The New Wave of IA

Catherine Bruder

CPA, CITP, CISA, CISM, CTGA

DoerenMayhew CPAs AND ADVISORS

Michigan ● Texas ● Florida

Insight. Oversight. Foresight. SM

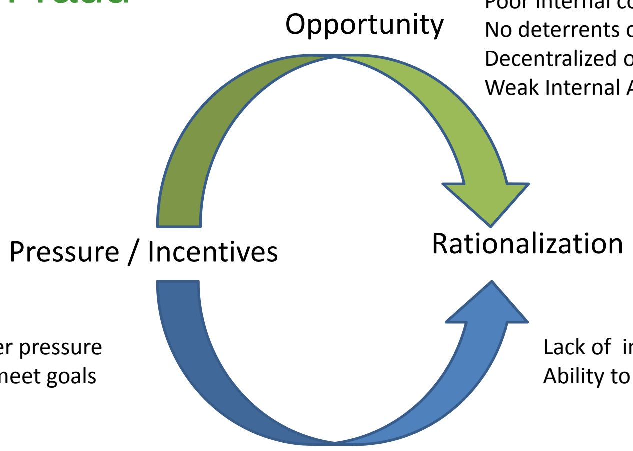
Fraud

DoerenMayhew CPAs AND ADVISORS

Insight. Oversight. Foresight. SM

Fraud

Cycle of Fraud



Poor internal controls
No deterrents or penalties
Decentralized organization
Weak Internal Audit

Lack of integrity
Ability to rationalize

Group or peer pressure
Pressure to meet goals
High stress

DoerenMayhew
CPAs AND ADVISORS

Fraud

Environment That Encourages Fraud

- Pressure or incentive
  - Meet expectations
  - Avoid criticism
  - Cover mistakes
- Perceived opportunity
  - Poor internal controls
  - Lack of oversight
- Rationalization
  - “I deserve more”

DoerenMayhew
CPAs AND ADVISORS

Fraud

Report To The Nations on Occupational Fraud and Abuse

DoerenMayhew
CPAs AND ADVISORS

REPORT TO THE NATIONS

ON OCCUPATIONAL **FRAUD** AND **ABUSE**

2012 GLOBAL FRAUD STUDY

ACFE®
Association of Certified Fraud Examiners

Together, Reducing Fraud Worldwide

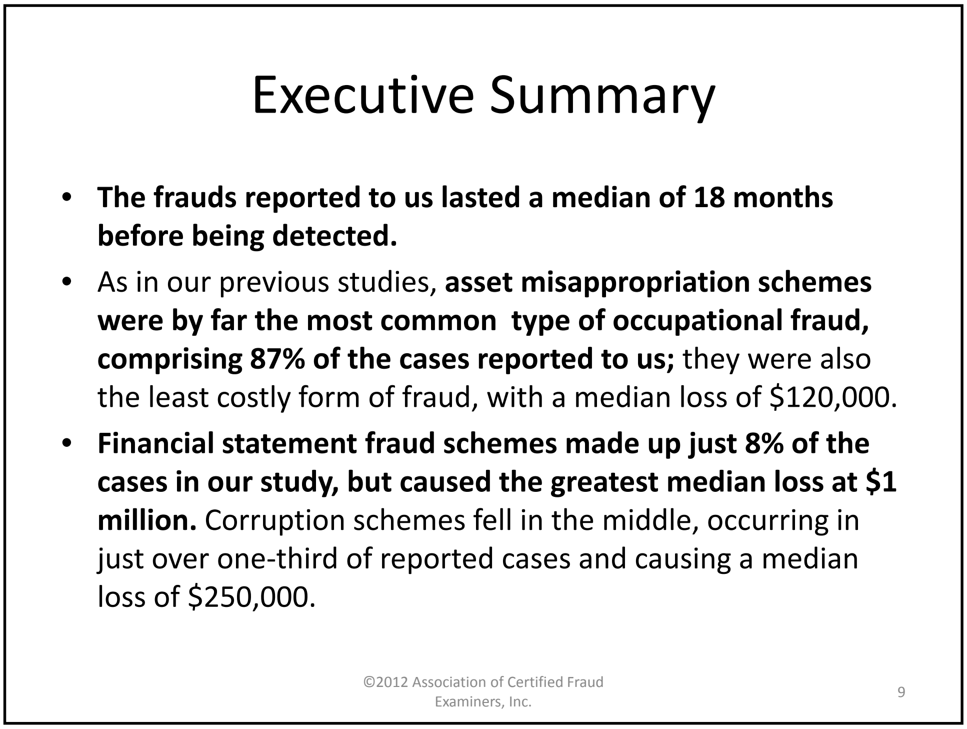
Executive Summary

More than one-fifth of frauds in our study caused at least $1 million in losses.

Executive Summary

Summary of Findings

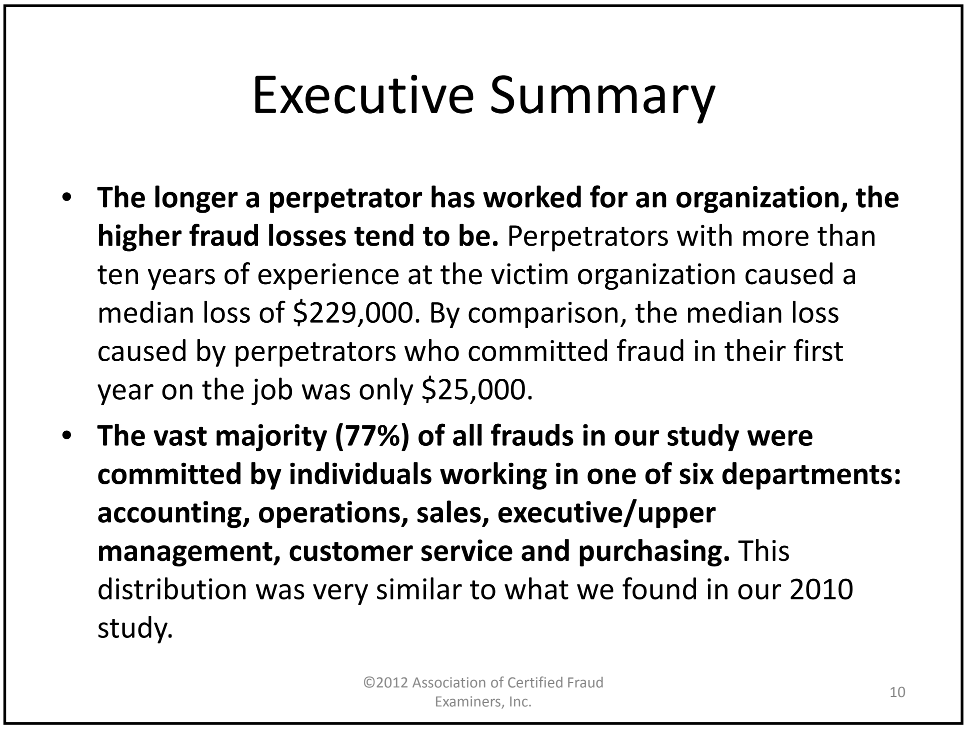
- **Survey participants estimated that the typical organization loses 5% of its revenues to fraud each year.** Applied to the 2011 Gross World Product, this figure translates to a potential projected annual fraud loss of more than $3.5 trillion.
- **The median loss caused by the occupational fraud cases in our study was $140,000.** More than one-fifth of these cases caused losses of at least $1 million.



Executive Summary

- **The frauds reported to us lasted a median of 18 months before being detected.**
- As in our previous studies, **asset misappropriation schemes were by far the most common type of occupational fraud, comprising 87% of the cases reported to us;** they were also the least costly form of fraud, with a median loss of $120,000.
- **Financial statement fraud schemes made up just 8% of the cases in our study, but caused the greatest median loss at $1 million.** Corruption schemes fell in the middle, occurring in just over one-third of reported cases and causing a median loss of $250,000.

9



Executive Summary

- **The longer a perpetrator has worked for an organization, the higher fraud losses tend to be.** Perpetrators with more than ten years of experience at the victim organization caused a median loss of $229,000. By comparison, the median loss caused by perpetrators who committed fraud in their first year on the job was only $25,000.
- **The vast majority (77%) of all frauds in our study were committed by individuals working in one of six departments: accounting, operations, sales, executive/upper management, customer service and purchasing.** This distribution was very similar to what we found in our 2010 study.

10

Executive Summary

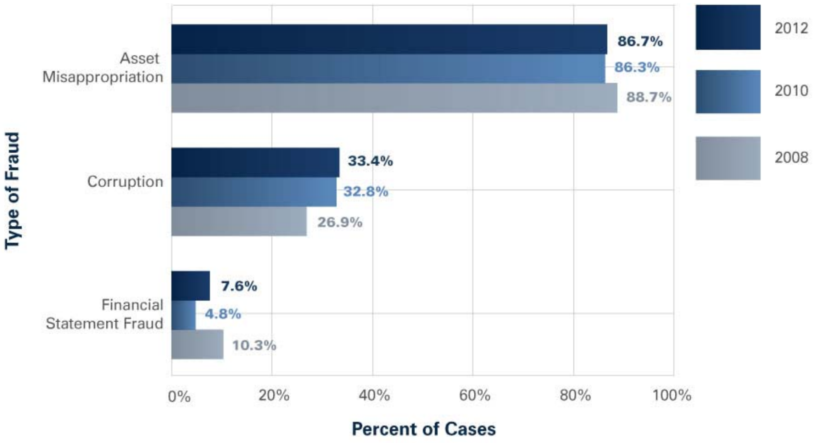
- **Most occupational fraudsters are first-time offenders with clean employment histories.** Approximately 87% of occupational fraudsters had never been charged or convicted of a fraud-related offense, and 84% had never been punished or terminated by an employer for fraud-related conduct.
- **In 81% of cases, the fraudster displayed one or more behavioral red flags that are often associated with fraudulent conduct.** Living beyond means (36% of cases), financial difficulties (27%), unusually close association with vendors or customers (19%) and excessive control issues (18%) were the most commonly observed behavioral warning signs.

Introduction

The term *fraud* has come to encompass many forms of misconduct.

How Occupational Fraud is Committed

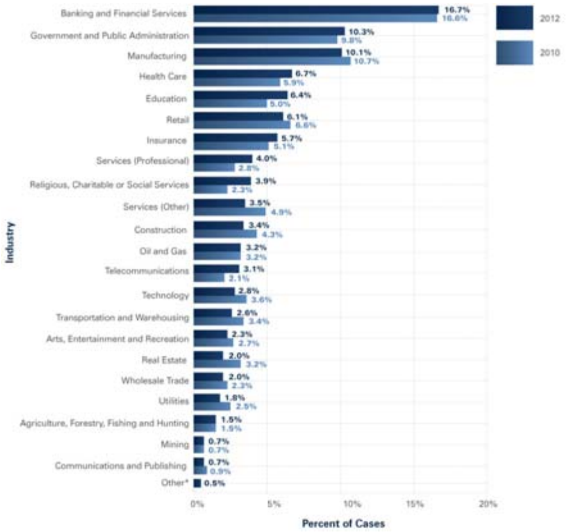
Occupational Frauds by Category — Frequency



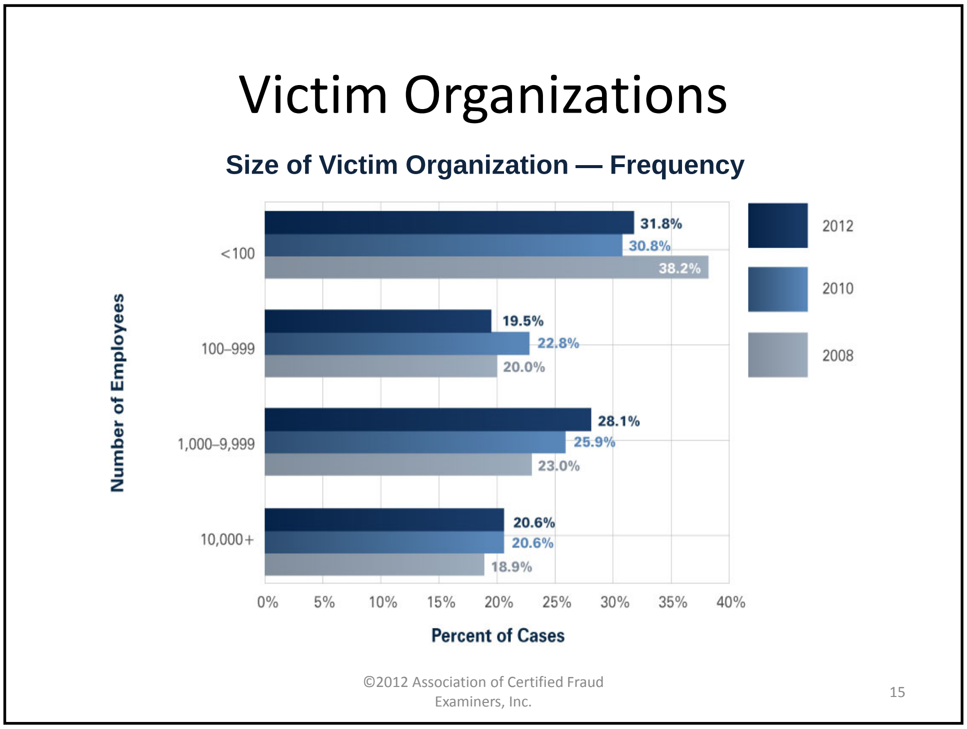
©2012 Association of Certified Fraud Examiners, Inc.

Victim Organizations

Industry of Victim Organizations



©2012 Association of Certified Fraud Examiners, Inc.

