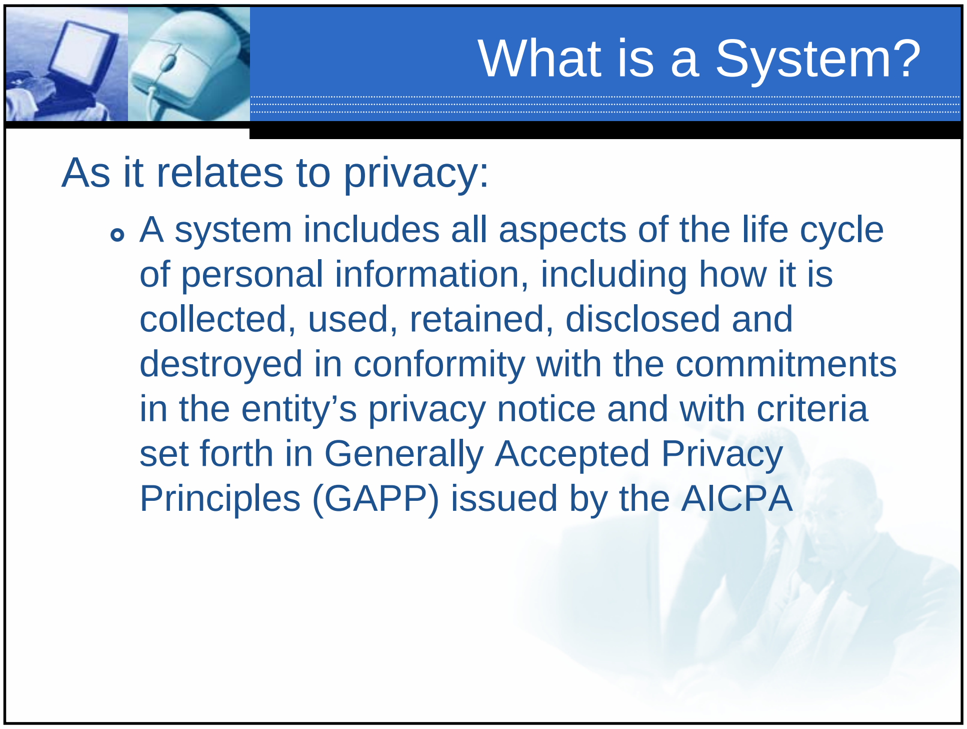
- Service organization
  - An organization or segment of an organization that provides services
- Service auditor
  - A CPA who reports on controls over its system relevant to internal controls over financial reporting (ICFR) or security, availability, processing integrity, confidentiality, and/or privacy at a service organization
- User entity
  - An entity that uses the services provided by the service organization. Constituents in the User Entity include management such as those with finance, internal audit, compliance, IT or other security and privacy responsibilities



What is a System?

It is important to note that a system is more than just computer hardware and software

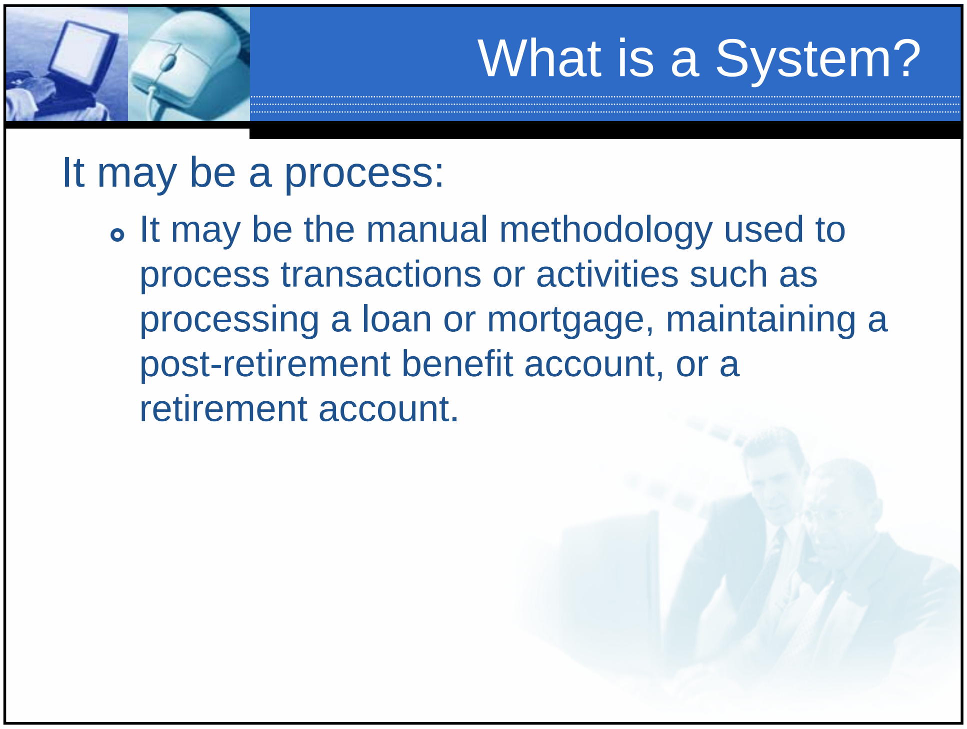
- It is the policies and procedures used by service organizations to provide services to its customers
- A system includes physical environment and hardware components of a system, application and operating system software, people, procedures and data



What is a System?

As it relates to privacy:

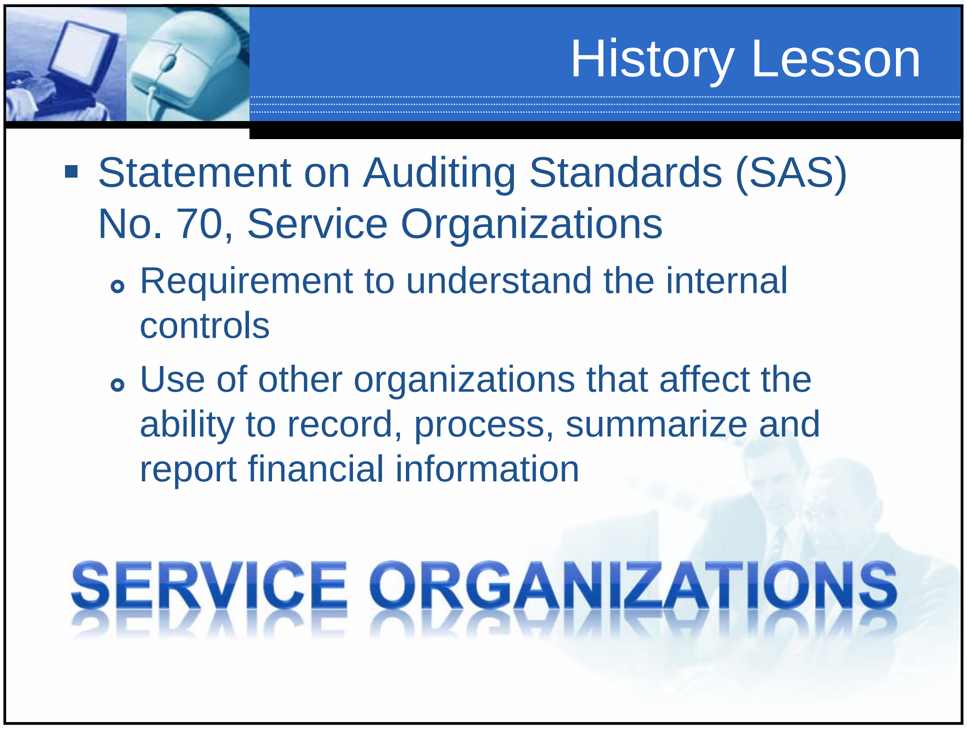
- A system includes all aspects of the life cycle of personal information, including how it is collected, used, retained, disclosed and destroyed in conformity with the commitments in the entity’s privacy notice and with criteria set forth in Generally Accepted Privacy Principles (GAPP) issued by the AICPA



What is a System?

It may be a process:

- It may be the manual methodology used to process transactions or activities such as processing a loan or mortgage, maintaining a post-retirement benefit account, or a retirement account.



History Lesson

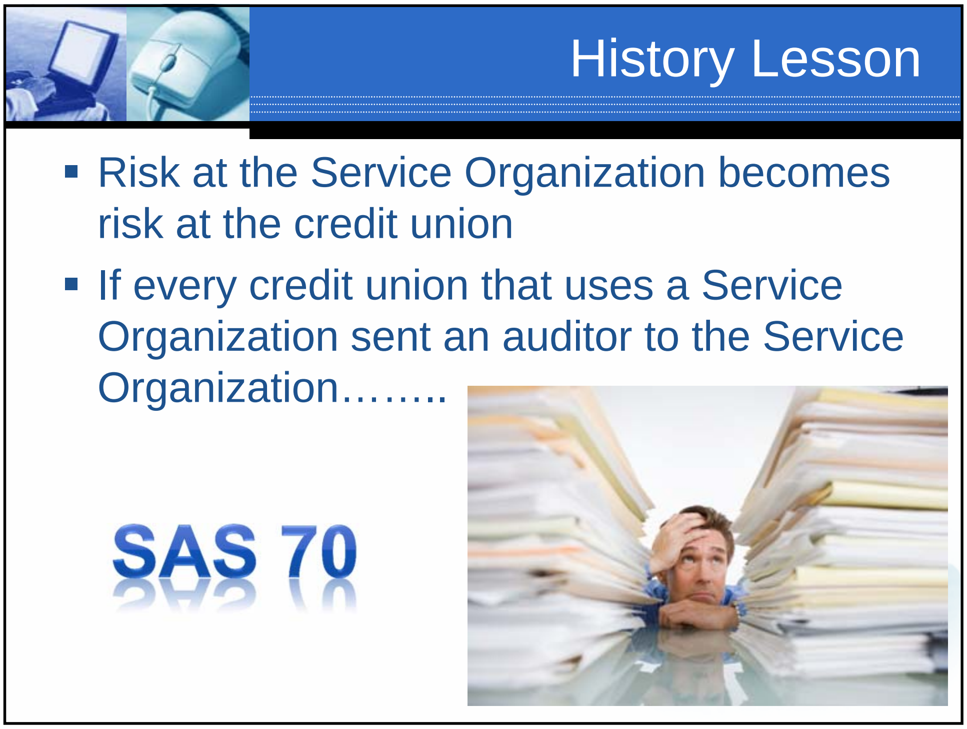
- Statement on Auditing Standards (SAS) No. 70, Service Organizations
  - Requirement to understand the internal controls
  - Use of other organizations that affect the ability to record, process, summarize and report financial information

SERVICE ORGANIZATIONS

History Lesson

- Examples of Service Organizations
  - Information Technology Providers
  - Benefit Plan Administrators
  - Mortgage Servicers
  - Statement Mailers

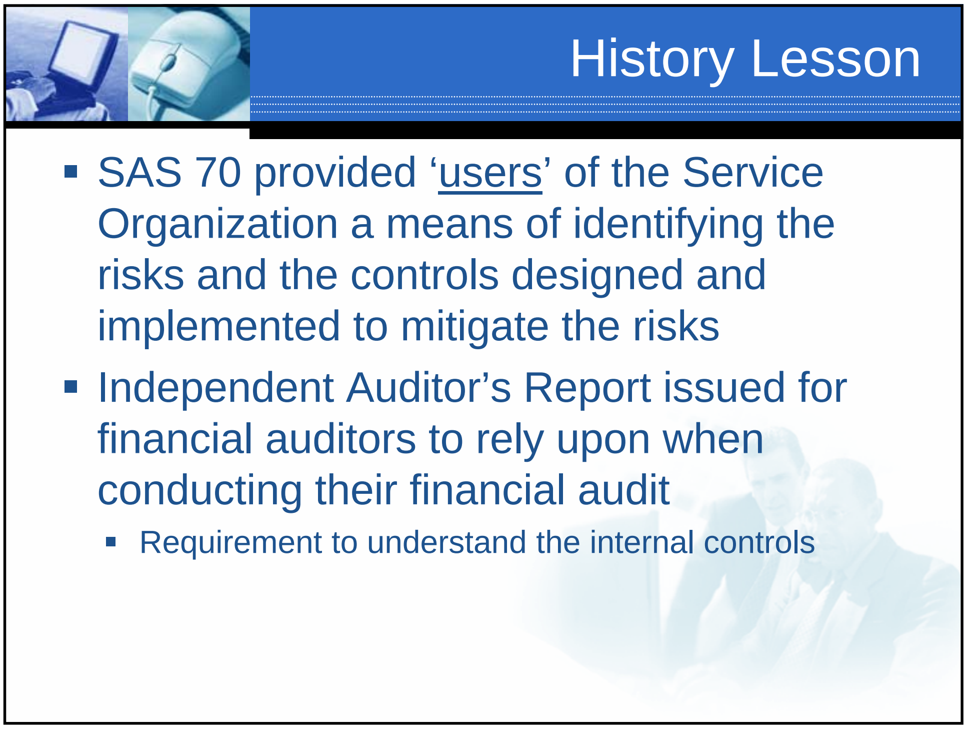
THIRD PARTY VENDORS



History Lesson

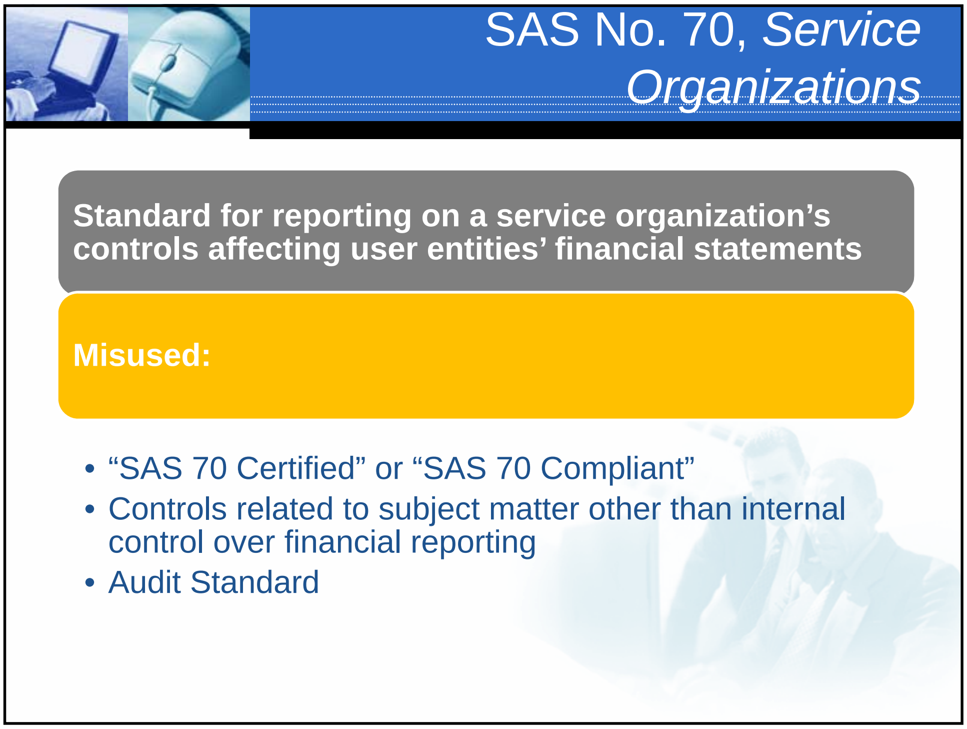
- Risk at the Service Organization becomes risk at the credit union
- If every credit union that uses a Service Organization sent an auditor to the Service Organization……..

SAS 70



History Lesson

- SAS 70 provided ‘users’ of the Service Organization a means of identifying the risks and the controls designed and implemented to mitigate the risks
- Independent Auditor’s Report issued for financial auditors to rely upon when conducting their financial audit
  - Requirement to understand the internal controls



SAS No. 70, *Service Organizations*

Standard for reporting on a service organization’s controls affecting user entities’ financial statements

Misused:

- “SAS 70 Certified” or “SAS 70 Compliant”
- Controls related to subject matter other than internal control over financial reporting
- Audit Standard

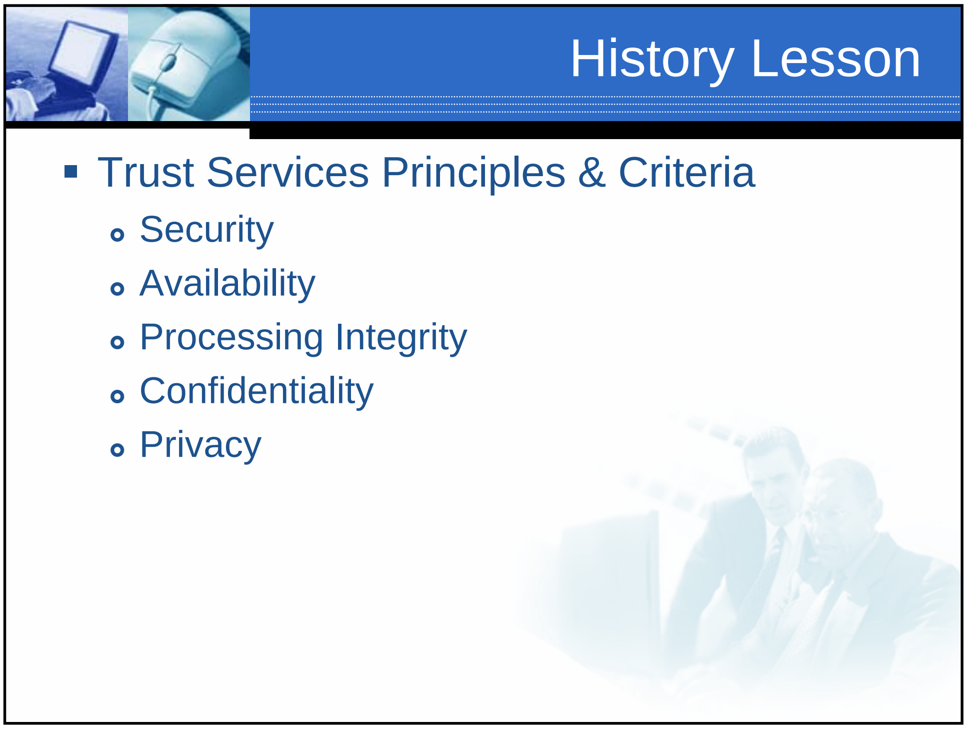
History Lesson

- Internal Control Failures
  - Enron
  - Health South
  - WorldCom
- Regulation and Oversight
  - Sarbanes-Oxley Act
  - Basel II
  - HIPAA and HITECH

History Lesson

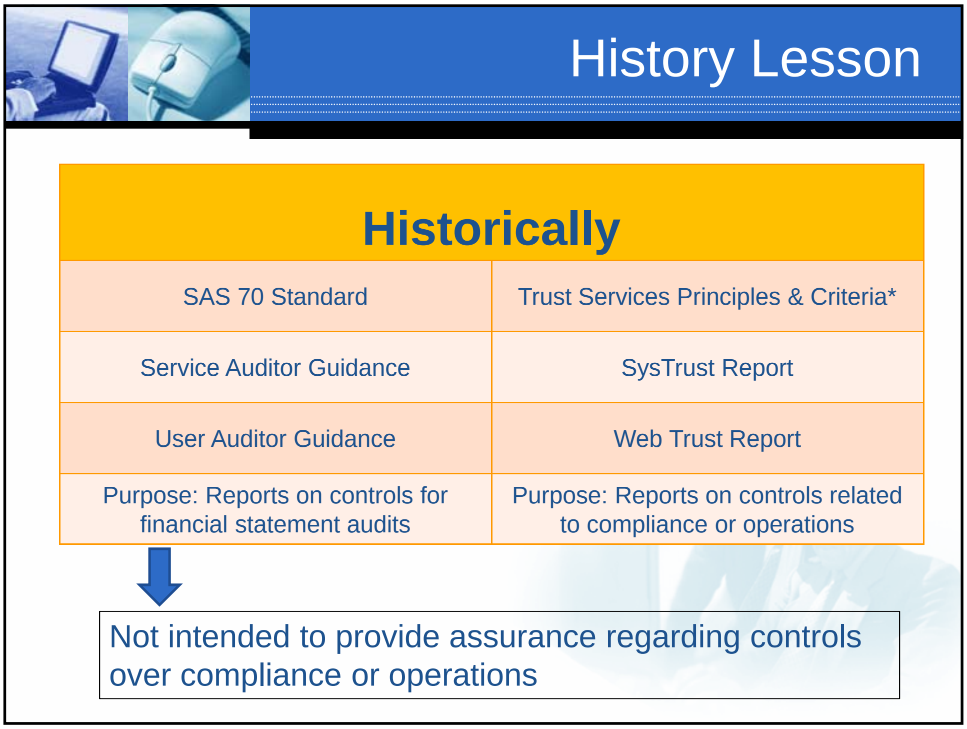
- Increased need to demonstrate security, availability and processing integrity of systems
- Increased need to ensure the confidentiality and privacy of the information processed

TRUST SERVICES PRINCIPLES, CRITERIA AND ILLUSTRATIONS



History Lesson

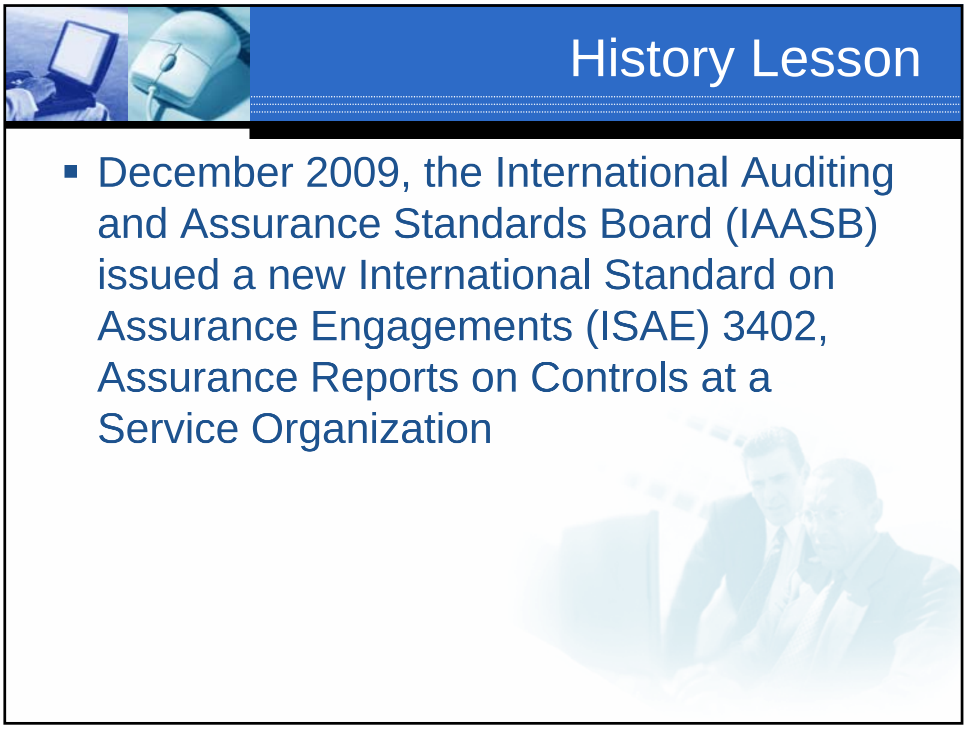
- Trust Services Principles & Criteria
  - Security
  - Availability
  - Processing Integrity
  - Confidentiality
  - Privacy



History Lesson

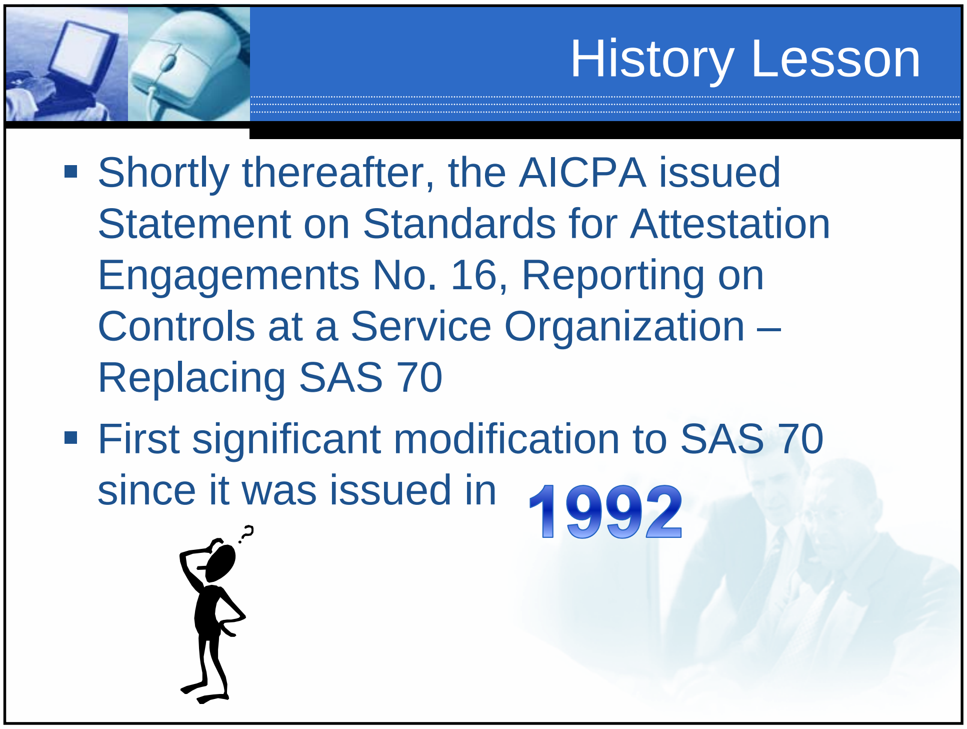
Historically	
SAS 70 Standard	Trust Services Principles & Criteria*
Service Auditor Guidance	SysTrust Report
User Auditor Guidance	Web Trust Report
Purpose: Reports on controls for financial statement audits	Purpose: Reports on controls related to compliance or operations

Not intended to provide assurance regarding controls over compliance or operations



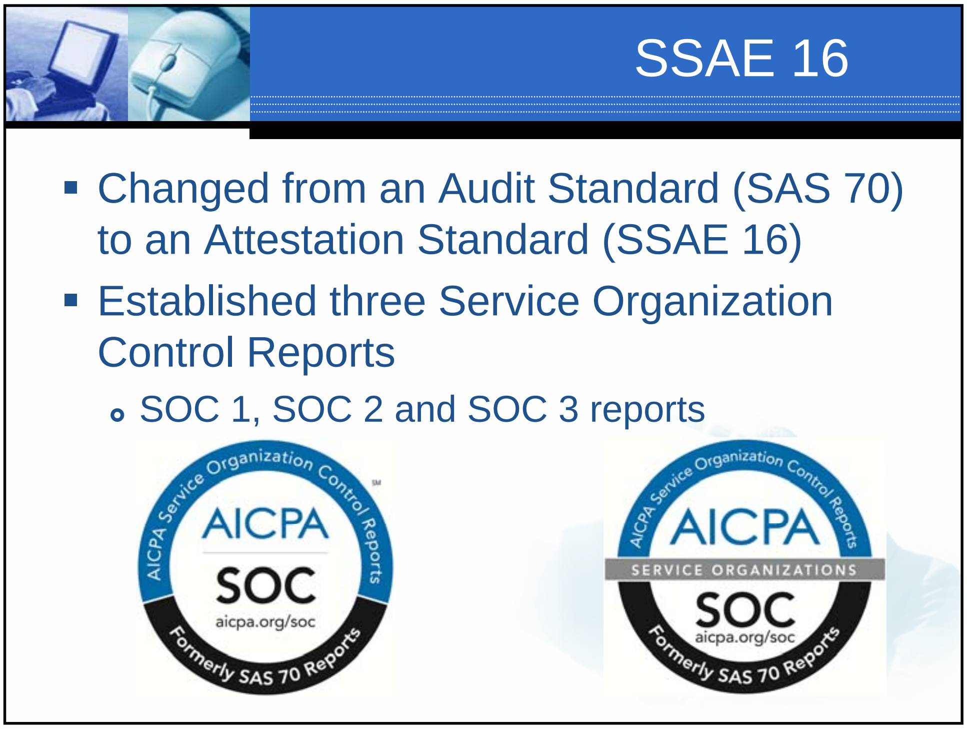
History Lesson

- December 2009, the International Auditing and Assurance Standards Board (IAASB) issued a new International Standard on Assurance Engagements (ISAE) 3402, Assurance Reports on Controls at a Service Organization