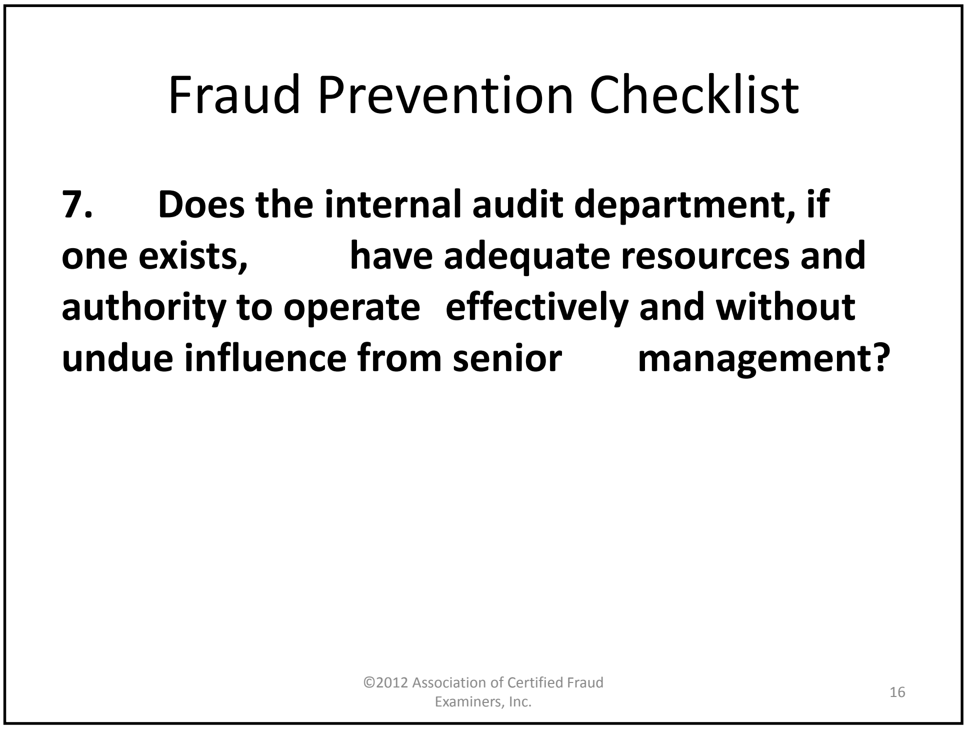


Victim Organizations

Size of Victim Organization — Frequency

©2012 Association of Certified Fraud Examiners, Inc.

15



Fraud Prevention Checklist

7. Does the internal audit department, if one exists, have adequate resources and authority to operate effectively and without undue influence from senior management?

©2012 Association of Certified Fraud Examiners, Inc.

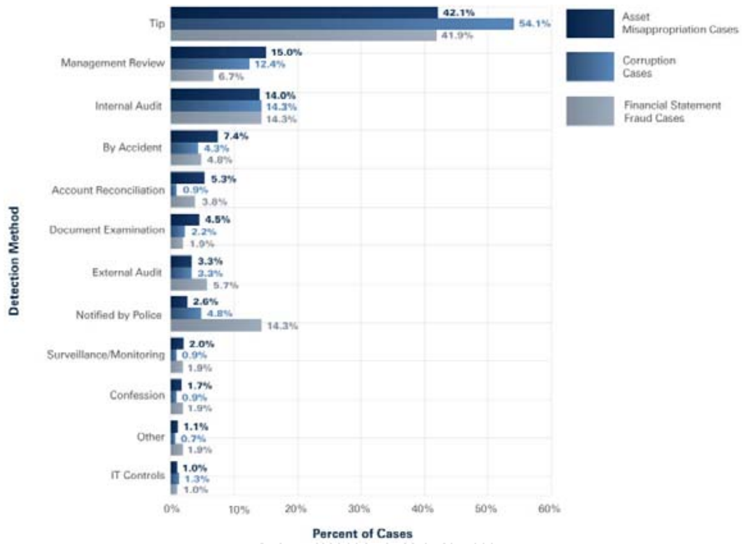
16

Detection of Fraud Schemes

- One interesting similarity in the data is the consistency with which internal audit was responsible for the detection of each scheme type. In each scheme category, 14% of the cases were detected through internal audits.

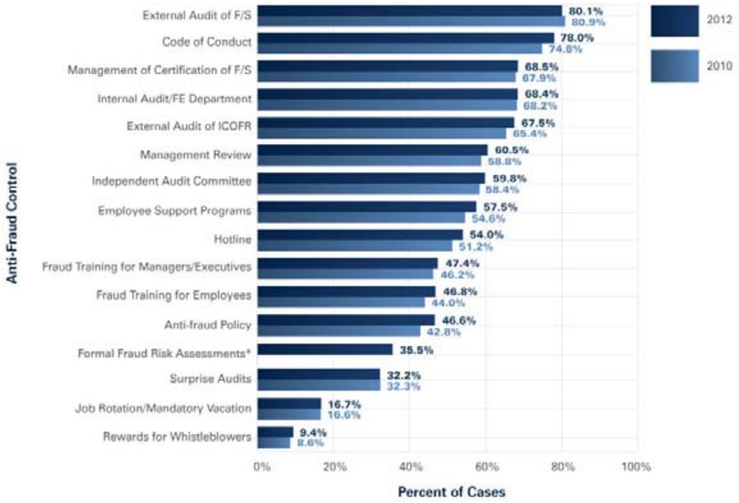
Detection of Fraud Schemes

Detection Method by Scheme Type



Victim Organizations

Frequency of Anti-Fraud Controls[8]



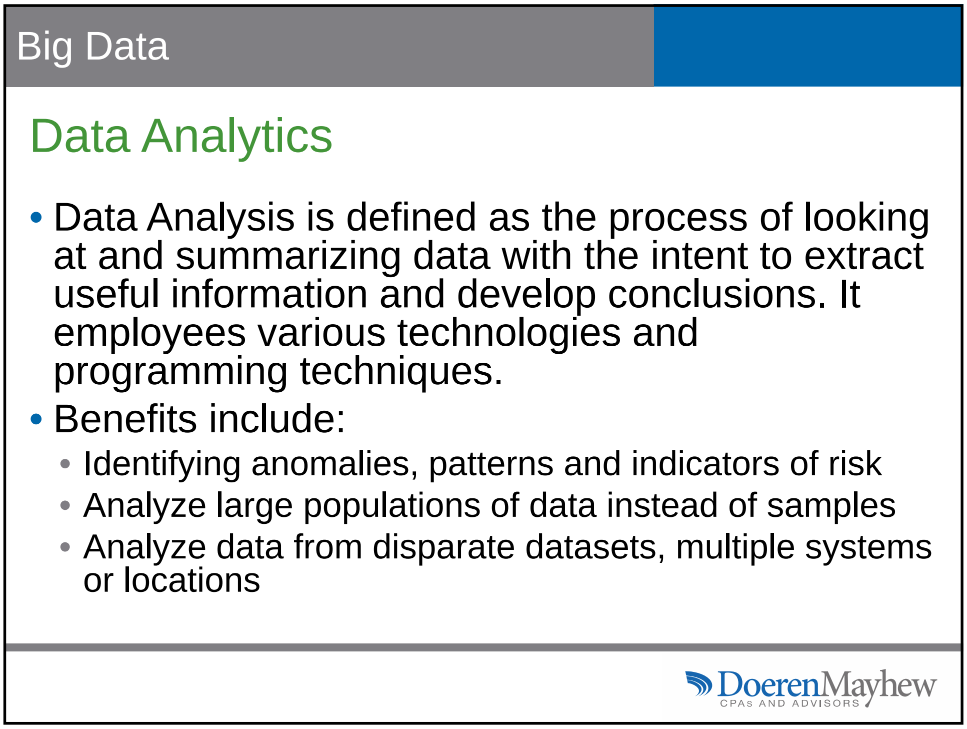
©2012 Association of Certified Fraud Examiners, Inc.

19

Big Data

DoerenMayhew
CPAs AND ADVISORS

Insight. Oversight. Foresight. SM

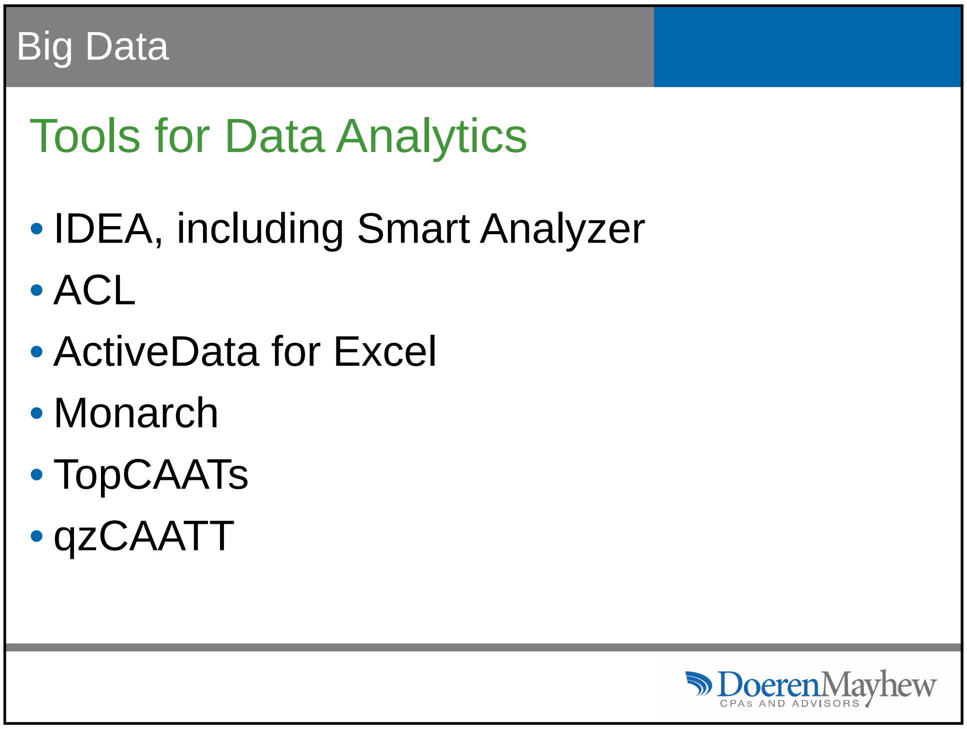


Big Data

Data Analytics

- Data Analysis is defined as the process of looking at and summarizing data with the intent to extract useful information and develop conclusions. It employees various technologies and programming techniques.
- Benefits include:
  - Identifying anomalies, patterns and indicators of risk
  - Analyze large populations of data instead of samples
  - Analyze data from disparate datasets, multiple systems or locations

DoerenMayhew
CPAs AND ADVISORS

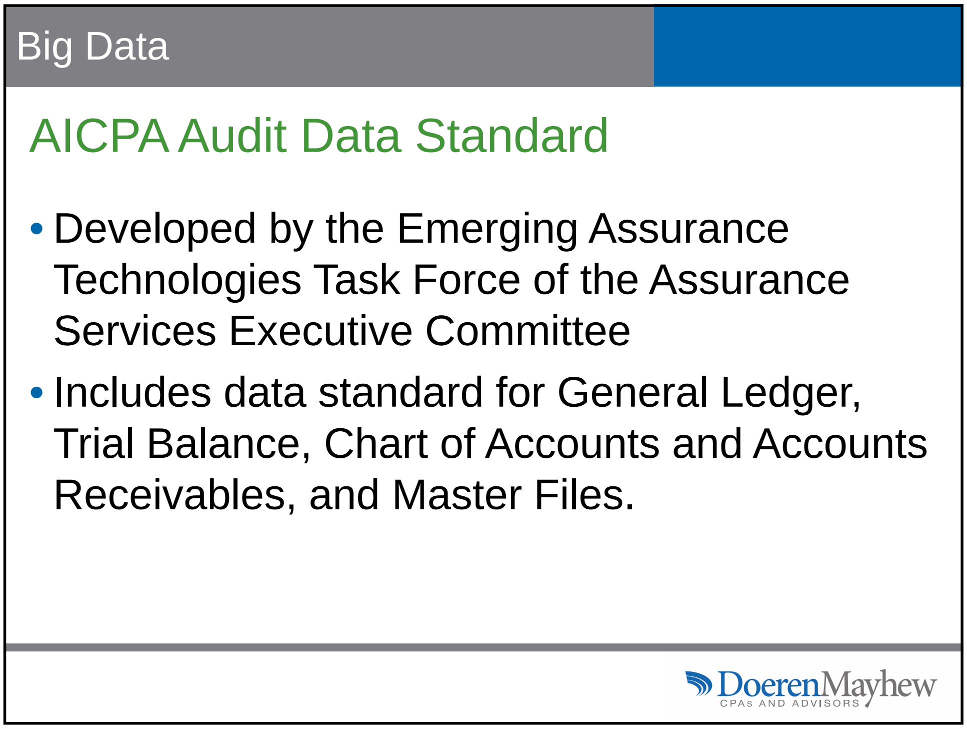


Big Data

Tools for Data Analytics

- IDEA, including Smart Analyzer
- ACL
- ActiveData for Excel
- Monarch
- TopCAATs
- qzCAATT

DoerenMayhew
CPAs AND ADVISORS

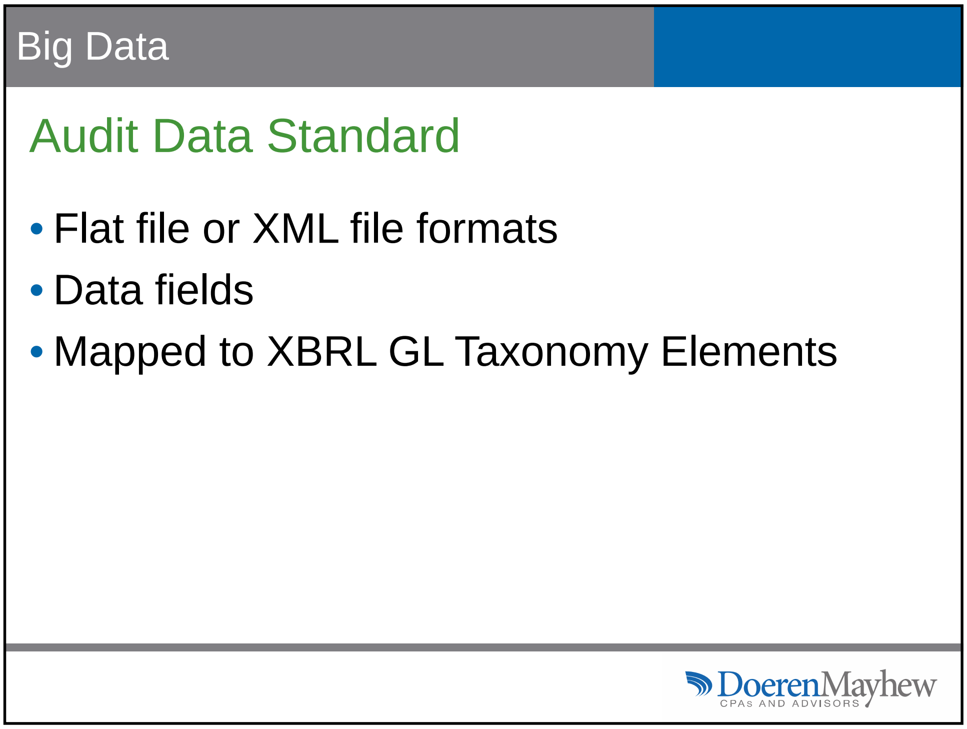


Big Data

AICPA Audit Data Standard

- Developed by the Emerging Assurance Technologies Task Force of the Assurance Services Executive Committee
- Includes data standard for General Ledger, Trial Balance, Chart of Accounts and Accounts Receivables, and Master Files.