History Lesson

- Shortly thereafter, the AICPA issued Statement on Standards for Attestation Engagements No. 16, Reporting on Controls at a Service Organization – Replacing SAS 70
- First significant modification to SAS 70 since it was issued in 1992



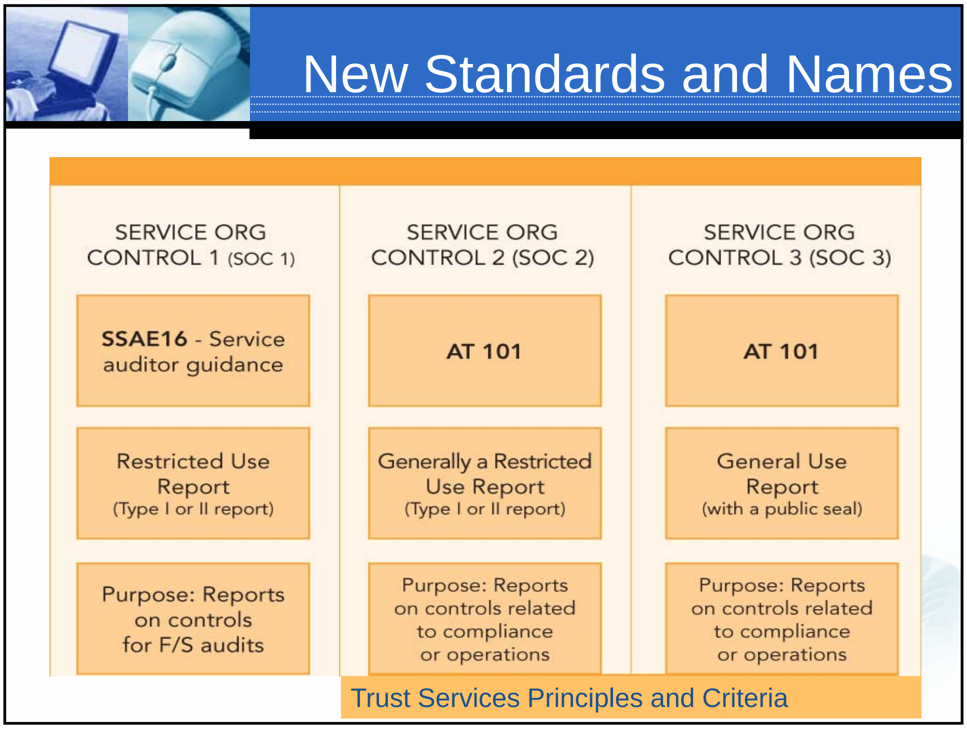
SSAE 16

- Changed from an Audit Standard (SAS 70) to an Attestation Standard (SSAE 16)
- Established three Service Organization Control Reports
  - SOC 1, SOC 2 and SOC 3 reports

AICPA Service Organization Control Reports
AICPA
SOC
aicpa.org/soc
Formerly SAS 70 Reports
AICPA Service Organization Control Reports
AICPA
SERVICE ORGANIZATIONS
SOC
aicpa.org/soc
Formerly SAS 70 Reports

SOC Reports

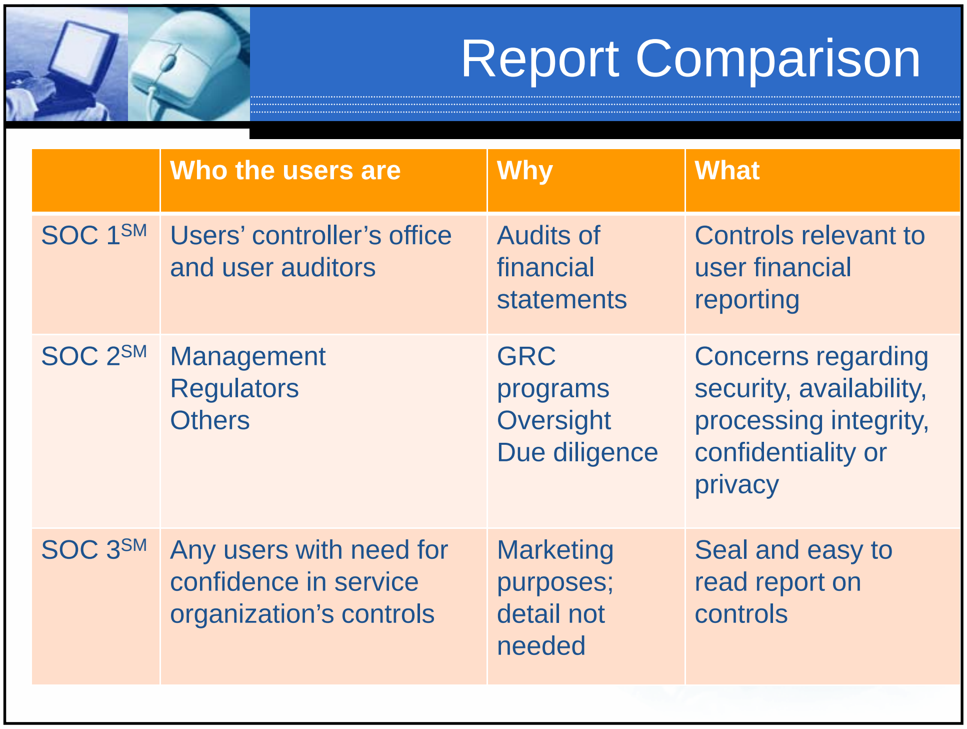
- SOC 1 reports are appropriate for service organizations whose customers are planning or performing an audit of their financial statements
- SOC 2 reports to report on the effectiveness of a Service Organization’s controls related to operations and compliance
- SOC 3, similar to SOC 2 if the report will be made available to the public, or if a seal is needed



New Standards and Names

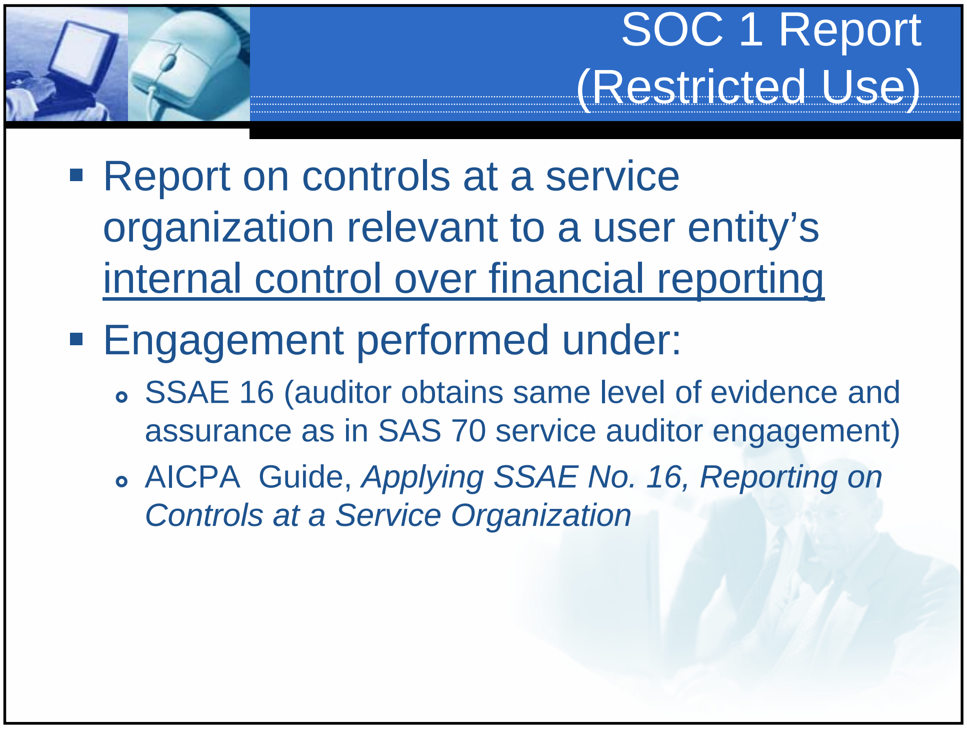
SERVICE ORG CONTROL 1 (SOC 1)	SERVICE ORG CONTROL 2 (SOC 2)	SERVICE ORG CONTROL 3 (SOC 3)
SSAE16 - Service auditor guidance	**AT 101**	**AT 101**
Restricted Use Report (Type I or II report)	Generally a Restricted Use Report (Type I or II report)	General Use Report (with a public seal)
Purpose: Reports 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 and Criteria



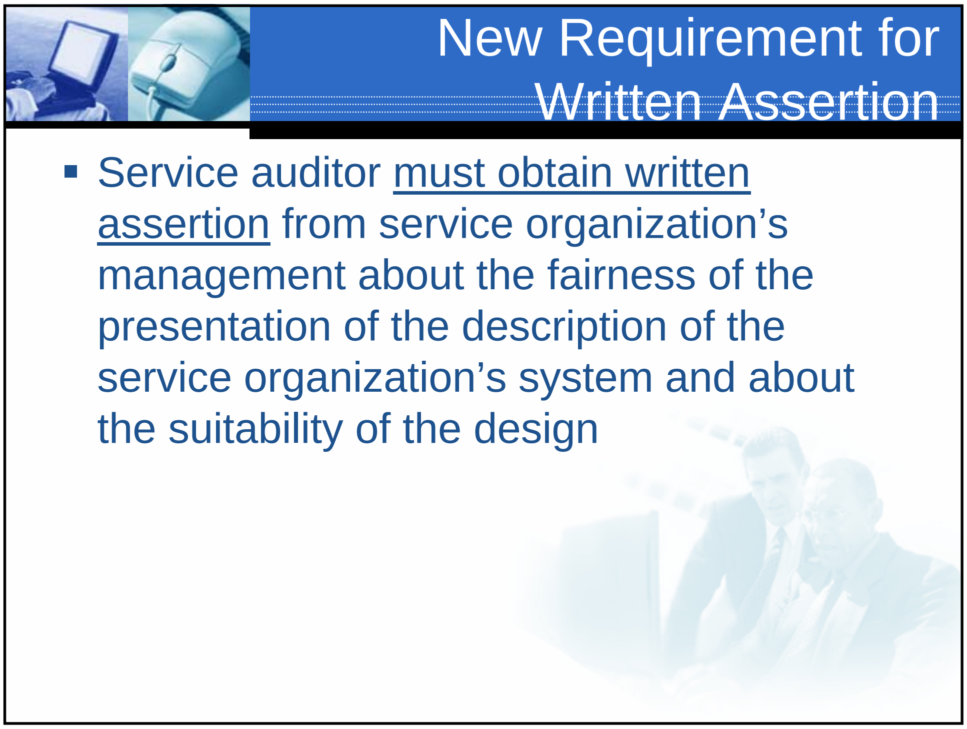
Report Comparison

	Who the users are	Why	What
SOC 1^{SM}	Users' controller's office and user auditors	Audits of financial statements	Controls relevant to user financial reporting
SOC 2^{SM}	Management Regulators Others	GRC programs Oversight Due diligence	Concerns regarding security, availability, processing integrity, confidentiality or privacy
SOC 3^{SM}	Any users with need for confidence in service organization's controls	Marketing purposes; detail not needed	Seal and easy to read report on controls



SOC 1 Report (Restricted Use)

- Report on controls at a service organization relevant to a user entity's internal control over financial reporting
- Engagement performed under:
  - SSAE 16 (auditor obtains same level of evidence and assurance as in SAS 70 service auditor engagement)
  - AICPA Guide, *Applying SSAE No. 16, Reporting on Controls at a Service Organization*

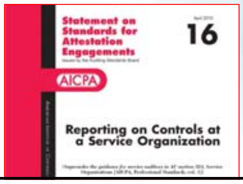


New Requirement for Written Assertion

- Service auditor must obtain written assertion from service organization's management about the fairness of the presentation of the description of the service organization's system and about the suitability of the design

Reports – Type 1 & Type 2

- Both report on the fairness of the presentation of management's description of the service organization's system, and…
  - Type 1 also reports on the suitability of the design of the controls to achieve the related control objectives included in the description as of a specified date
  - Type 2 also reports on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives included in the description throughout a specified period



Statement on Standards for Attestation Engagements

16

AICPA

Reporting on Controls at a Service Organization

GUIDE

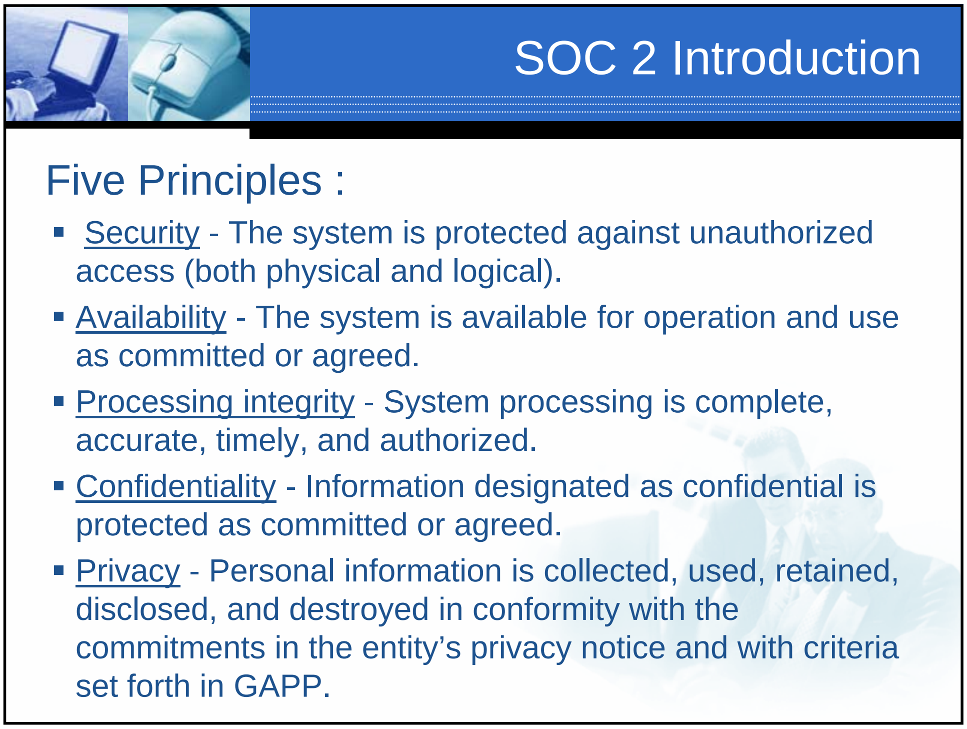
Service Organizations

Applying SSAE No. 16, *Reporting on Controls at a Service Organization* (SOC 1)

JUNE 1, 2011

SOC 2 Report (Management Use)

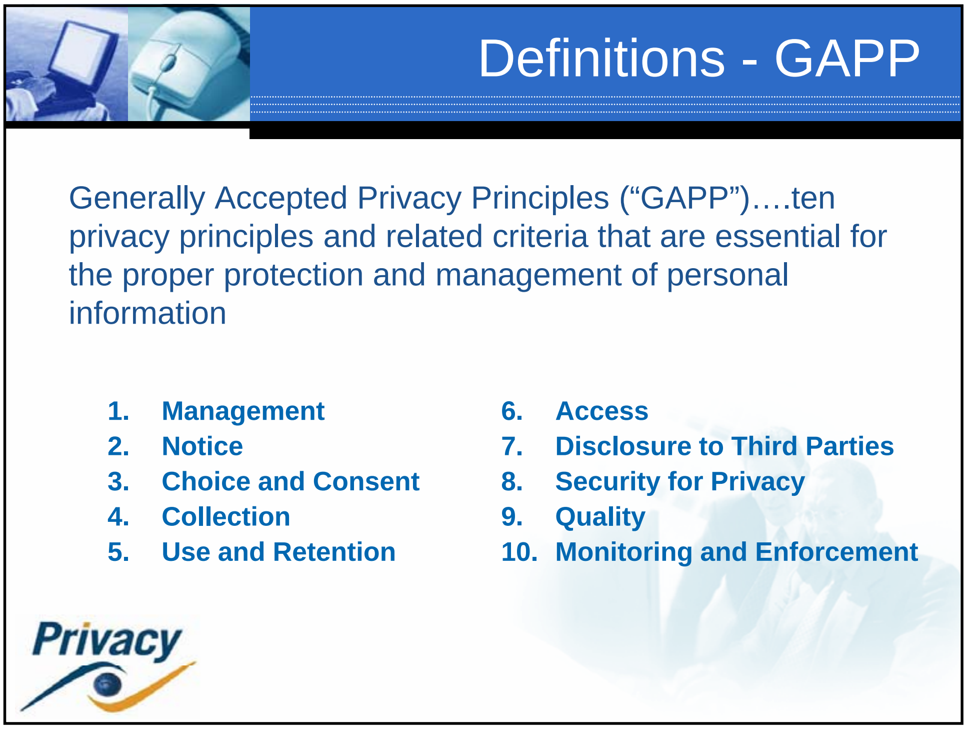
- Report on controls at a service organization relevant to security, availability, processing integrity, confidentiality or privacy
- Engagement performed under:
  - AT 101, *Attestation Engagements*
  - AICPA Guide, *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy*



SOC 2 Introduction

Five Principles :

- Security - The system is protected against unauthorized access (both 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 - Information designated as confidential is protected as committed or agreed.
- Privacy - Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy notice and with criteria set forth in GAPP.



Definitions - GAPP

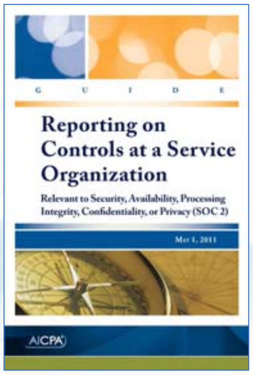
Generally Accepted Privacy Principles ("GAPP")….ten privacy principles and related criteria that are essential for the proper protection and management of personal information

1. **Management**
2. **Notice**
3. **Choice and Consent**
4. **Collection**
5. **Use and Retention**
6. **Access**
7. **Disclosure to Third Parties**
8. **Security for Privacy**
9. **Quality**
10. **Monitoring and Enforcement**

Privacy

SOC 2 Reports
Type 1 and Type 2

- Both report on management's description of a service organization's system, and …
  - Type 1 also reports on suitability of design of controls
  - Type 2 also reports on suitability of design and operating effectiveness of controls



GUIDE

Reporting on Controls at a Service Organization

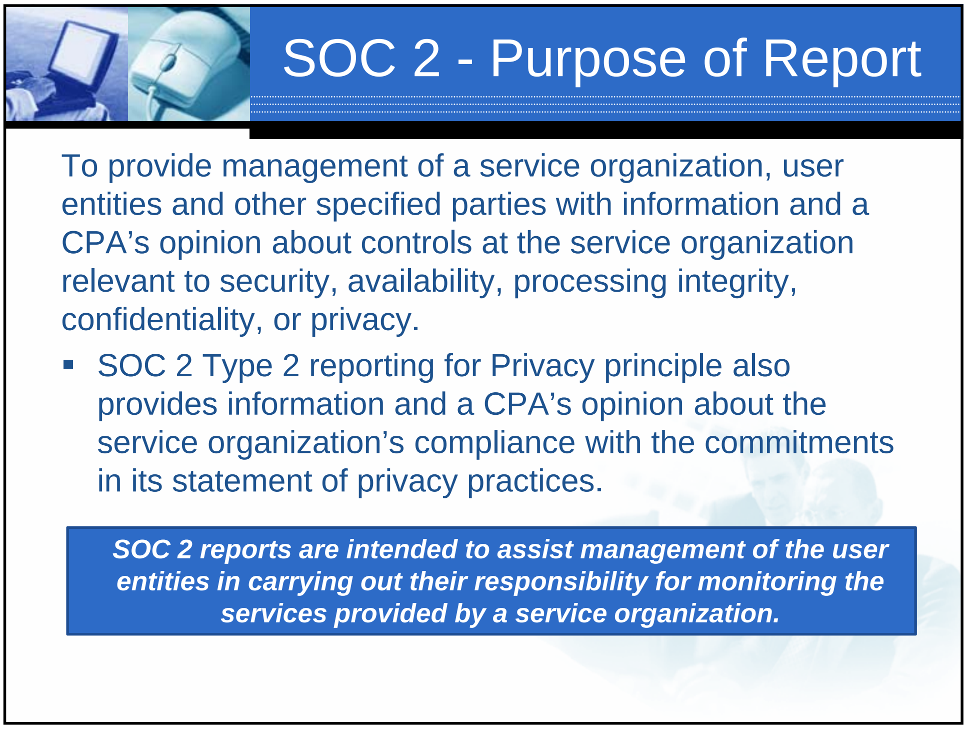
Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2)

May 1, 2011

AICPA

SOC 2 Introduction

- Many entities outsource tasks or entire functions to service organizations that operate, collect, process, transmit, store, organize, maintain, and dispose of information for user entities
  - Type 1 or type 2 report may be issued

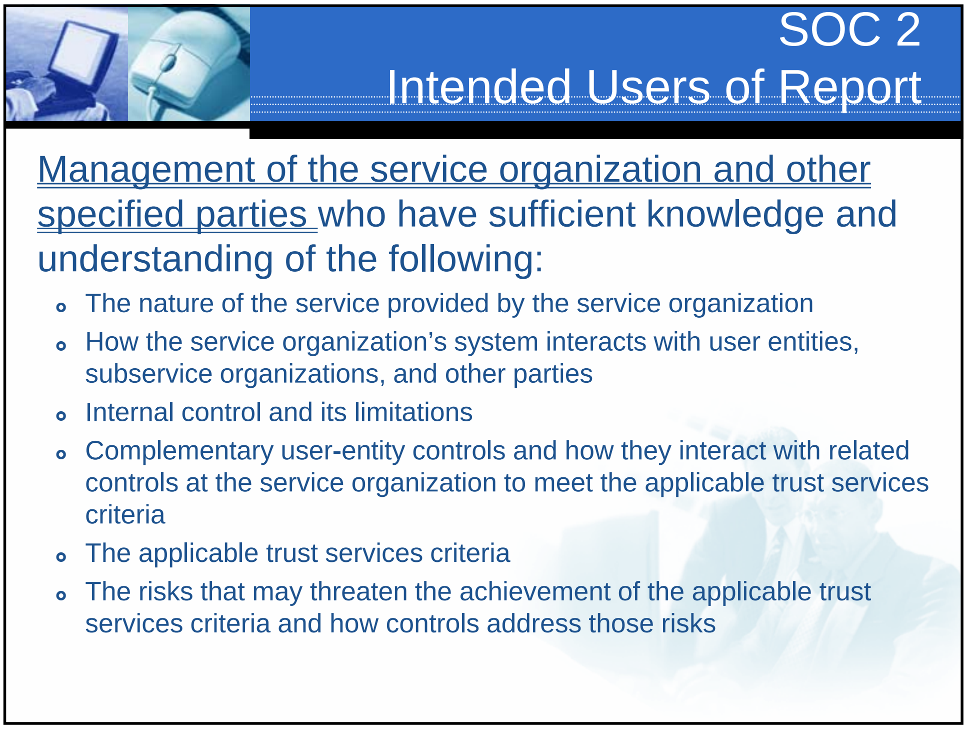


SOC 2 - Purpose of Report

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 relevant to security, availability, processing integrity, confidentiality, or privacy.

- SOC 2 Type 2 reporting for Privacy principle also provides information and a CPA's opinion about the service organization's compliance with the commitments in its statement of privacy practices.

SOC 2 reports are intended to assist management of the user entities in carrying out their responsibility for monitoring the services provided by a service organization.

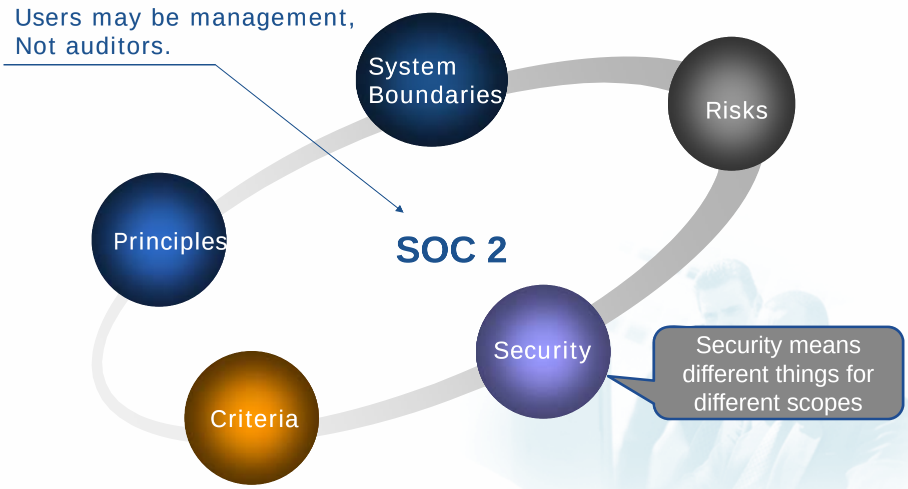


SOC 2
Intended Users of Report

Management of the service organization and other specified parties who have sufficient knowledge and understanding of the following:

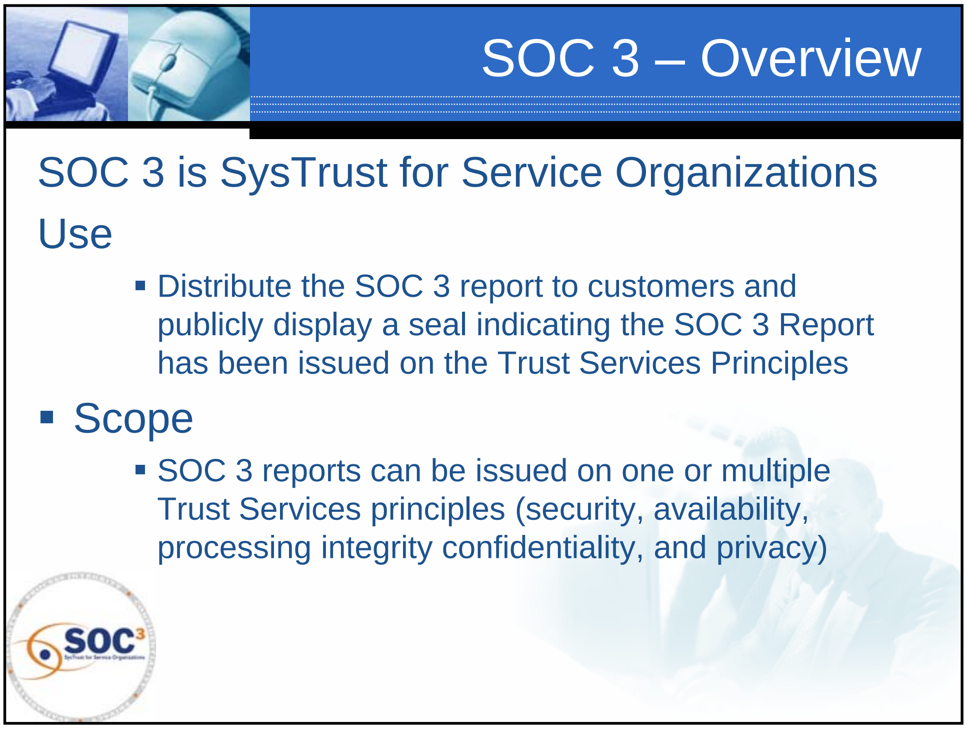
- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria
- The applicable trust services criteria
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks

SOC 2 – Scoping



SOC 3 Report (General Use)

- Trust Services Report for Service Organizations
- Engagement performed under:
  - AT 101, *Attestation Engagements*
  - AICPA TPA, *Trust Services Principles, Criteria and Illustrations*
  - *Canadian Institute Charter Accountants (CICA) holds the Seal*
- *Scope may not be modified*