DoerenMayhew CPAs AND ADVISORS

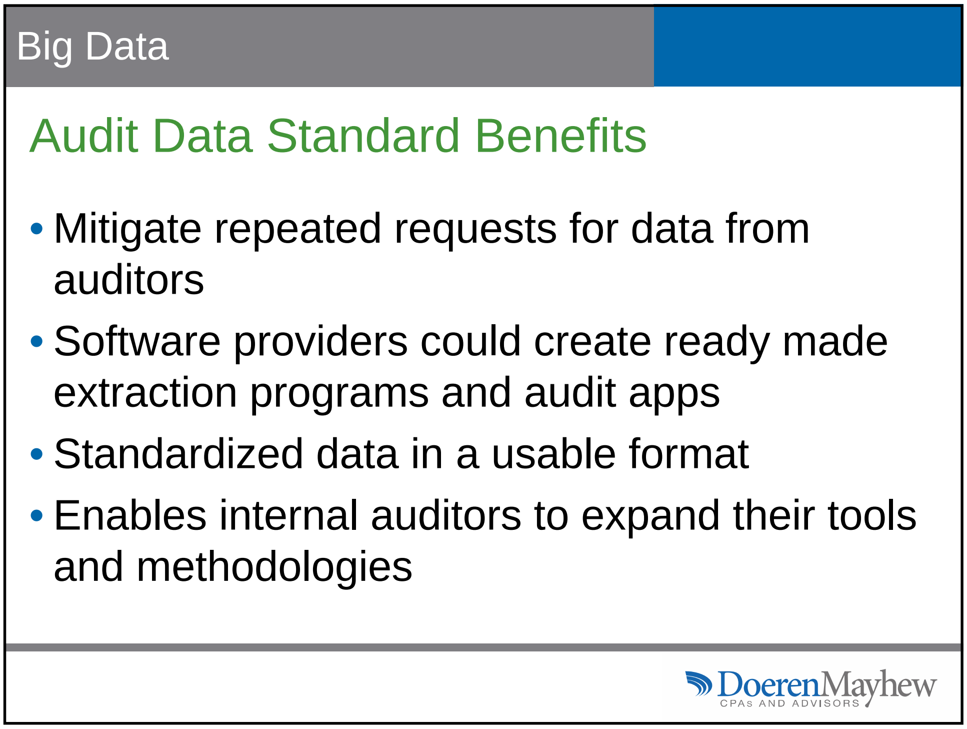


Big Data

Audit Data Standard

- Flat file or XML file formats
- Data fields
- Mapped to XBRL GL Taxonomy Elements

DoerenMayhew CPAs AND ADVISORS

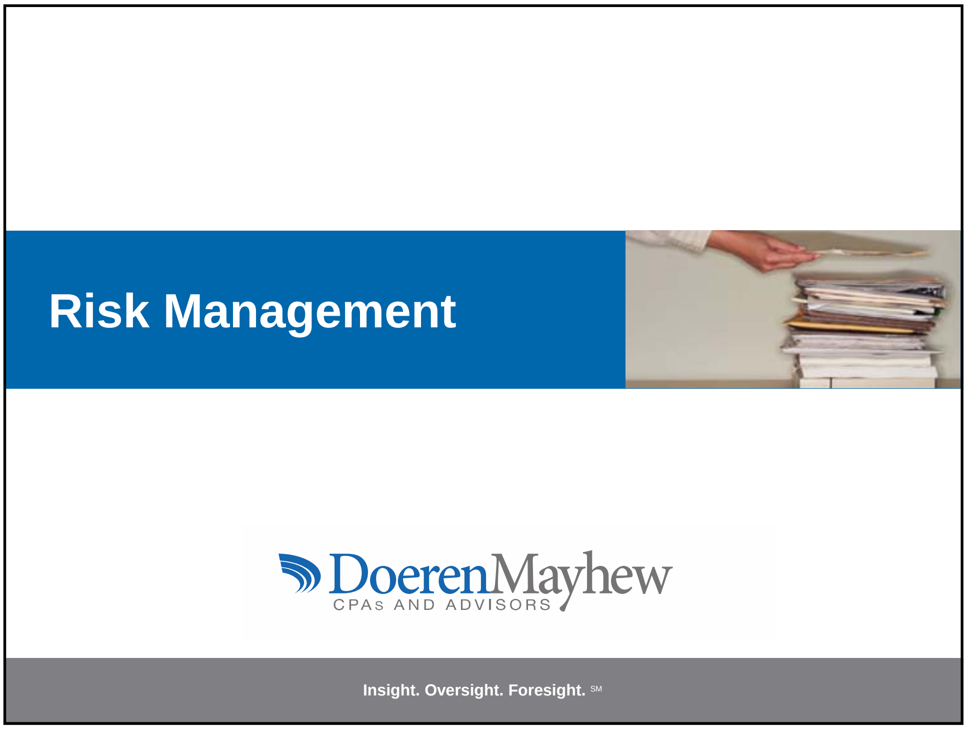


Big Data

Audit Data Standard Benefits

- Mitigate repeated requests for data from auditors
- Software providers could create ready made extraction programs and audit apps
- Standardized data in a usable format
- Enables internal auditors to expand their tools and methodologies

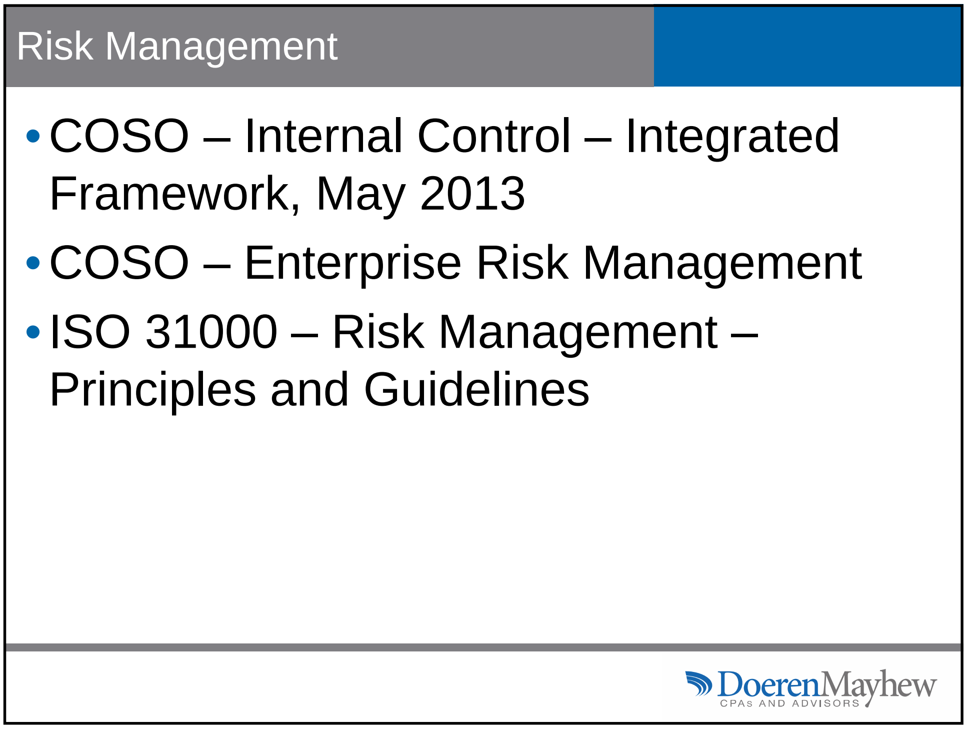
DoerenMayhew
CPAs AND ADVISORS



Risk Management

DoerenMayhew
CPAs AND ADVISORS

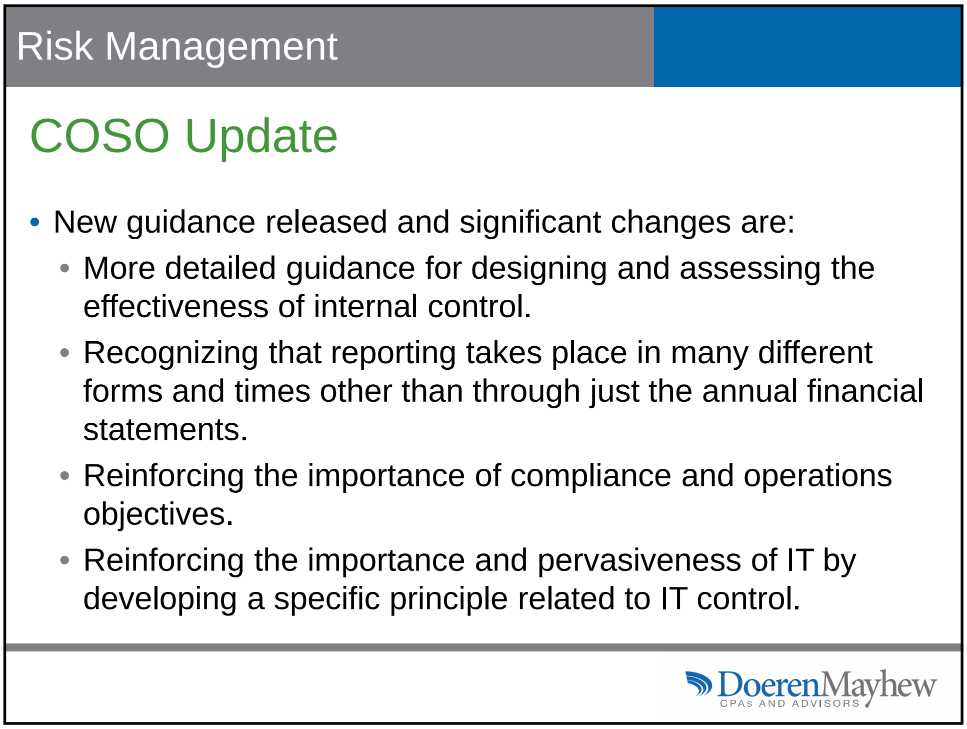
Insight. Oversight. Foresight. SM



Risk Management

- COSO – Internal Control – Integrated Framework, May 2013
- COSO – Enterprise Risk Management
- ISO 31000 – Risk Management – Principles and Guidelines

DoerenMayhew
CPAs AND ADVISORS

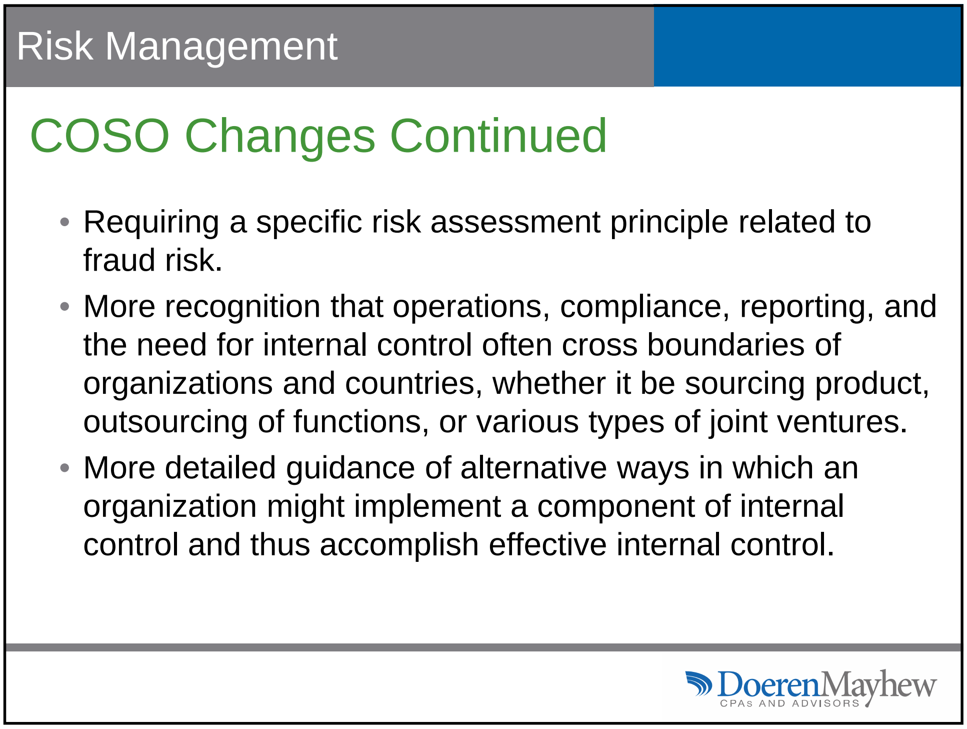


Risk Management

COSO Update

- New guidance released and significant changes are:
  - More detailed guidance for designing and assessing the effectiveness of internal control.
  - Recognizing that reporting takes place in many different forms and times other than through just the annual financial statements.
  - Reinforcing the importance of compliance and operations objectives.
  - Reinforcing the importance and pervasiveness of IT by developing a specific principle related to IT control.