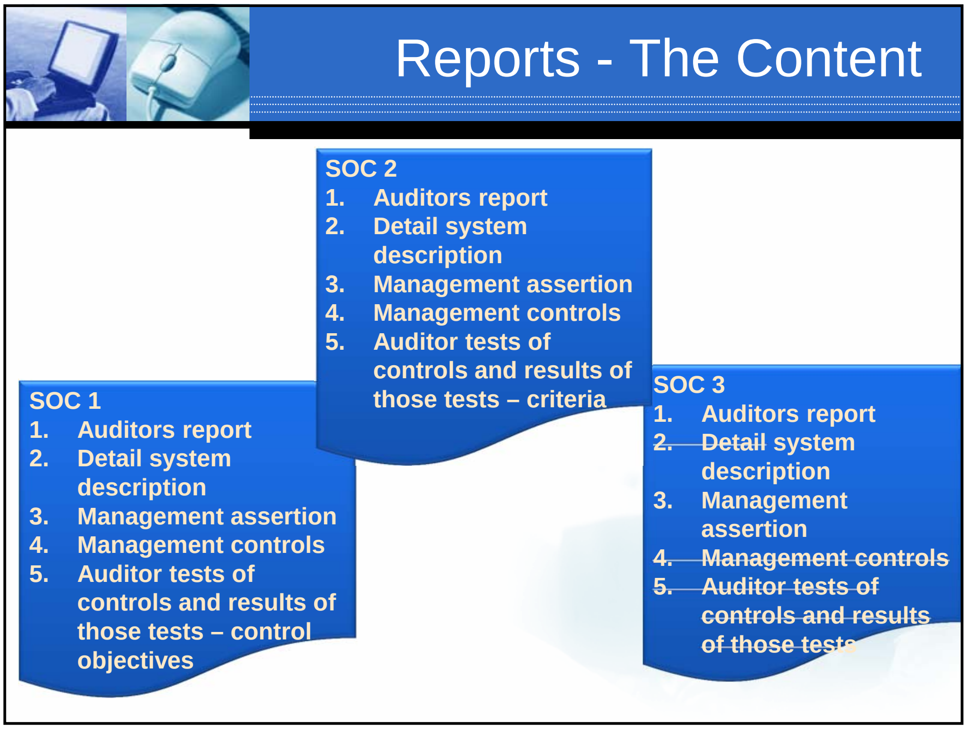
SOC 3 – Overview

SOC 3 is SysTrust for Service Organizations

Use

- Distribute the SOC 3 report to customers and publicly display a seal indicating the SOC 3 Report has been issued on the Trust Services Principles

- Scope
  - SOC 3 reports can be issued on one or multiple Trust Services principles (security, availability, processing integrity confidentiality, and privacy)

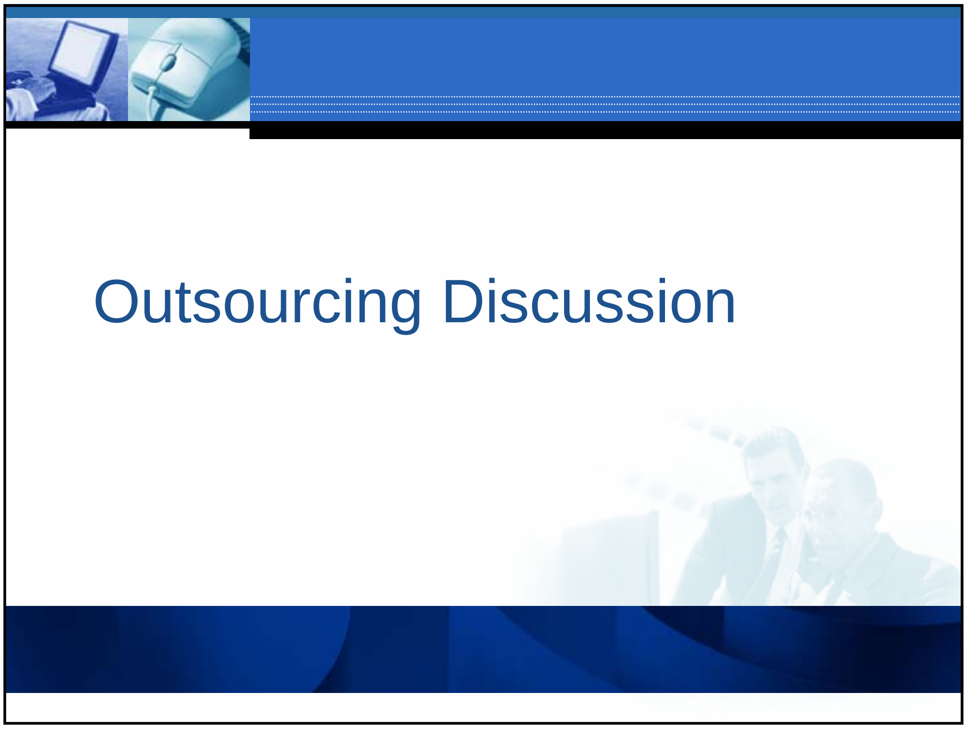


Reports - The Content

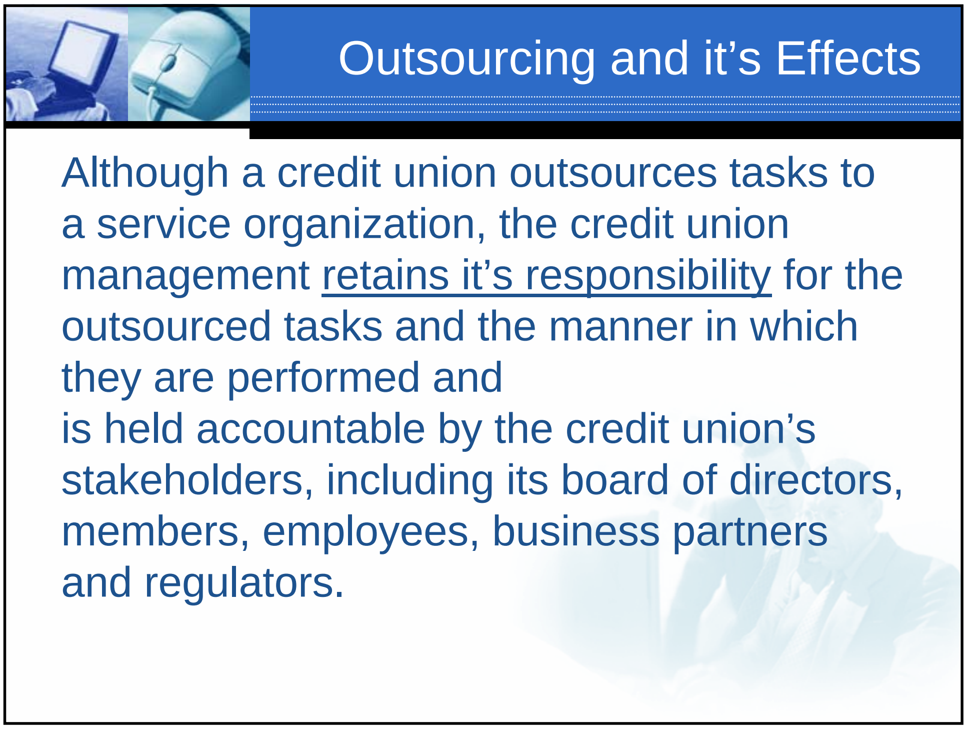
SOC 1
1. Auditors report
2. Detail system description
3. Management assertion
4. Management controls
5. Auditor tests of controls and results of those tests – control objectives

SOC 2
1. Auditors report
2. Detail system description
3. Management assertion
4. Management controls
5. Auditor tests of controls and results of those tests – criteria

SOC 3
1. Auditors report
2. ~~Detail~~ system description
3. Management assertion
4. ~~Management controls~~
5. ~~Auditor tests of controls and results of those tests~~

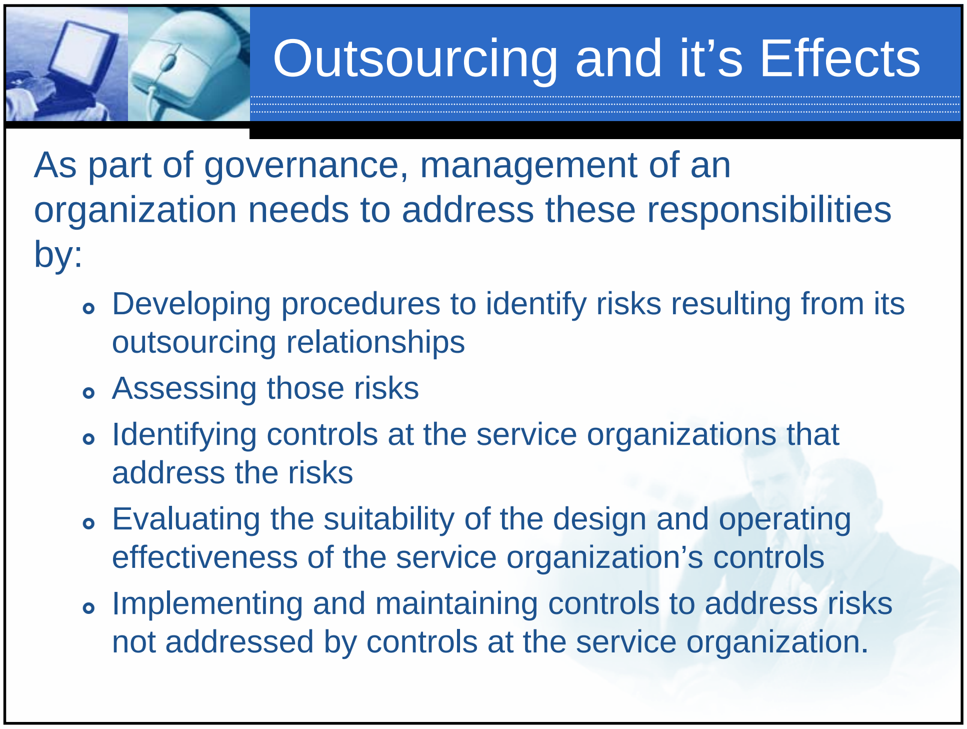


Outsourcing Discussion



Outsourcing and it's Effects

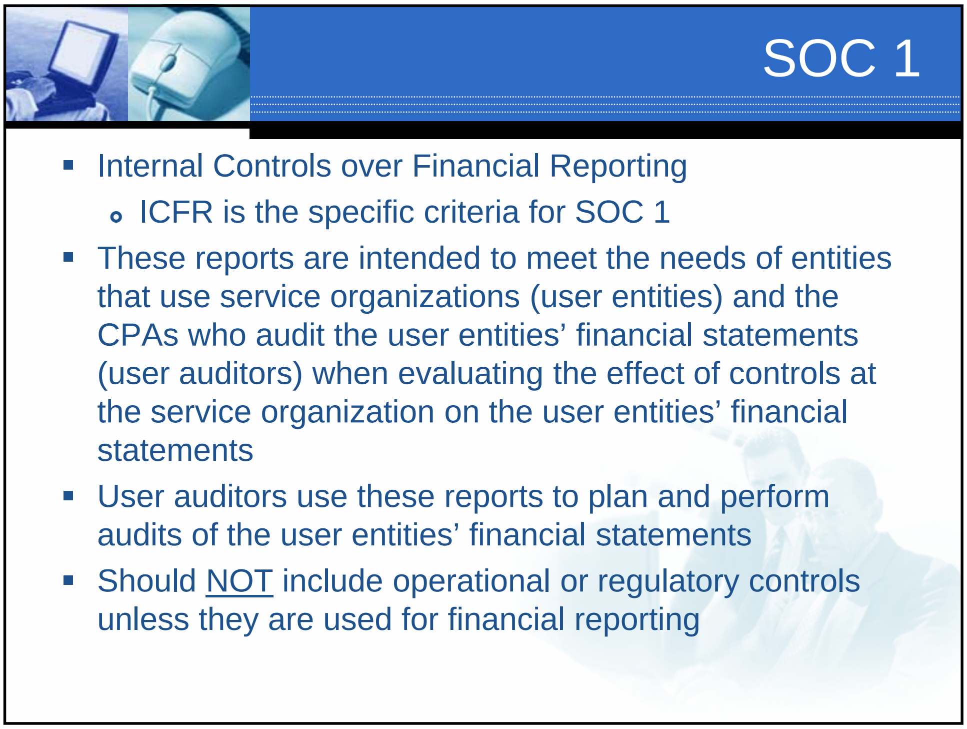
Although a credit union outsources tasks to a service organization, the credit union management retains it's responsibility for the outsourced tasks and the manner in which they are performed and
is held accountable by the credit union's stakeholders, including its board of directors, members, employees, business partners and regulators.



Outsourcing and it’s Effects

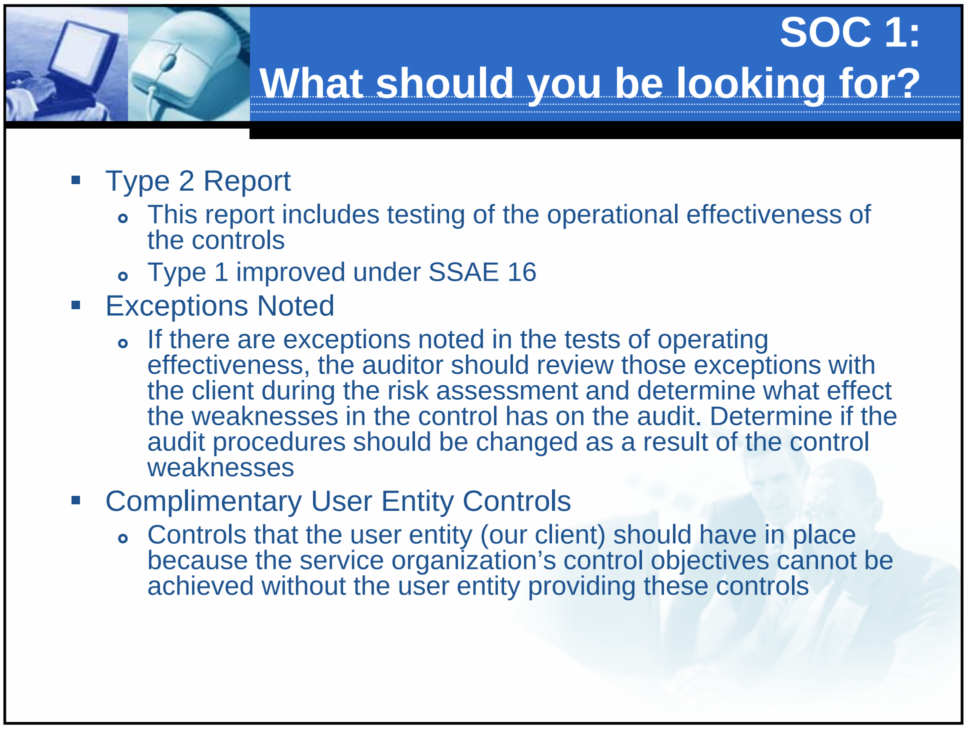
As part of governance, management of an organization needs to address these responsibilities by:

- Developing procedures to identify risks resulting from its outsourcing relationships
- Assessing those risks
- Identifying controls at the service organizations that address the risks
- Evaluating the suitability of the design and operating effectiveness of the service organization’s controls
- Implementing and maintaining controls to address risks not addressed by controls at the service organization.



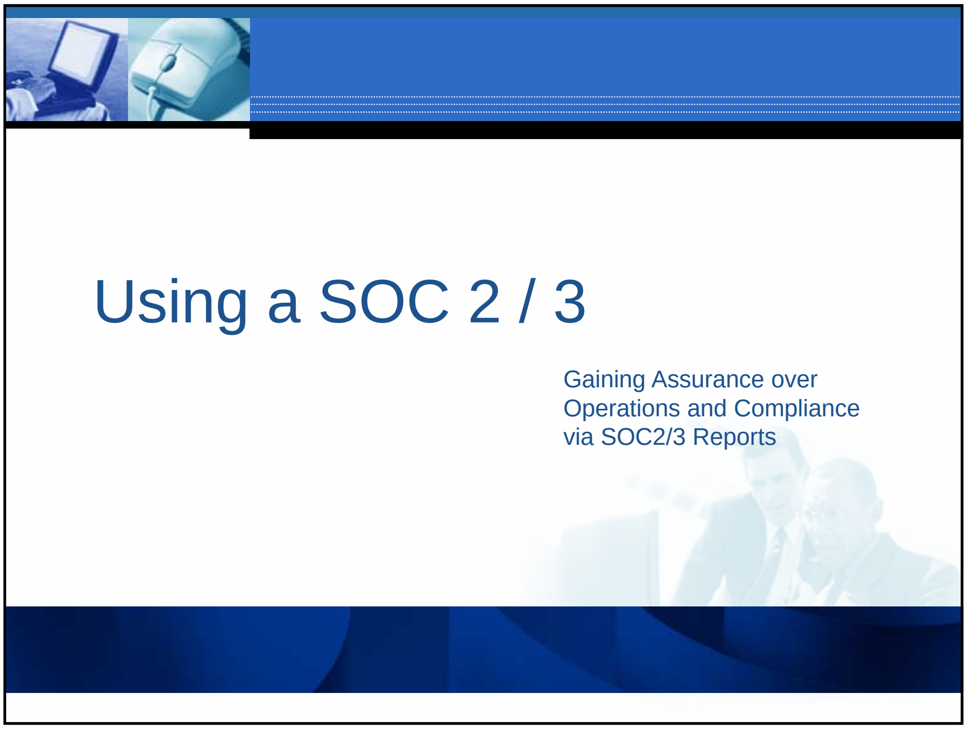
SOC 1

- Internal Controls over Financial Reporting
  - ICFR is the specific criteria for SOC 1
- These reports are intended to meet the needs of entities that use service organizations (user entities) and the CPAs who audit the user entities’ financial statements (user auditors) when evaluating the effect of controls at the service organization on the user entities’ financial statements
- User auditors use these reports to plan and perform audits of the user entities’ financial statements
- Should NOT include operational or regulatory controls unless they are used for financial reporting



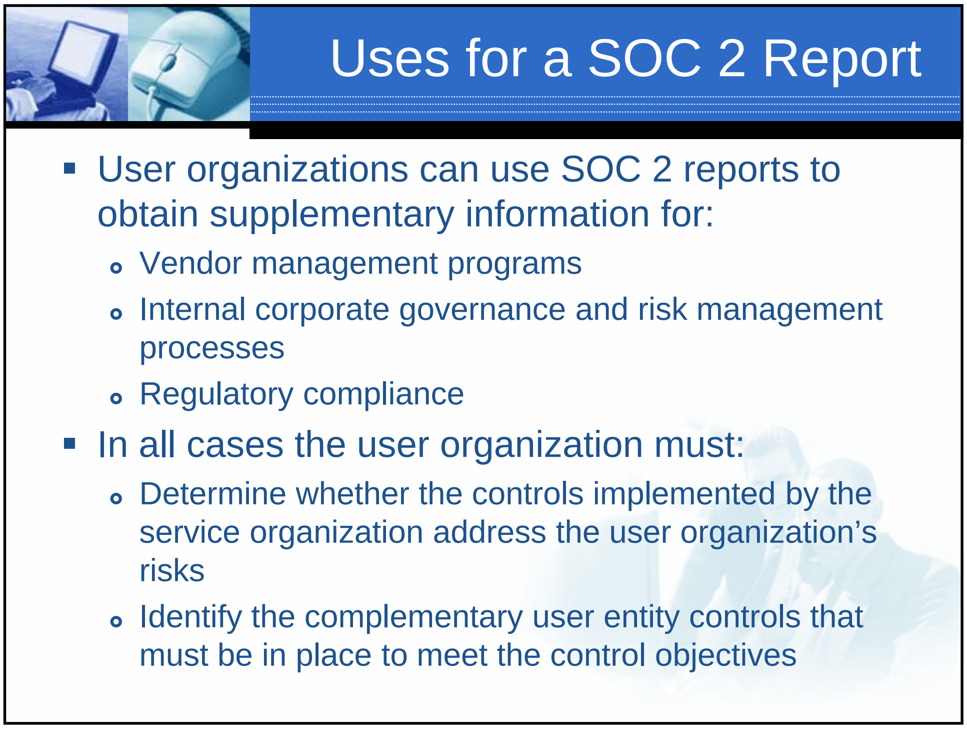
SOC 1: What should you be looking for?

- Type 2 Report
  - This report includes testing of the operational effectiveness of the controls
  - Type 1 improved under SSAE 16
- Exceptions Noted
  - If there are exceptions noted in the tests of operating effectiveness, the auditor should review those exceptions with the client during the risk assessment and determine what effect the weaknesses in the control has on the audit. Determine if the audit procedures should be changed as a result of the control weaknesses
- Complimentary User Entity Controls
  - Controls that the user entity (our client) should have in place because the service organization’s control objectives cannot be achieved without the user entity providing these controls



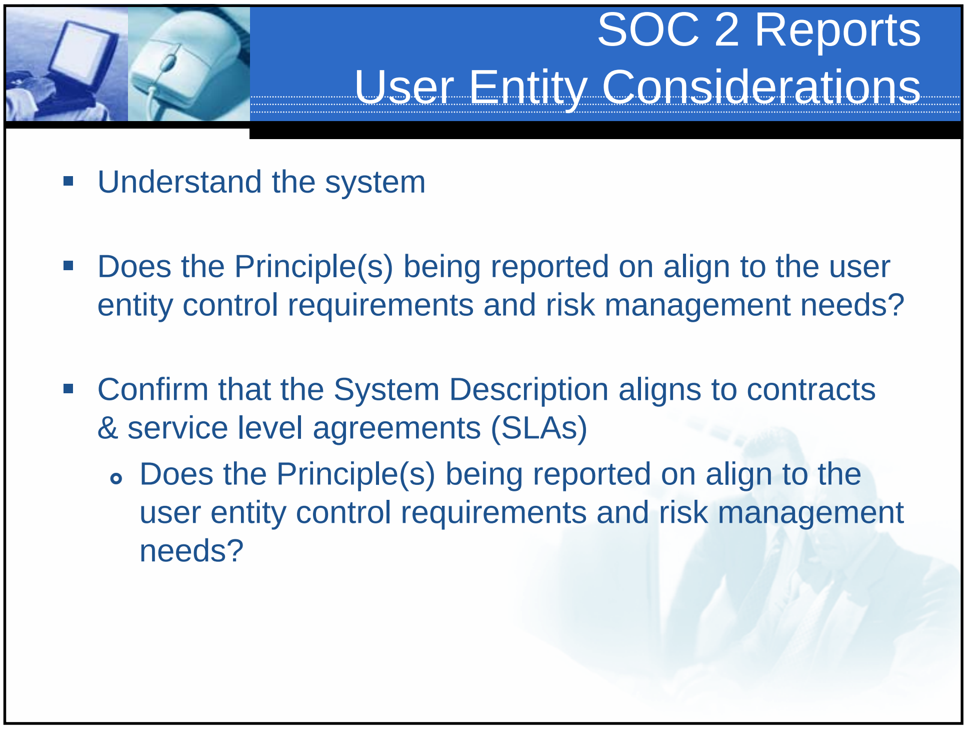
Using a SOC 2 / 3

Gaining Assurance over
Operations and Compliance
via SOC2/3 Reports



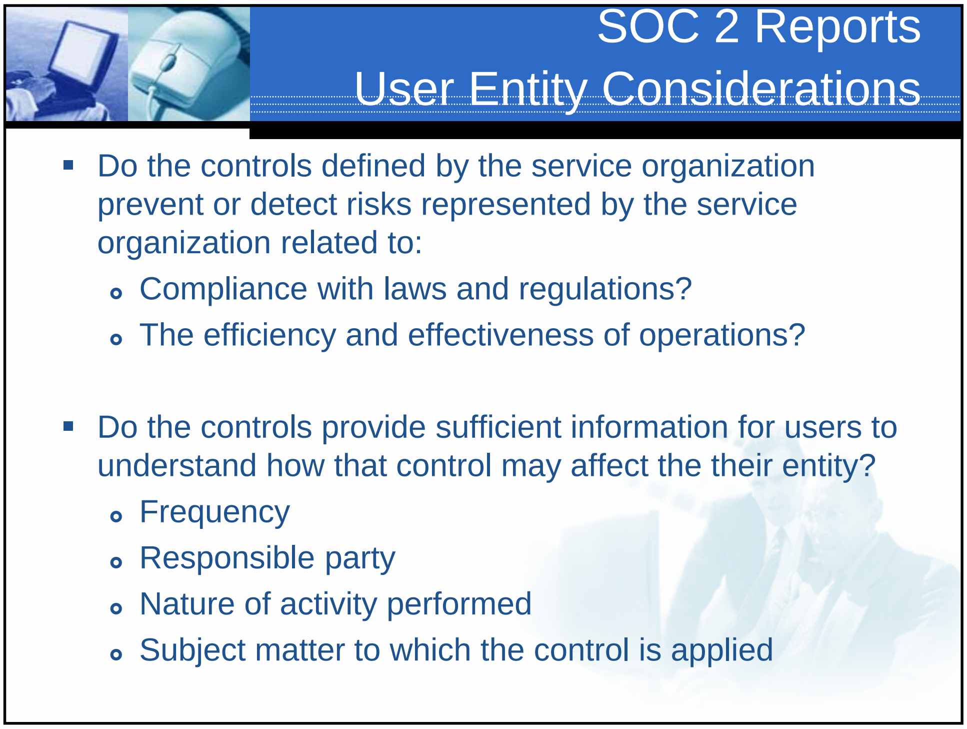
Uses for a SOC 2 Report

- User organizations can use SOC 2 reports to obtain supplementary information for:
  - Vendor management programs
  - Internal corporate governance and risk management processes
  - Regulatory compliance
- In all cases the user organization must:
  - Determine whether the controls implemented by the service organization address the user organization’s risks
  - Identify the complementary user entity controls that must be in place to meet the control objectives



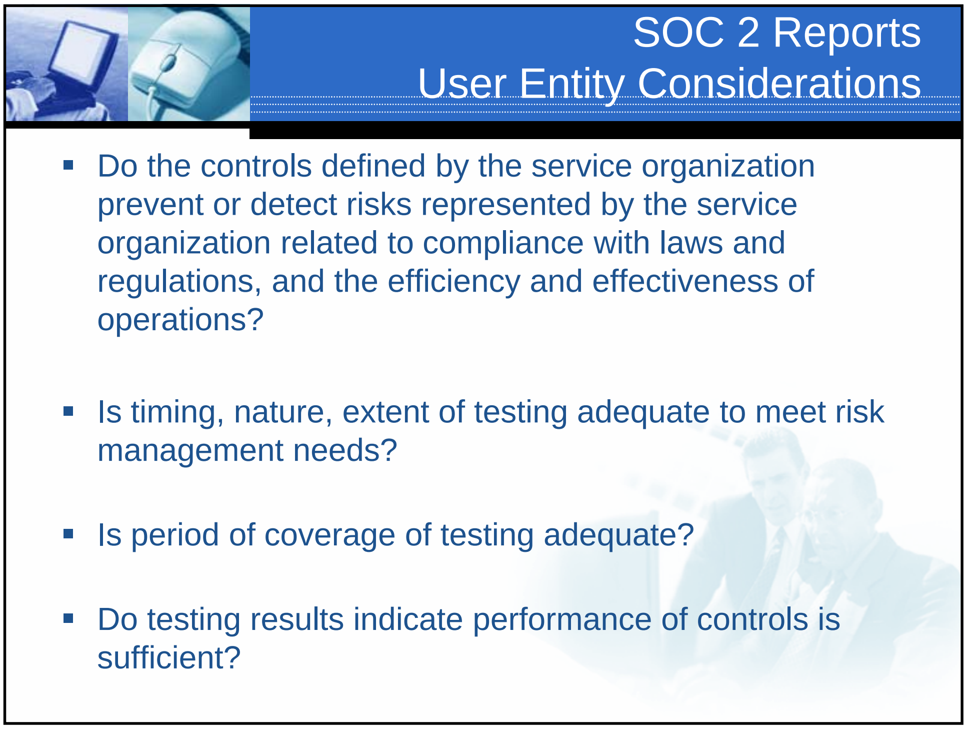
SOC 2 Reports
User Entity Considerations

- Understand the system
- Does the Principle(s) being reported on align to the user entity control requirements and risk management needs?
- Confirm that the System Description aligns to contracts & service level agreements (SLAs)
  - Does the Principle(s) being reported on align to the user entity control requirements and risk management needs?