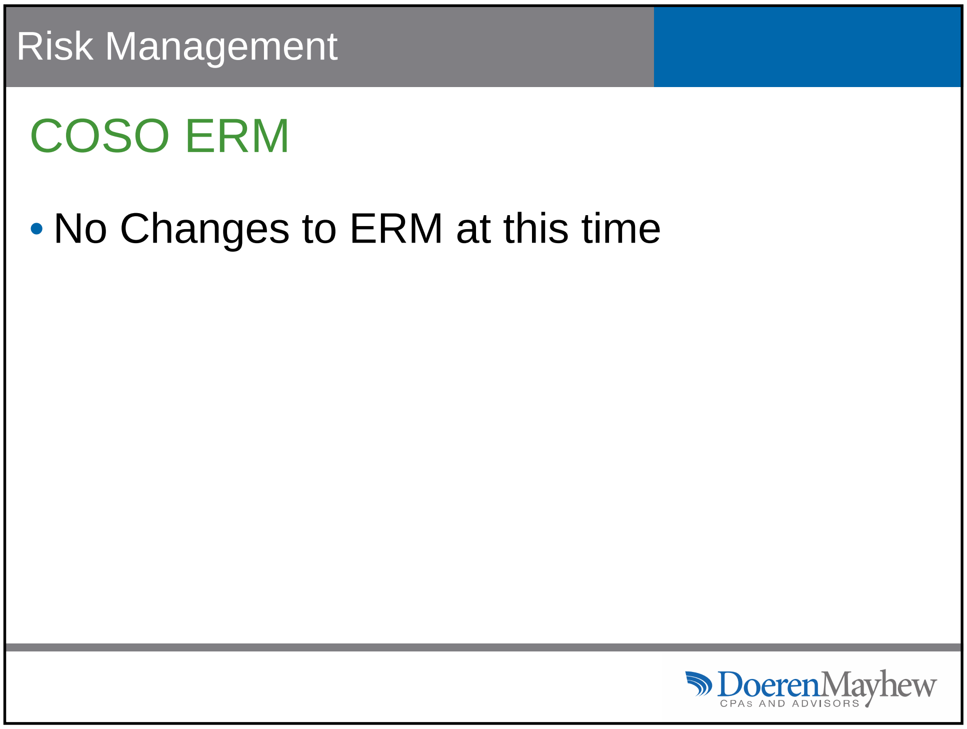
DoerenMayhew
CPAs AND ADVISORS



Risk Management

COSO Changes Continued

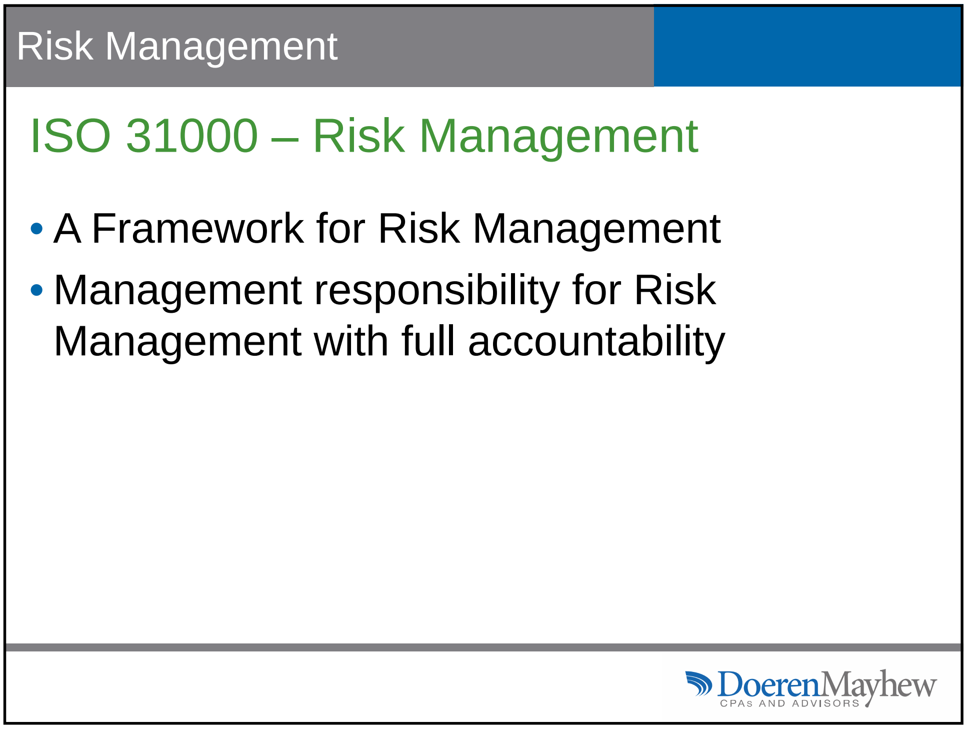
- Requiring a specific risk assessment principle related to fraud risk.
- More recognition that operations, compliance, reporting, and the need for internal control often cross boundaries of organizations and countries, whether it be sourcing product, outsourcing of functions, or various types of joint ventures.
- More detailed guidance of alternative ways in which an organization might implement a component of internal control and thus accomplish effective internal control.



Risk Management

COSO ERM

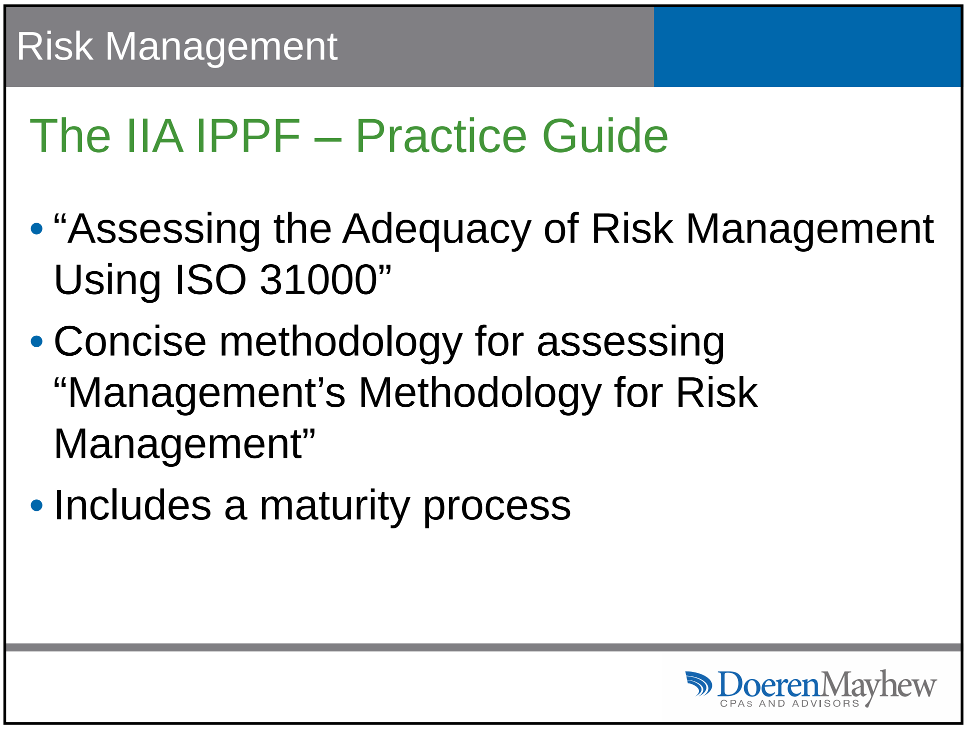
- No Changes to ERM at this time



Risk Management

ISO 31000 – Risk Management

- A Framework for Risk Management
- Management responsibility for Risk Management with full accountability



Risk Management

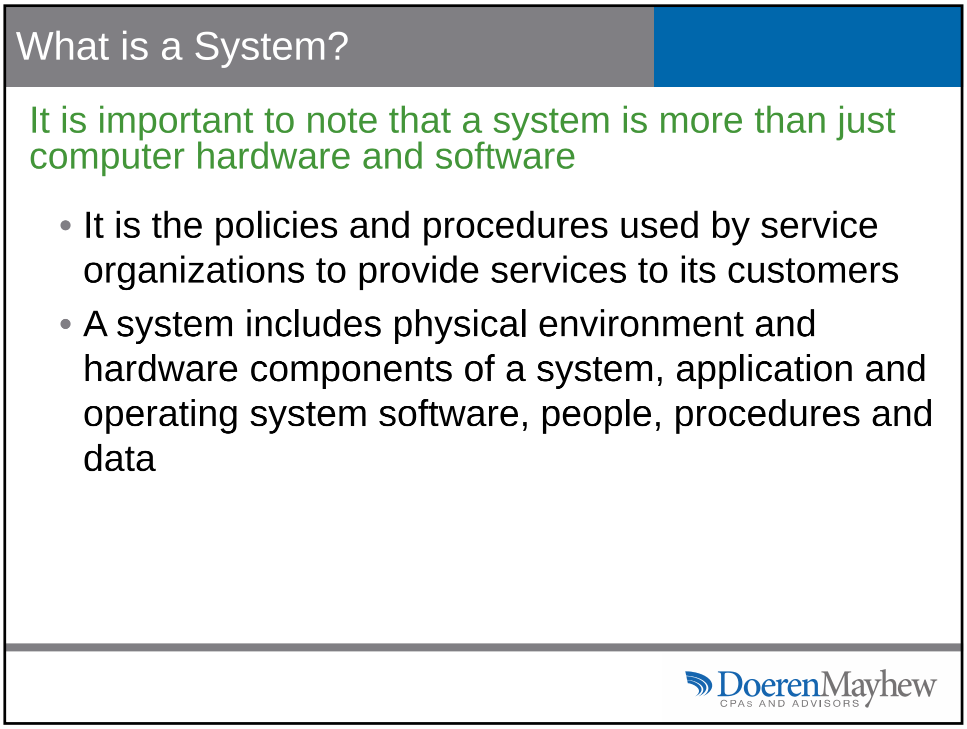
The IIA IPPF – Practice Guide

- “Assessing the Adequacy of Risk Management Using ISO 31000”
- Concise methodology for assessing “Management’s Methodology for Risk Management”
- Includes a maturity process

The Cloud

DoerenMayhew
CPAs AND ADVISORS

Insight. Oversight. Foresight. SM

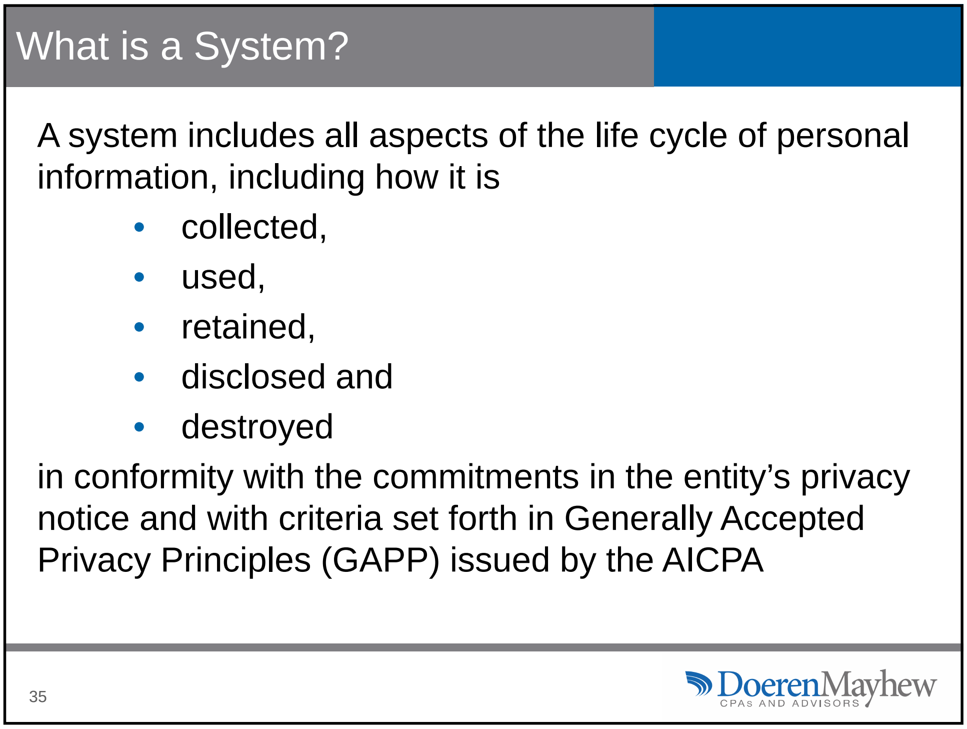


What is a System?

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

DoerenMayhew
CPAs AND ADVISORS

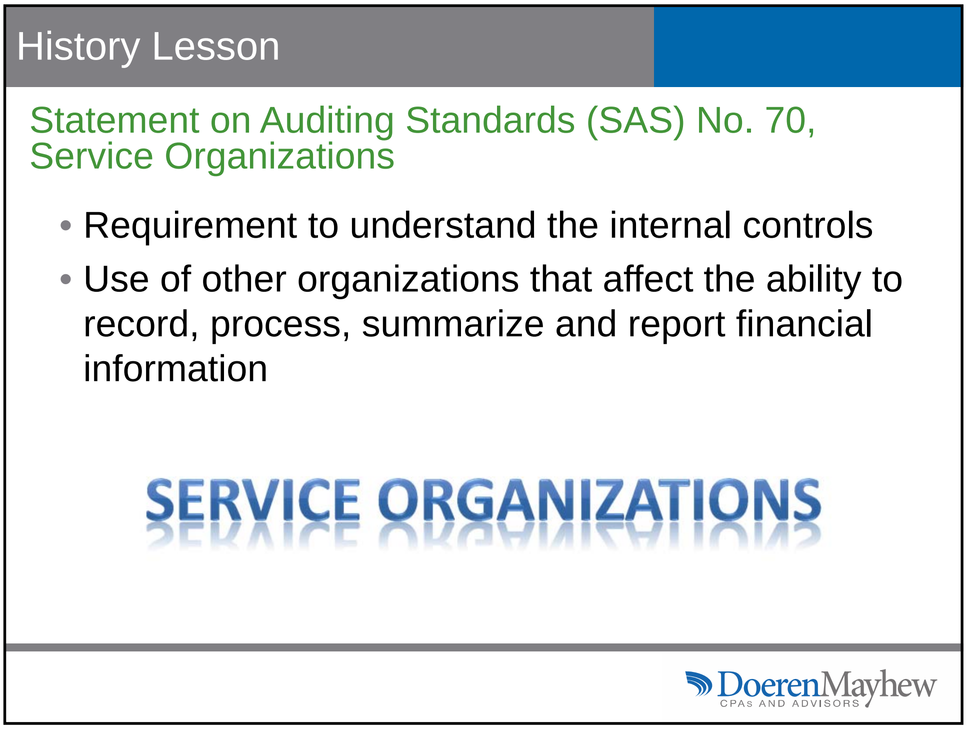


What is a System?