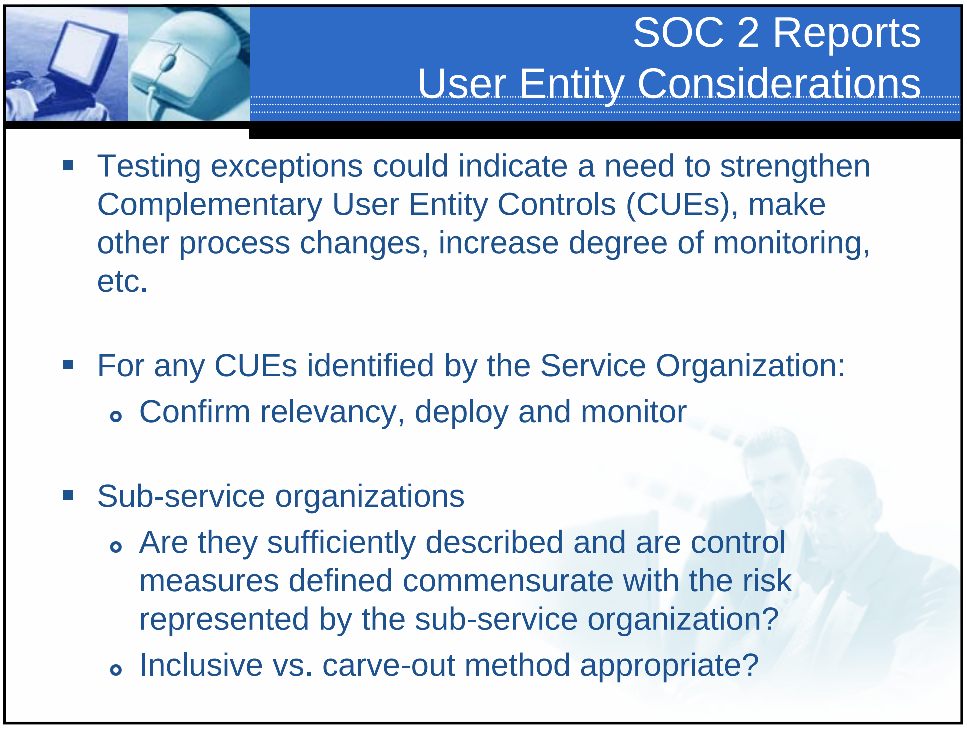
SOC 2 Reports
User Entity Considerations

- Do the controls defined by the service organization prevent or detect risks represented by the service organization related to:
  - Compliance with laws and regulations?
  - The efficiency and effectiveness of operations?
- Do the controls provide sufficient information for users to understand how that control may affect the their entity?
  - Frequency
  - Responsible party
  - Nature of activity performed
  - Subject matter to which the control is applied



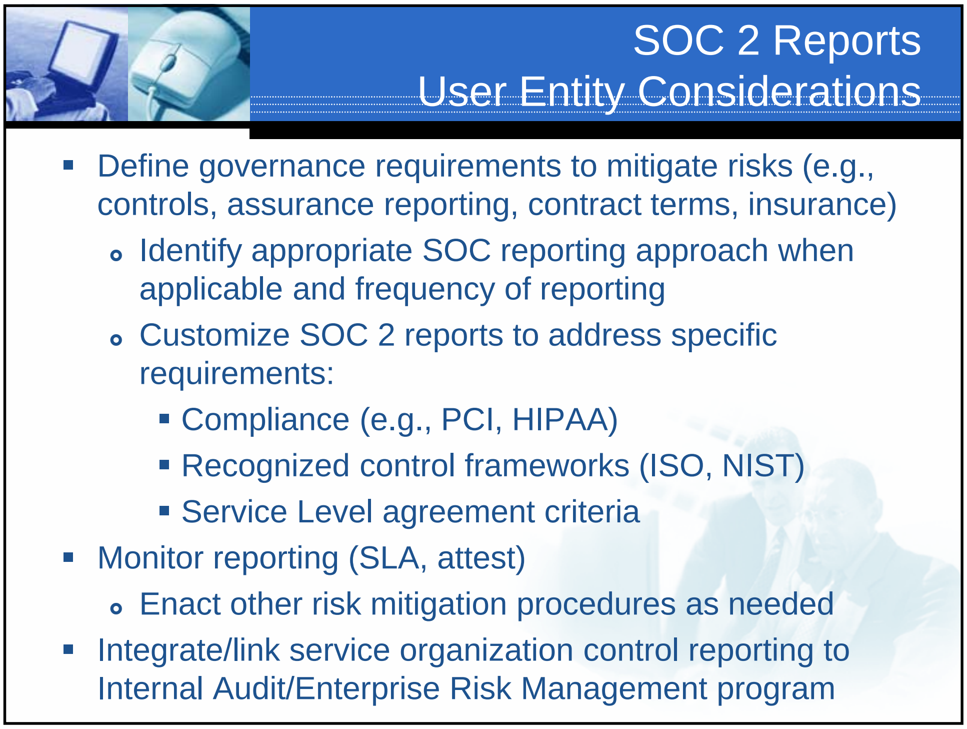
SOC 2 Reports
User Entity Considerations

- Do the controls defined by the service organization prevent or detect risks represented by the service organization related to compliance with laws and regulations, and the efficiency and effectiveness of operations?
- Is timing, nature, extent of testing adequate to meet risk management needs?
- Is period of coverage of testing adequate?
- Do testing results indicate performance of controls is sufficient?



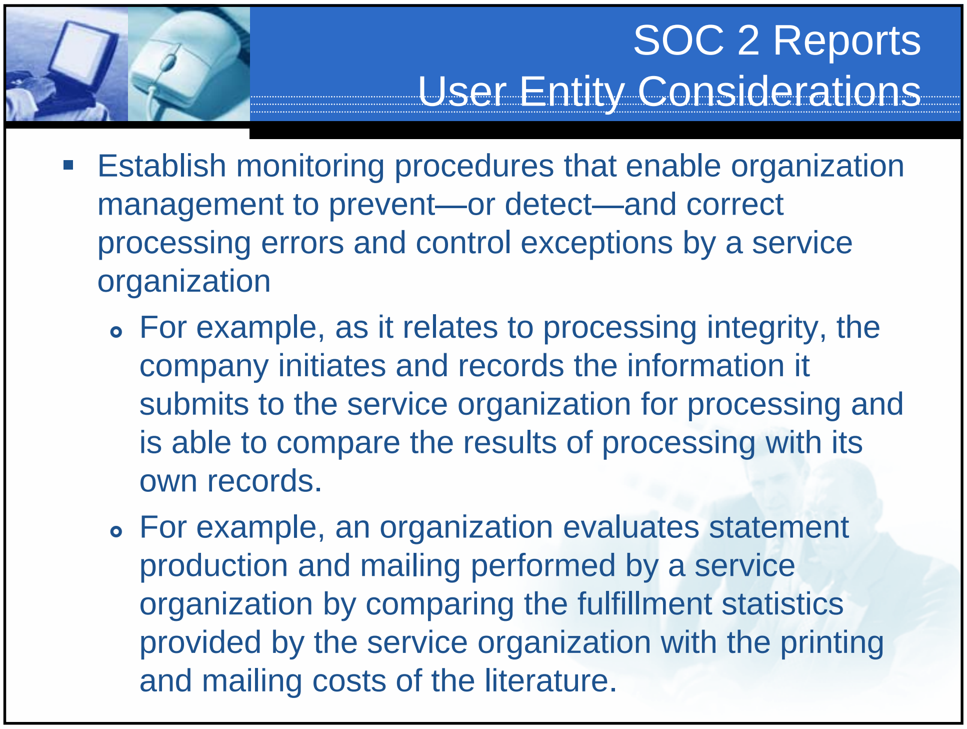
SOC 2 Reports
User Entity Considerations

- Testing exceptions could indicate a need to strengthen Complementary User Entity Controls (CUEs), make other process changes, increase degree of monitoring, etc.
- For any CUEs identified by the Service Organization:
  - Confirm relevancy, deploy and monitor
- Sub-service organizations
  - Are they sufficiently described and are control measures defined commensurate with the risk represented by the sub-service organization?
  - Inclusive vs. carve-out method appropriate?



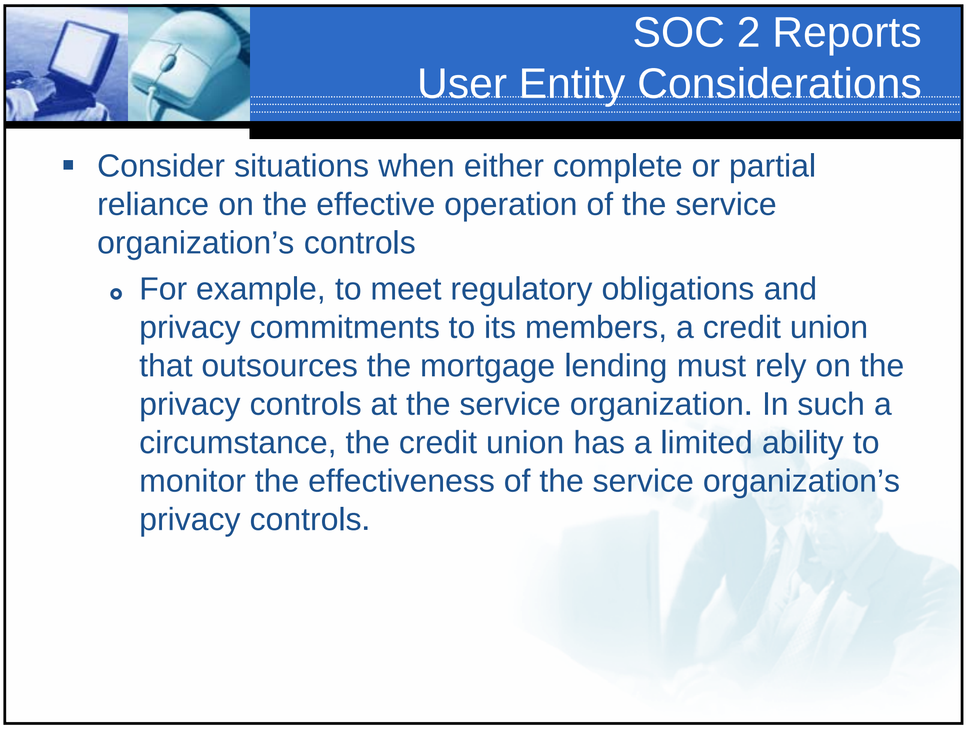
SOC 2 Reports
User Entity Considerations

- Define governance requirements to mitigate risks (e.g., controls, assurance reporting, contract terms, insurance)
  - Identify appropriate SOC reporting approach when applicable and frequency of reporting
  - Customize SOC 2 reports to address specific requirements:
    - Compliance (e.g., PCI, HIPAA)
    - Recognized control frameworks (ISO, NIST)
    - Service Level agreement criteria
- Monitor reporting (SLA, attest)
  - Enact other risk mitigation procedures as needed
- Integrate/link service organization control reporting to Internal Audit/Enterprise Risk Management program



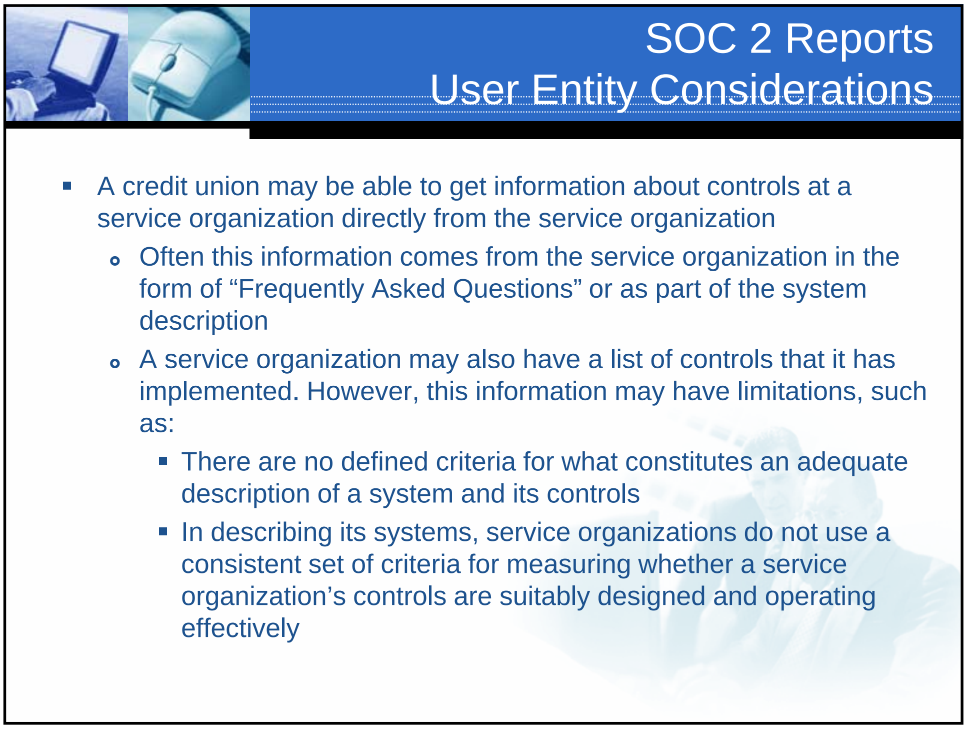
SOC 2 Reports
User Entity Considerations

- Establish monitoring procedures that enable organization management to prevent—or detect—and correct processing errors and control exceptions by a service organization
  - For example, as it relates to processing integrity, the company initiates and records the information it submits to the service organization for processing and is able to compare the results of processing with its own records.
  - For example, an organization evaluates statement production and mailing performed by a service organization by comparing the fulfillment statistics provided by the service organization with the printing and mailing costs of the literature.