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



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

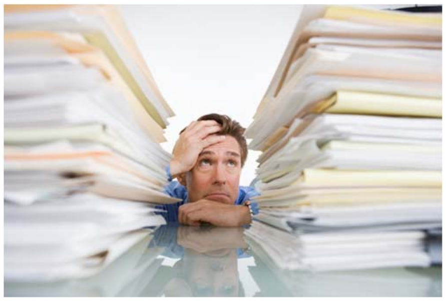
Examples of Service Organizations

- 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

DoerenMayhew
CPAs AND ADVISORS

SAS 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
- An Audit Standard

DoerenMayhew
CPAs AND ADVISORS

More than SAS 70

- 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

DoerenMayhew
CPAs AND ADVISORS

More than SAS 70

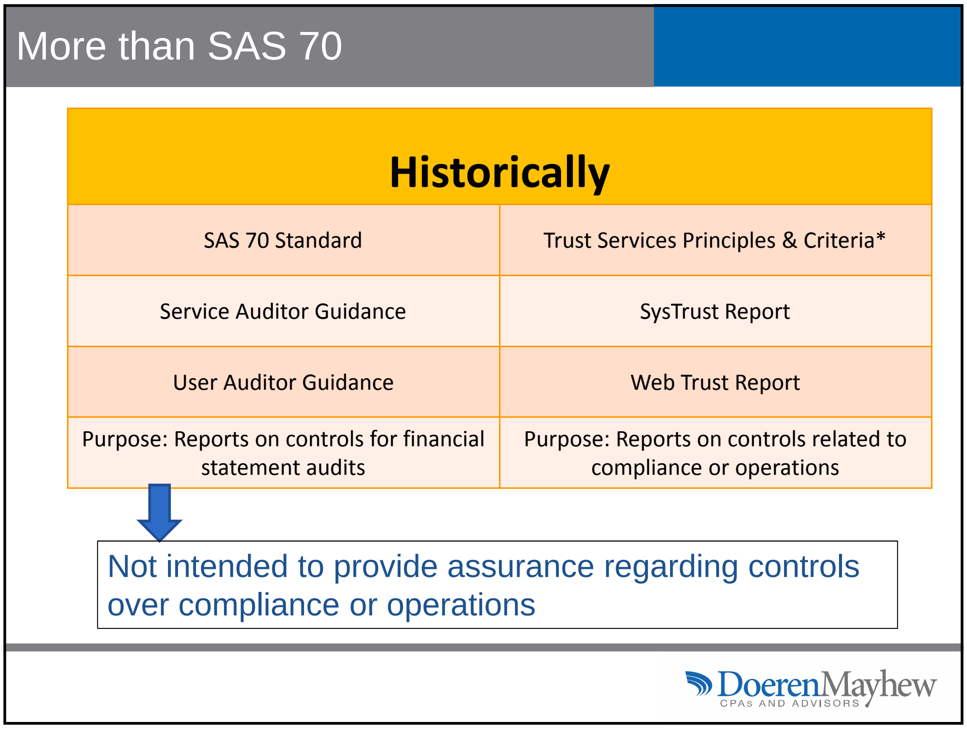
Trust Services Principles & Criteria

- Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy

SysTrust℠

Member of AICPA®

DoerenMayhew
CPAs AND ADVISORS

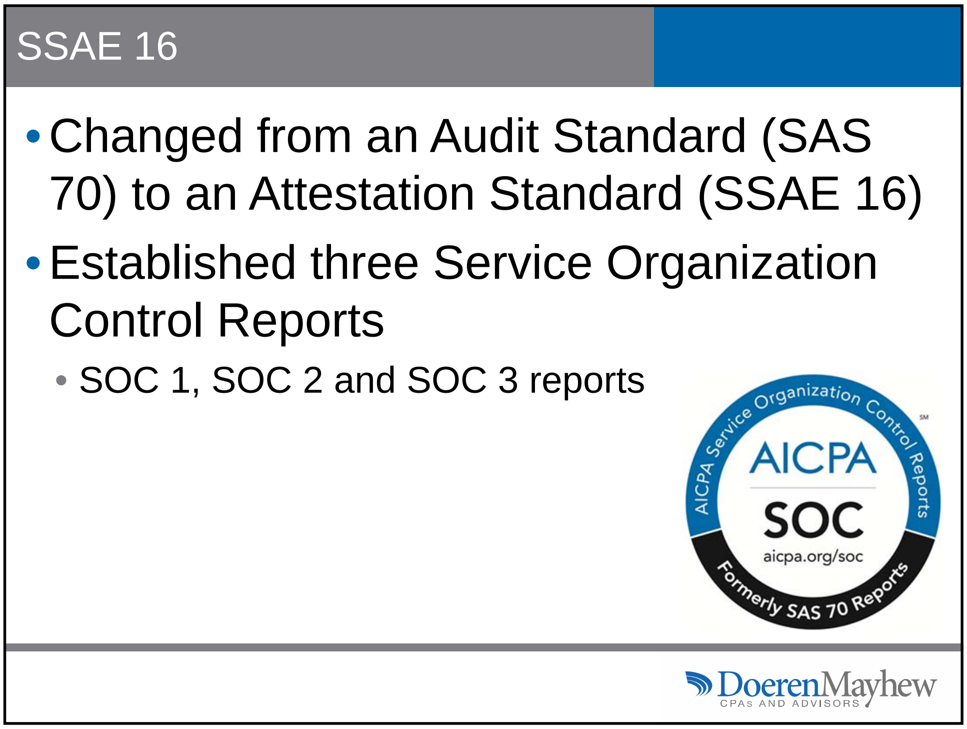


More than SAS 70

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

DoerenMayhew
CPAs AND ADVISORS



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

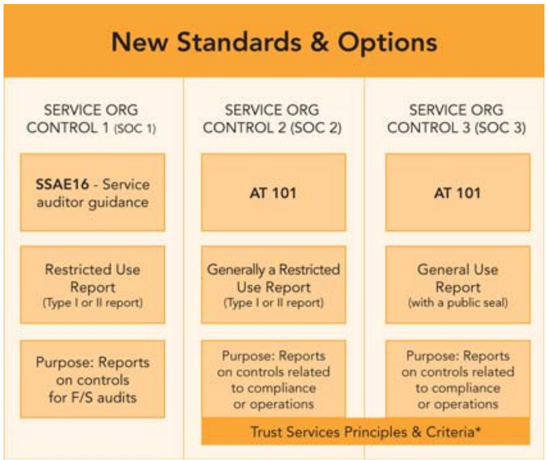
AICPA Service Organization Control Reports℠
AICPA
SOC
aicpa.org/soc
Formerly SAS 70 Reports

DoerenMayhew
CPAs AND ADVISORS

SOC Reports

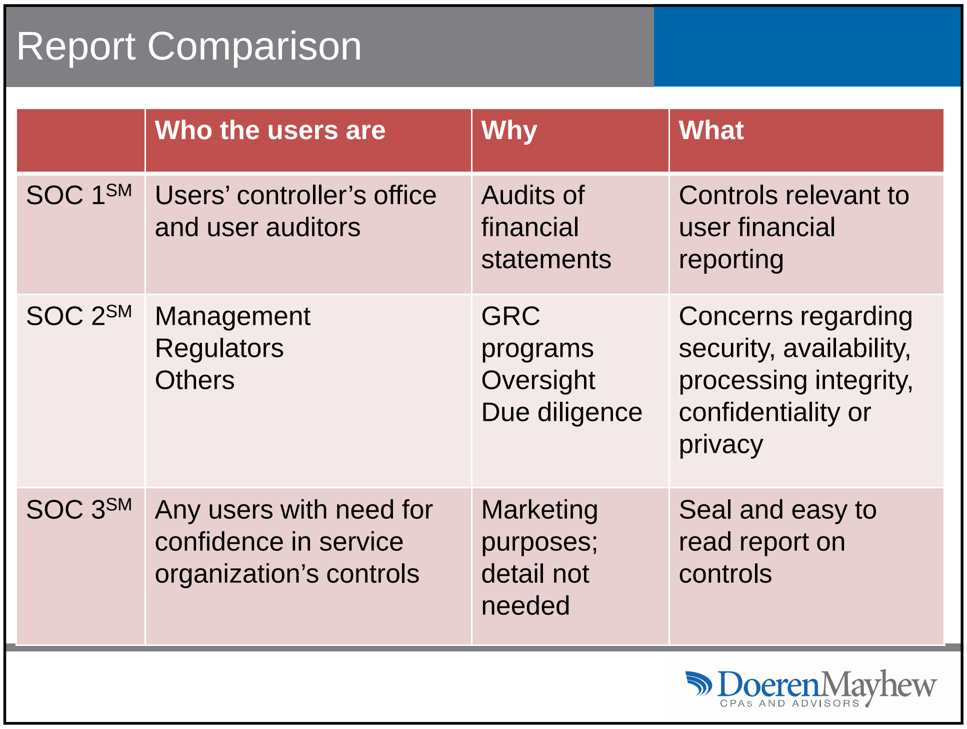
- SOC 1 reports are appropriate for service organizations whose customers are planning or performing an audit of their financial statements
- SOC 2 reports to report on the effectiveness of a Service Organization’s controls related to operations and compliance
- SOC 3, similar to SOC 2 if the report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

New Standard and Names



New Standards & Options

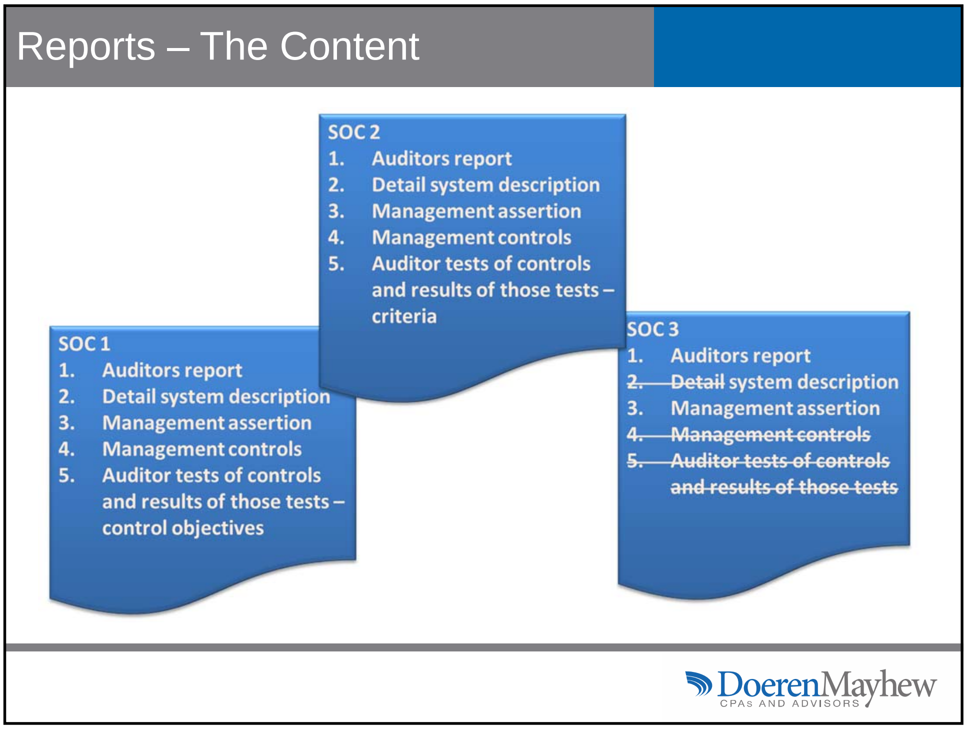
SERVICE ORG CONTROL 1 (SOC 1)	SERVICE ORG CONTROL 2 (SOC 2)	SERVICE ORG CONTROL 3 (SOC 3)
SSAE16 - Service auditor guidance	**AT 101**	**AT 101**
Restricted Use Report (Type I or II report)	Generally a Restricted Use Report (Type I or II report)	General Use Report (with a public seal)
Purpose: Reports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



Report Comparison

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

DoerenMayhew
CPAs AND ADVISORS



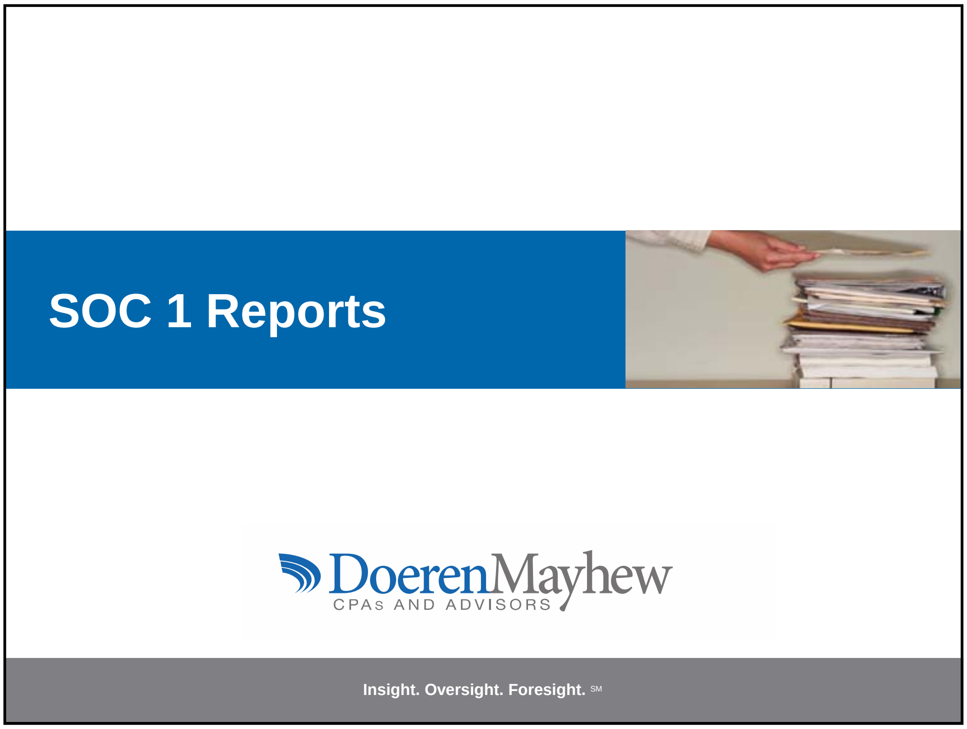
Reports – The Content

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

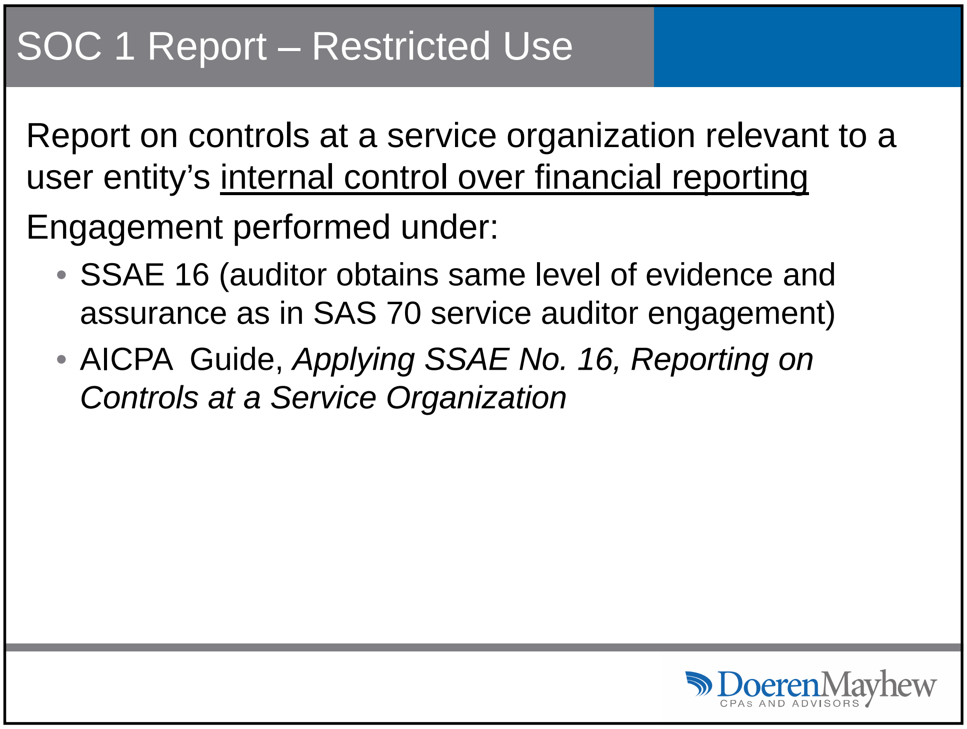
DoerenMayhew
CPAs AND ADVISORS



SOC 1 Reports

DoerenMayhew CPAs AND ADVISORS

Insight. Oversight. Foresight. SM



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*

DoerenMayhew CPAs AND ADVISORS

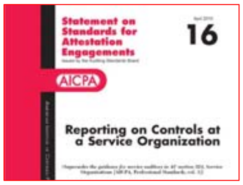
New Requirement for Assertion

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 – Types 1 & 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

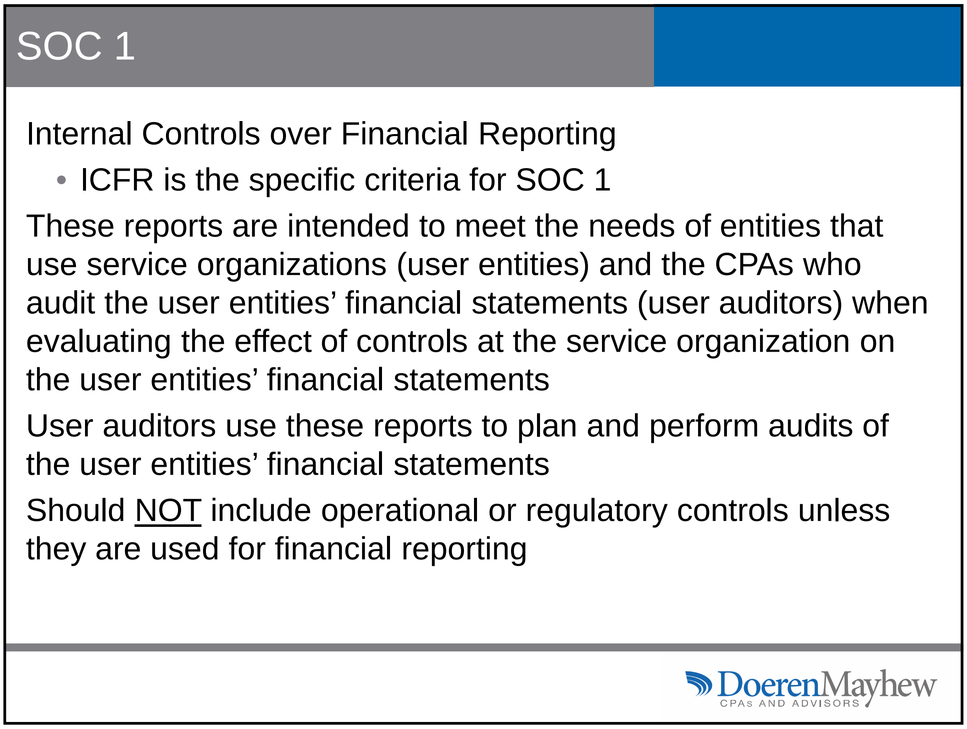
Reporting on Controls at a Service Organization

G U I D E

Service Organizations

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

JUNE 1, 2011



SOC 1

Internal Controls over Financial Reporting

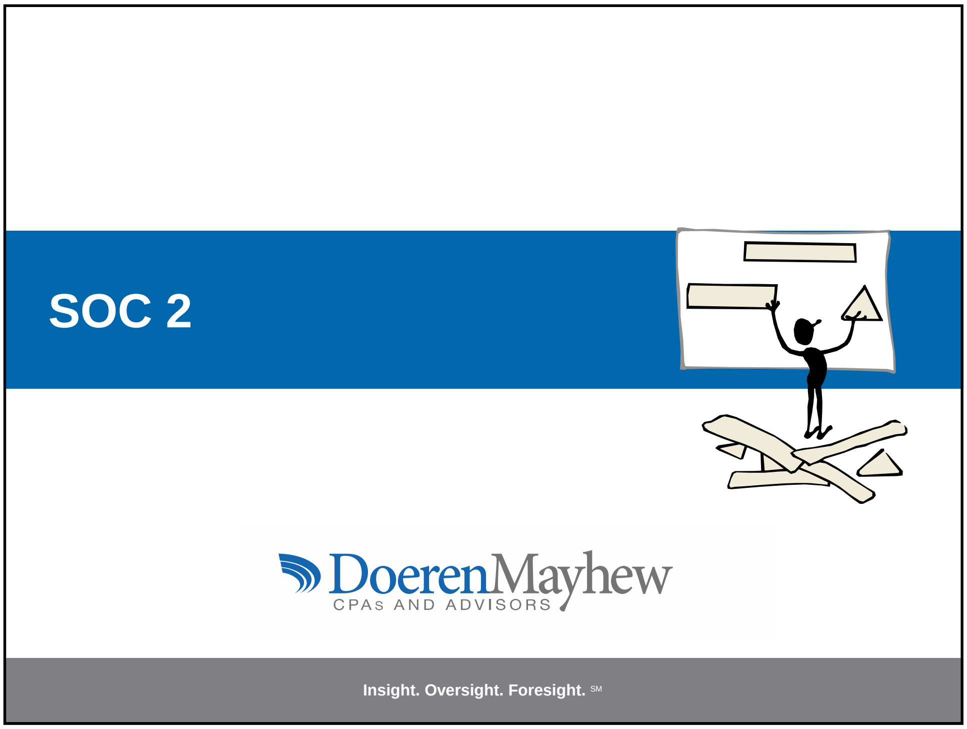
- ICFR is the specific criteria for SOC 1

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

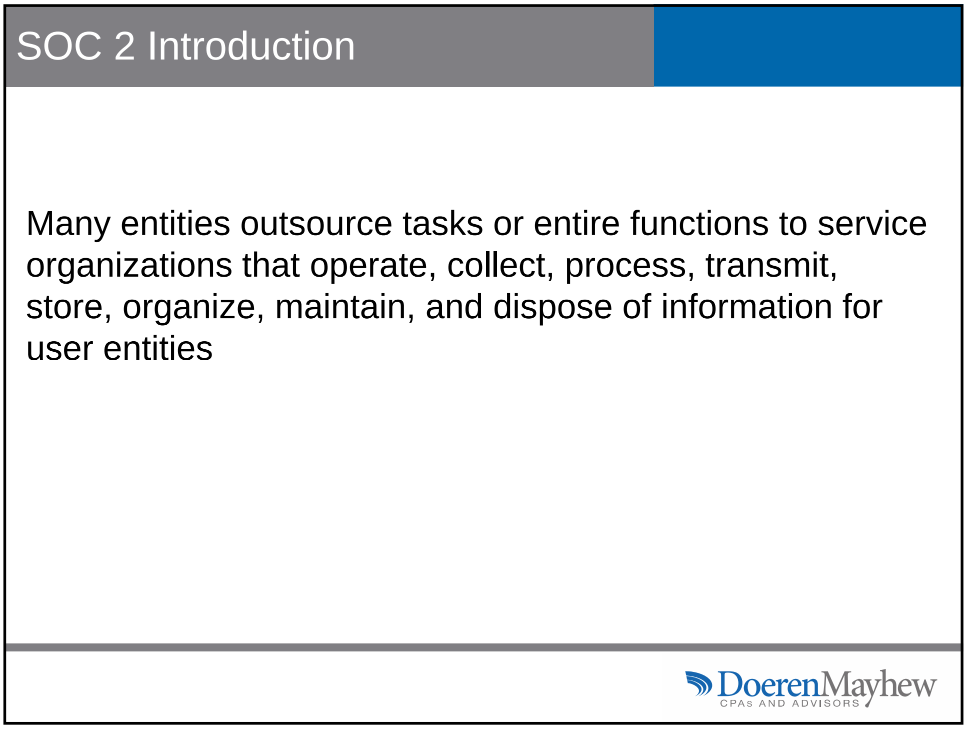
DoerenMayhew CPAs AND ADVISORS



SOC 2

DoerenMayhew CPAs AND ADVISORS

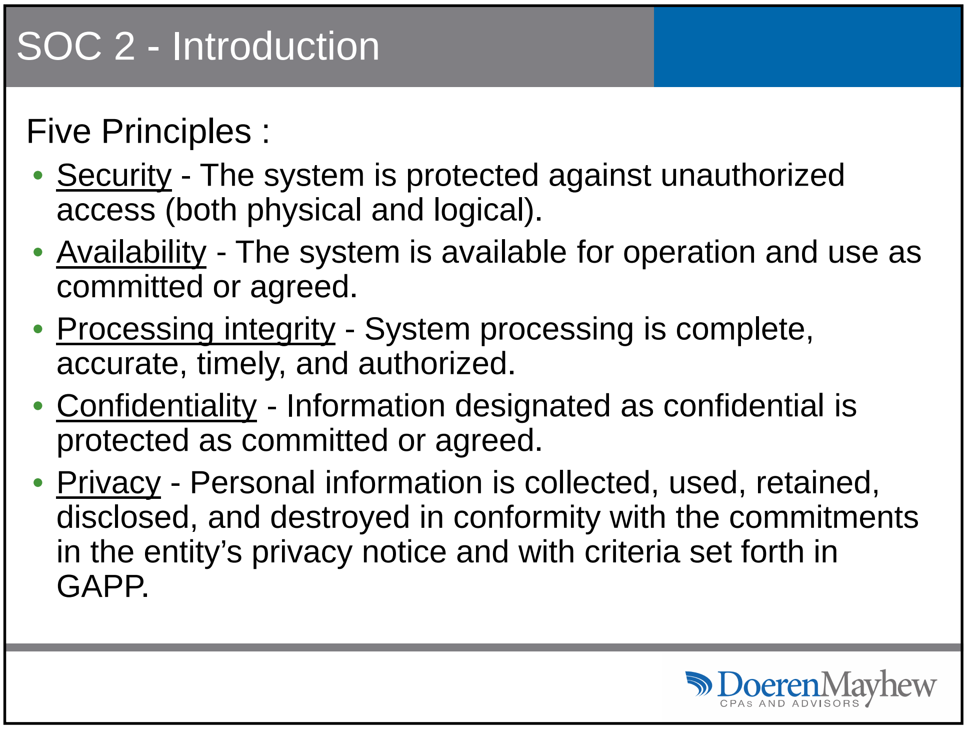
Insight. Oversight. Foresight. SM



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

DoerenMayhew
CPAs AND ADVISORS

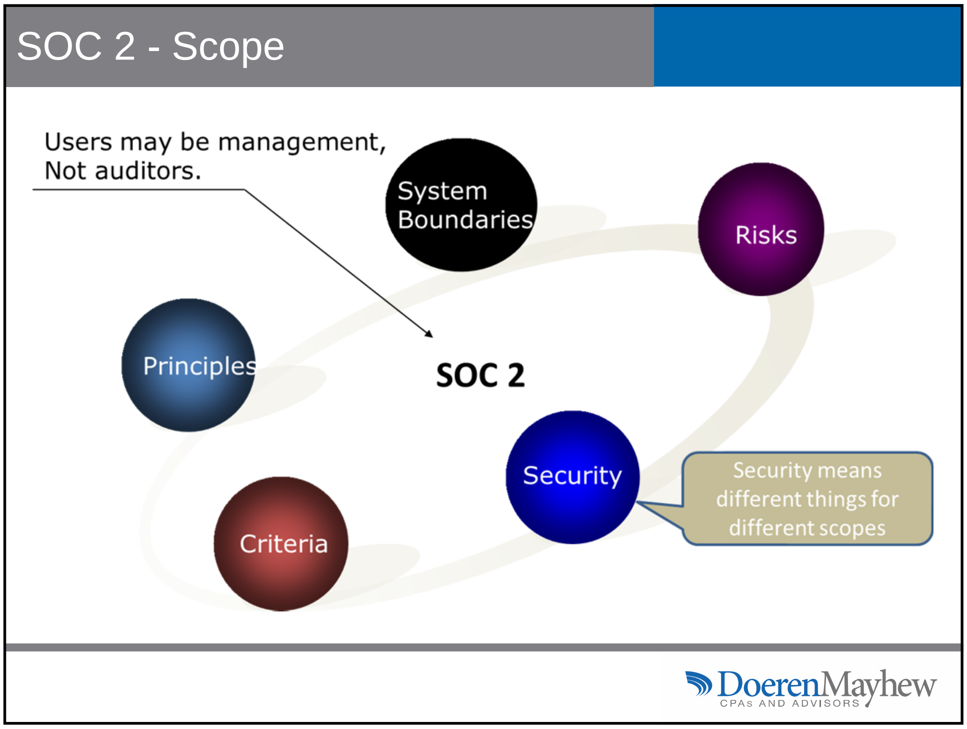


SOC 2 - Introduction

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.