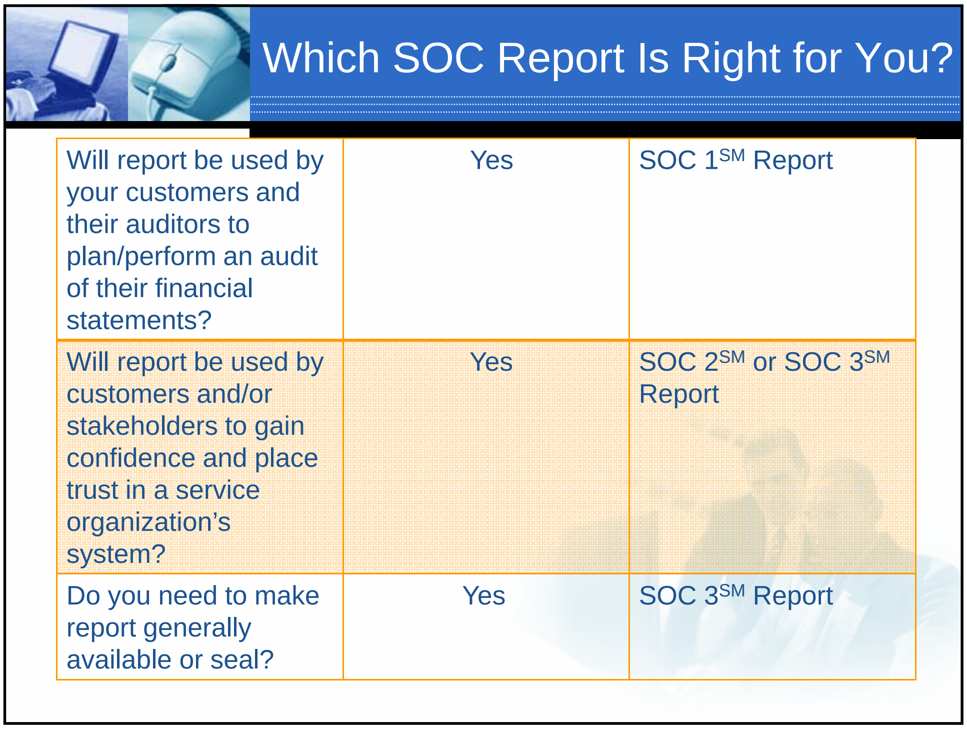
SOC 2 Reports
User Entity Considerations

- Consider situations when either complete or partial reliance on the effective operation of the service organization’s controls
  - For example, to meet regulatory obligations and privacy commitments to its members, a credit union that outsources the mortgage lending must rely on the privacy controls at the service organization. In such a circumstance, the credit union has a limited ability to monitor the effectiveness of the service organization’s privacy controls.



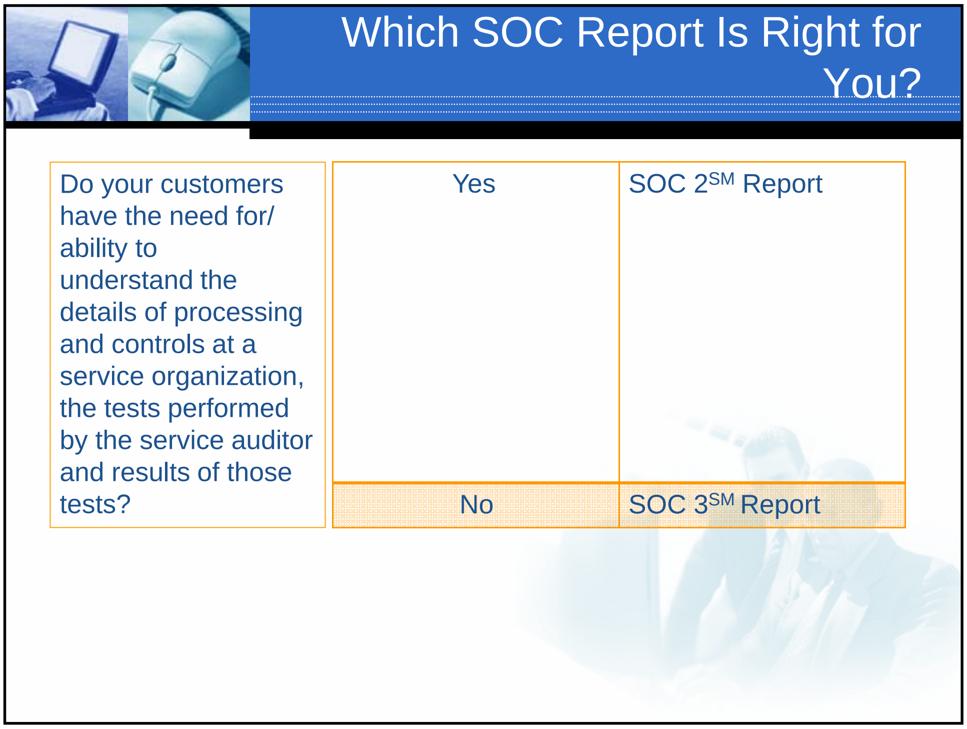
SOC 2 Reports
User Entity Considerations

- A credit union may be able to get information about controls at a service organization directly from the service organization
  - Often this information comes from the service organization in the form of “Frequently Asked Questions” or as part of the system description
  - A service organization may also have a list of controls that it has implemented. However, this information may have limitations, such as:
    - There are no defined criteria for what constitutes an adequate description of a system and its controls
    - In describing its systems, service organizations do not use a consistent set of criteria for measuring whether a service organization’s controls are suitably designed and operating effectively



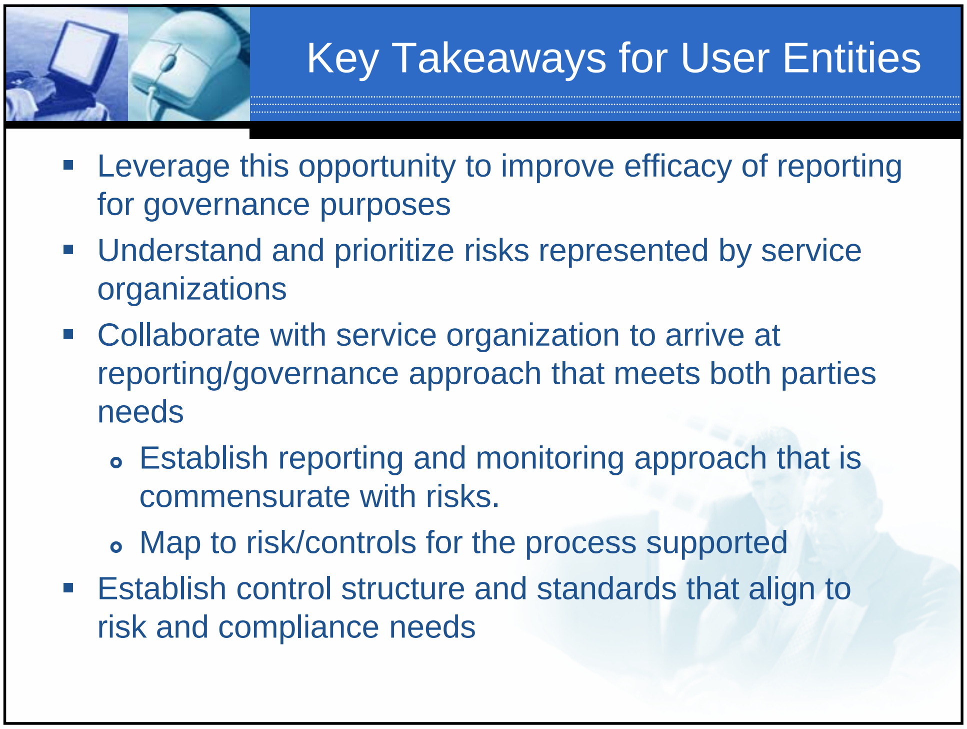
Which SOC Report Is Right for You?

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



Which SOC Report Is Right for You?

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^{SM} Report
	No	SOC 3^{SM} Report



Key Takeaways for User Entities

- Leverage this opportunity to improve efficacy of reporting for governance purposes
- Understand and prioritize risks represented by service organizations
- Collaborate with service organization to arrive at reporting/governance approach that meets both parties needs
  - Establish reporting and monitoring approach that is commensurate with risks.
  - Map to risk/controls for the process supported
- Establish control structure and standards that align to risk and compliance needs

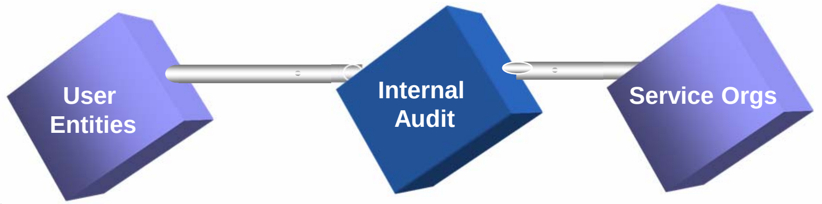
Key Takeaways for User Entities

- Do not assume that legacy SAS 70 reports naturally convert to SSAE 16/SOC 1
  - SOC 2 may be more appropriate
  - SOC 1 and SOC 2 together may be more appropriate
- Contracts with Service Organizations:
  - Write reporting requirements into contract before closing deal
  - Revise existing contracts to reflect change represented by SOC
- Vendor management
  - Leverage SOC reporting to minimize questionnaires

Additional Takeaways

- SOC 2 engagements
  - designed to meet the needs of service organization users and other stakeholders
  - provide organizations that outsource tasks and functions a mechanism for improving governance and oversight of service providers
  - enable service organizations to communicate the suitability of the design and operating effectiveness of their controls through a widely accepted reporting format.
  - Type 1 and Type 2

Summary Thoughts



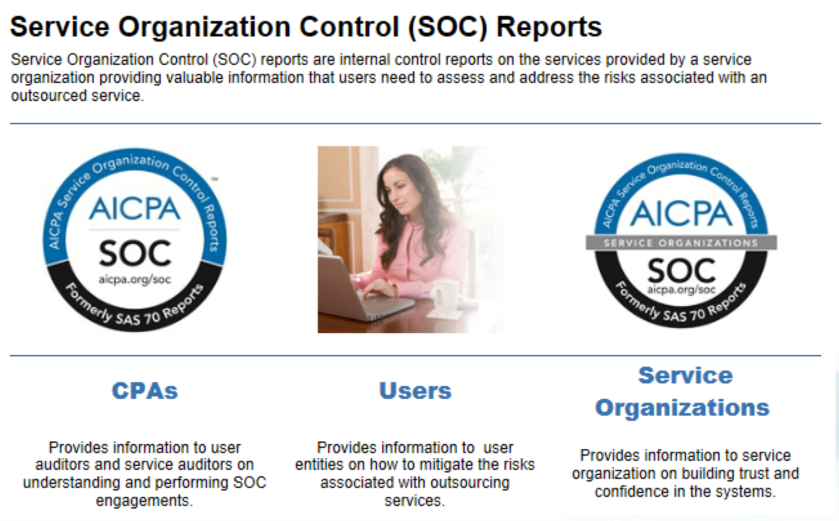
- System Description/Boundaries
- User Controls
- Relationship with Service Orgs
- Nature of Services
- Inherent Risk
- Internal Control

- Understand the standards
- Evaluate your needs
- Talk to your clients (both service orgs and users)

- Assertion
- Management Representation System Description / Boundaries
- User needs

Which report? – SAS 70 in the past does not mean SOC 1 going forward

AICPA Resources



Service Organization Control (SOC) Reports

Service Organization Control (SOC) reports are internal control reports on the services provided by a service organization providing valuable information that users need to assess and address the risks associated with an outsourced service.

CPAs

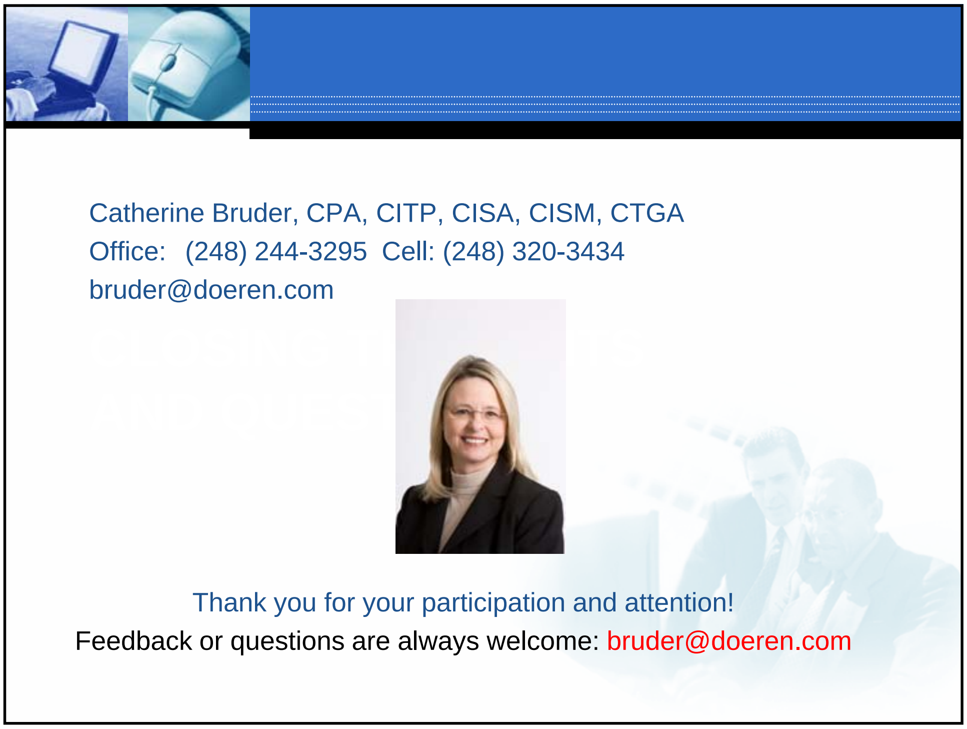
Provides information to user auditors and service auditors on understanding and performing SOC engagements.

Users

Provides information to user entities on how to mitigate the risks associated with outsourcing services.

Service Organizations

Provides information to service organization on building trust and confidence in the systems.



Catherine Bruder, CPA, CITP, CISA, CISM, CTGA
Office: (248) 244-3295 Cell: (248) 320-3434
bruder@doeren.com

Thank you for your participation and attention!

Feedback or questions are always welcome: bruder@doeren.com