DoerenMayhew
CPAs AND ADVISORS



SOC 2 - Scope

Users may be management, Not auditors.

System Boundaries

Risks

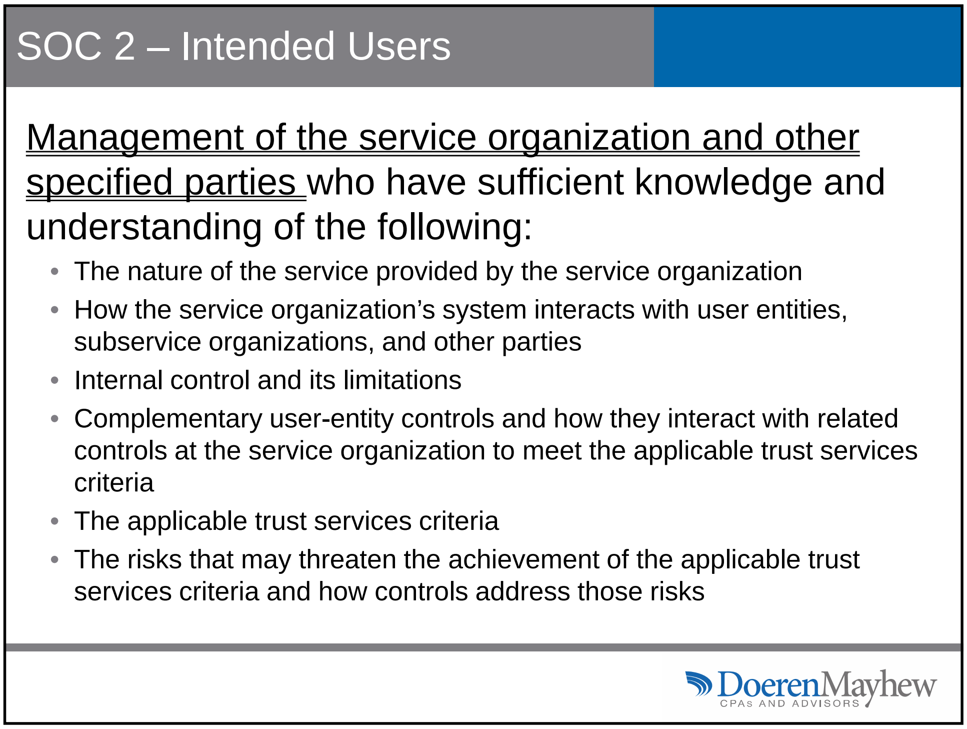
Principles

SOC 2

Security

Security means different things for different scopes

Criteria



SOC 2 – Intended Users

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

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:

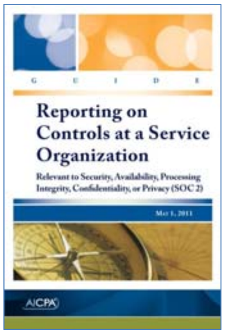
- Determine whether the controls implemented by the service organization address the user organization's risks
- Identify the complementary user entity controls that must be in place to meet the control objectives

DoerenMayhew
CPAs AND ADVISORS

SOC 2 Reports – Types 1 & 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

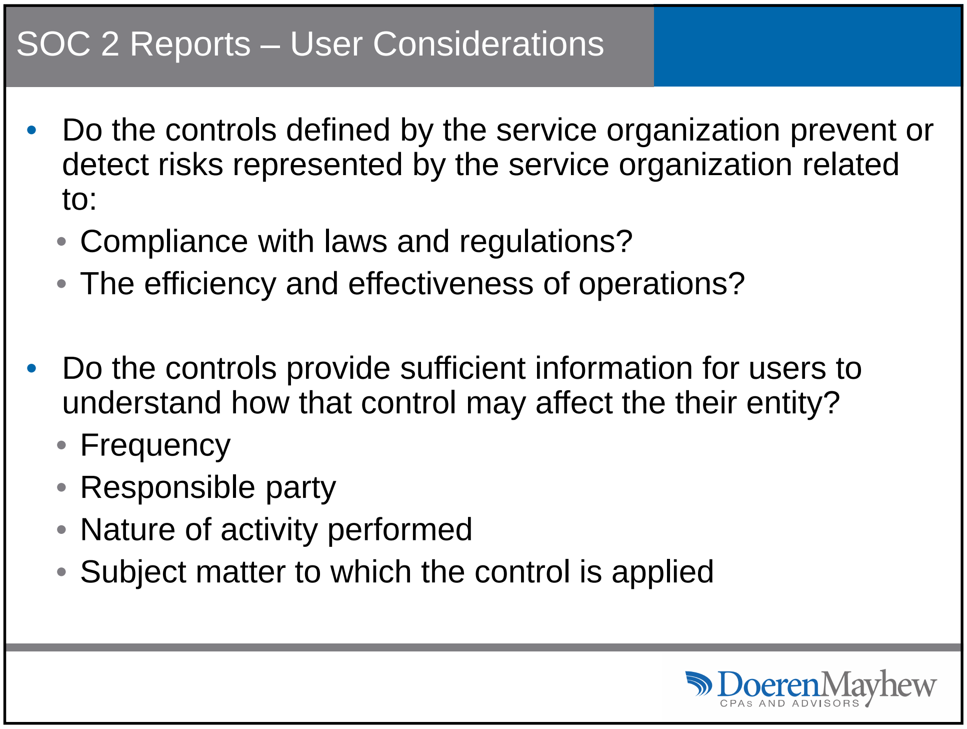
Reporting on Controls at a Service Organization

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

May 1, 2011

AICPA

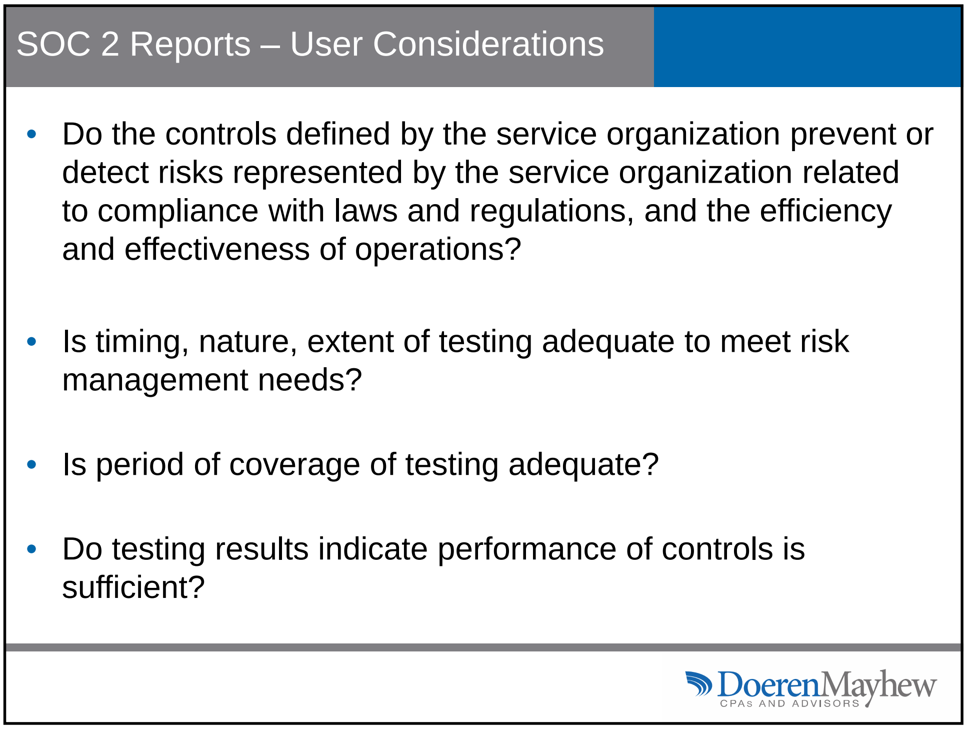
DoerenMayhew
CPAs AND ADVISORS



SOC 2 Reports – User 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

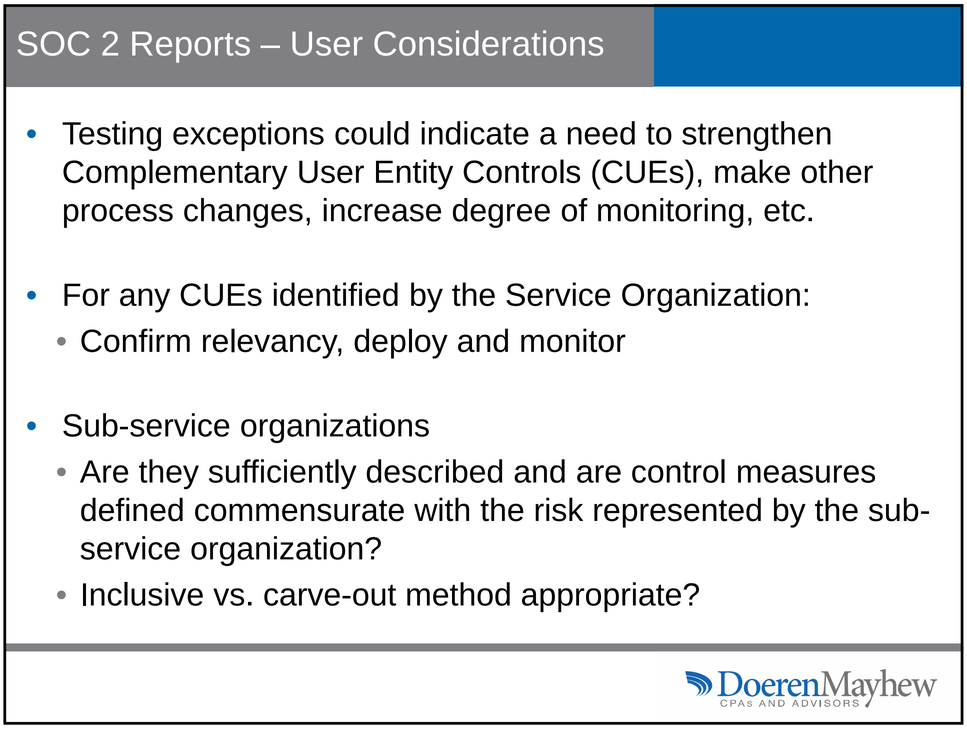
DoerenMayhew CPAs AND ADVISORS



SOC 2 Reports – User 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?

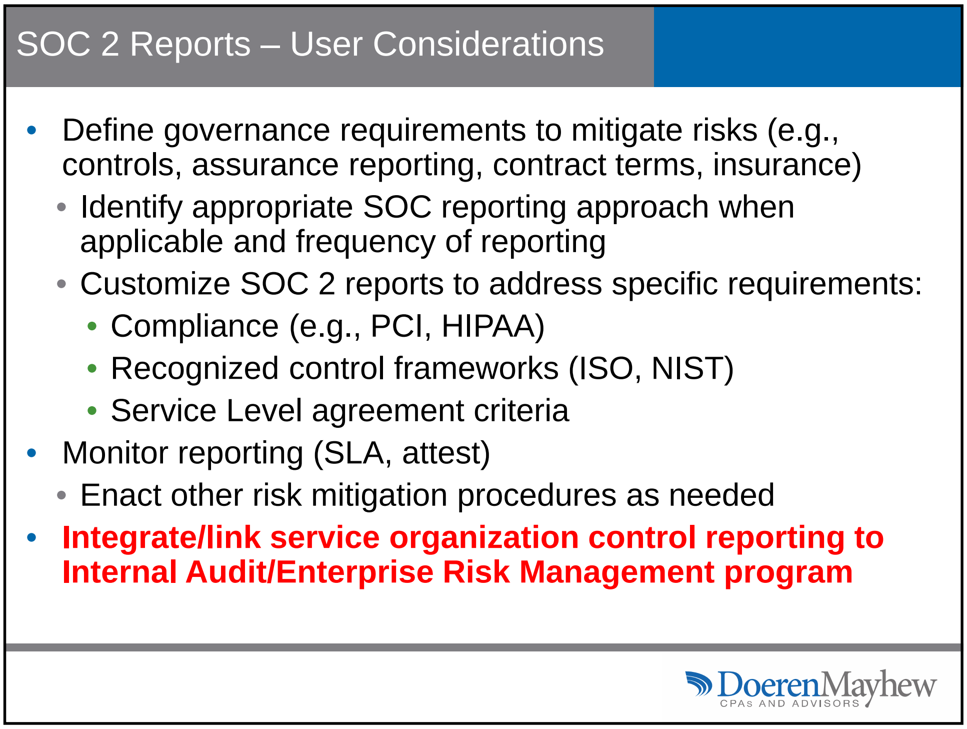
DoerenMayhew CPAs AND ADVISORS



SOC 2 Reports – User 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?

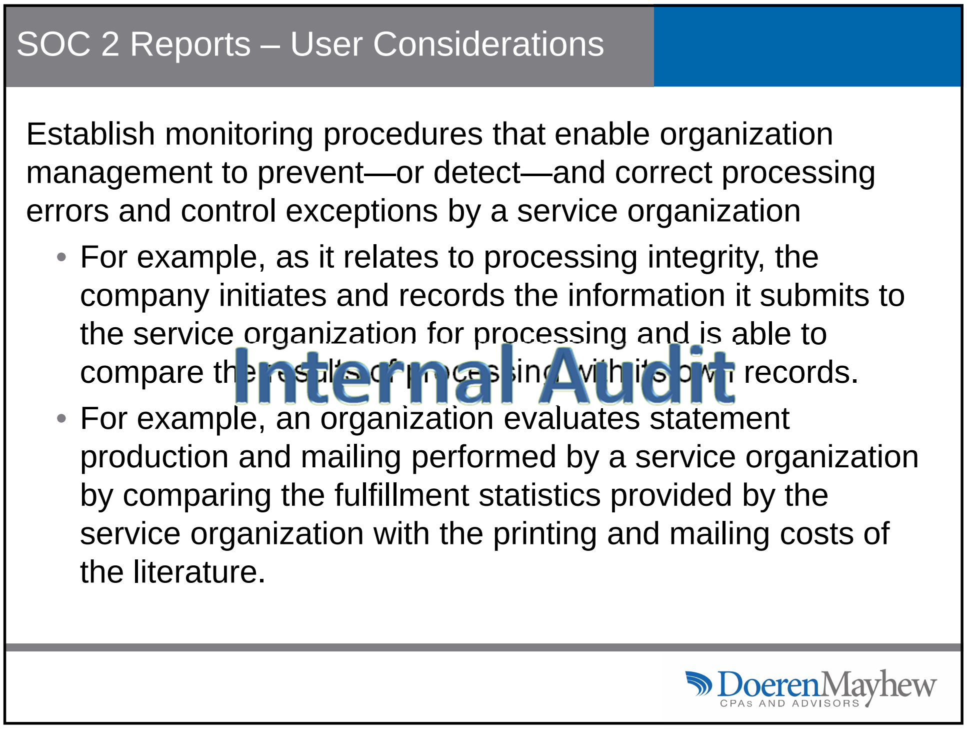
DoerenMayhew CPAs AND ADVISORS



SOC 2 Reports – User 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**

DoerenMayhew CPAs AND ADVISORS

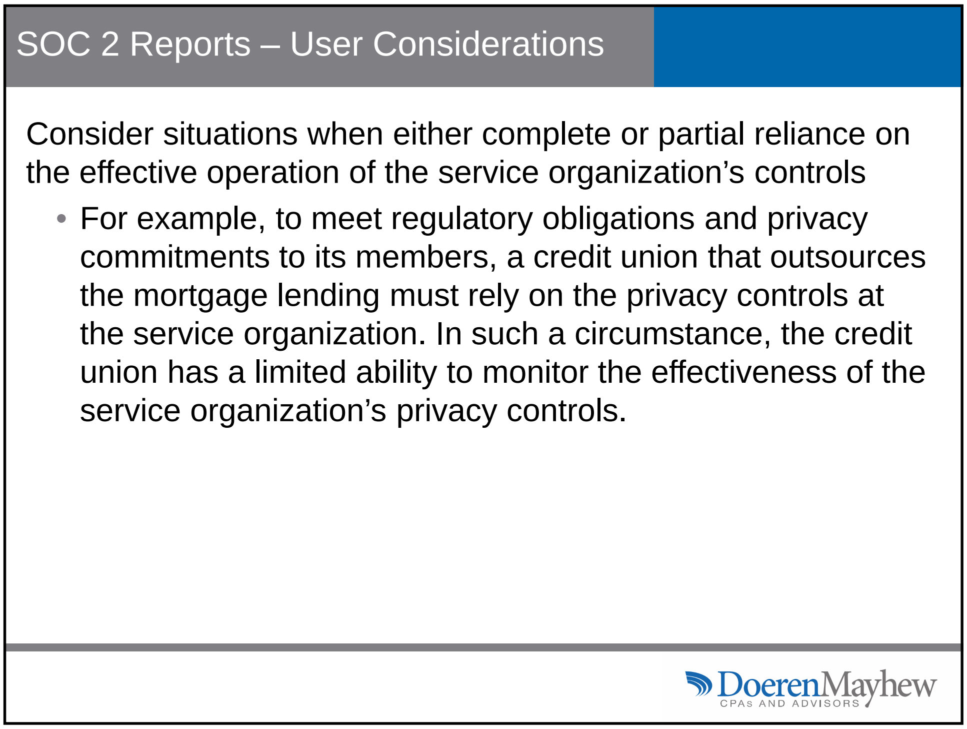


SOC 2 Reports – User Considerations

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.

DoerenMayhew
CPAs AND ADVISORS

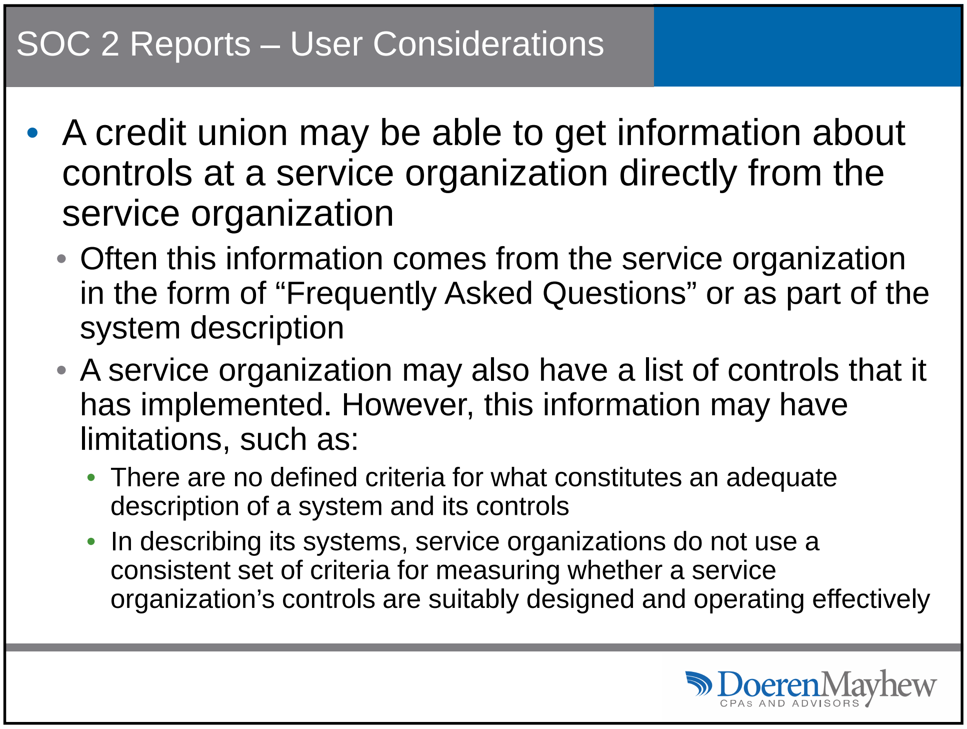


SOC 2 Reports – User Considerations

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.

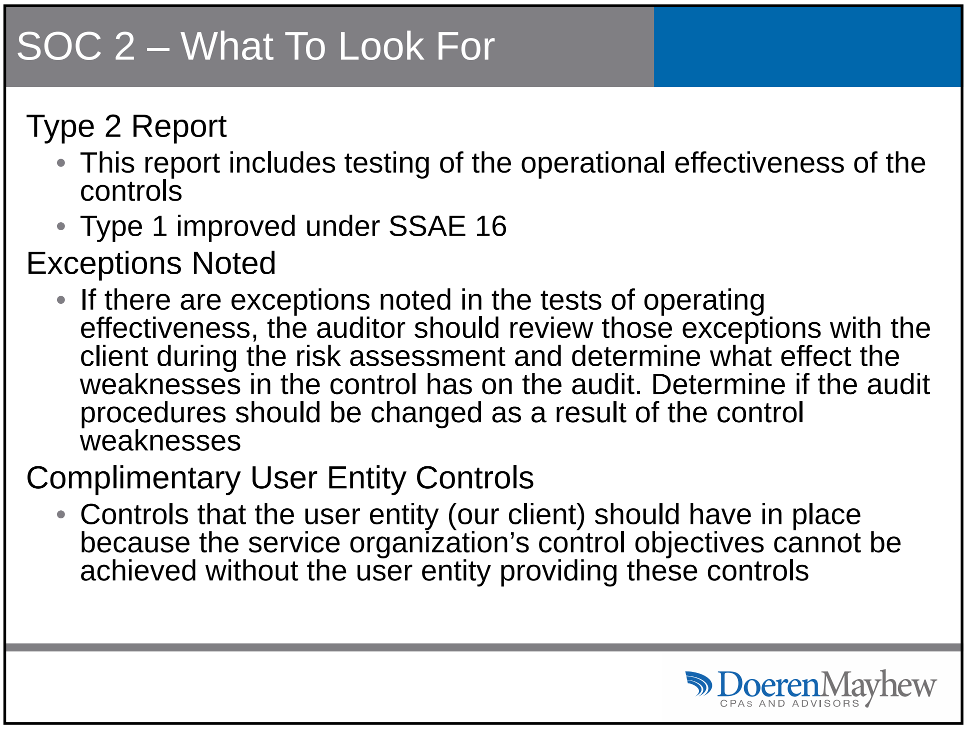
DoerenMayhew
CPAs AND ADVISORS



SOC 2 Reports – User 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

DoerenMayhew
CPAs AND ADVISORS



SOC 2 – What To Look 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

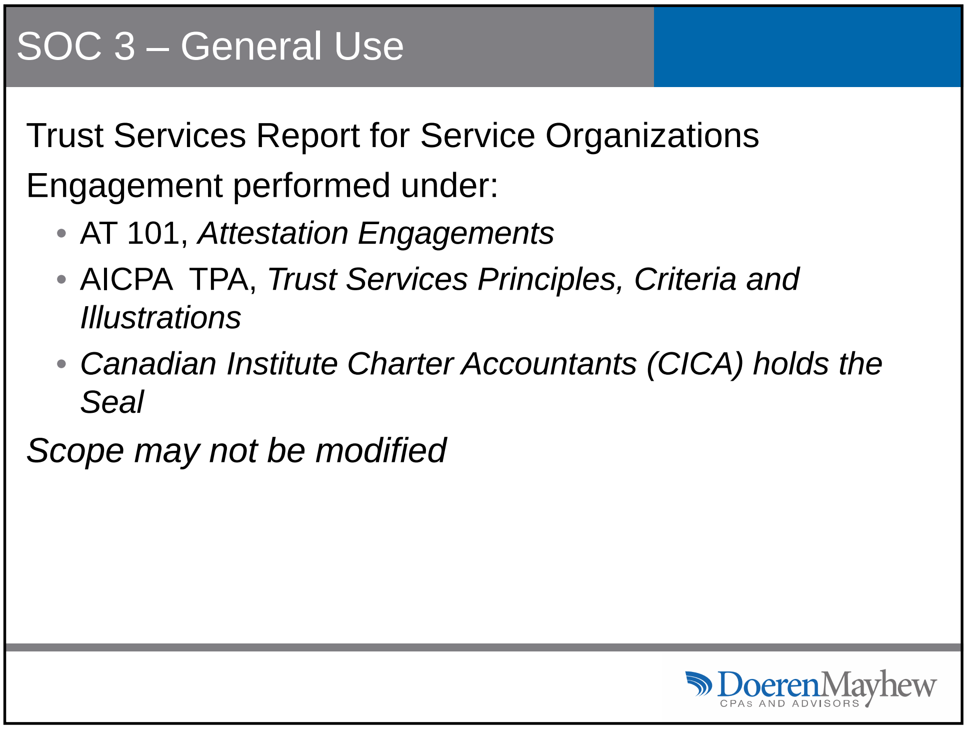
- Controls that the user entity (our client) should have in place because the service organization's control objectives cannot be achieved without the user entity providing these controls

DoerenMayhew
CPAs AND ADVISORS

SOC 3

DoerenMayhew
CPAs AND ADVISORS

Insight. Oversight. Foresight. SM



SOC 3 – General Use

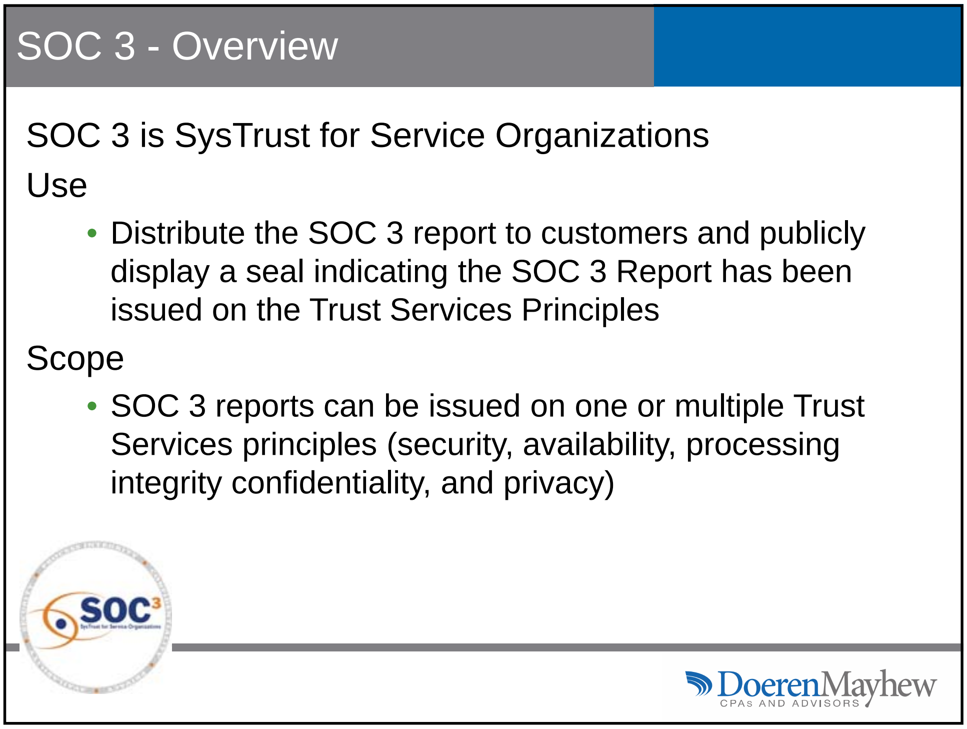
Trust Services Report for Service Organizations

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

DoerenMayhew
CPAs AND ADVISORS



SOC 3 - Overview

SOC 3 is SysTrust for Service Organizations

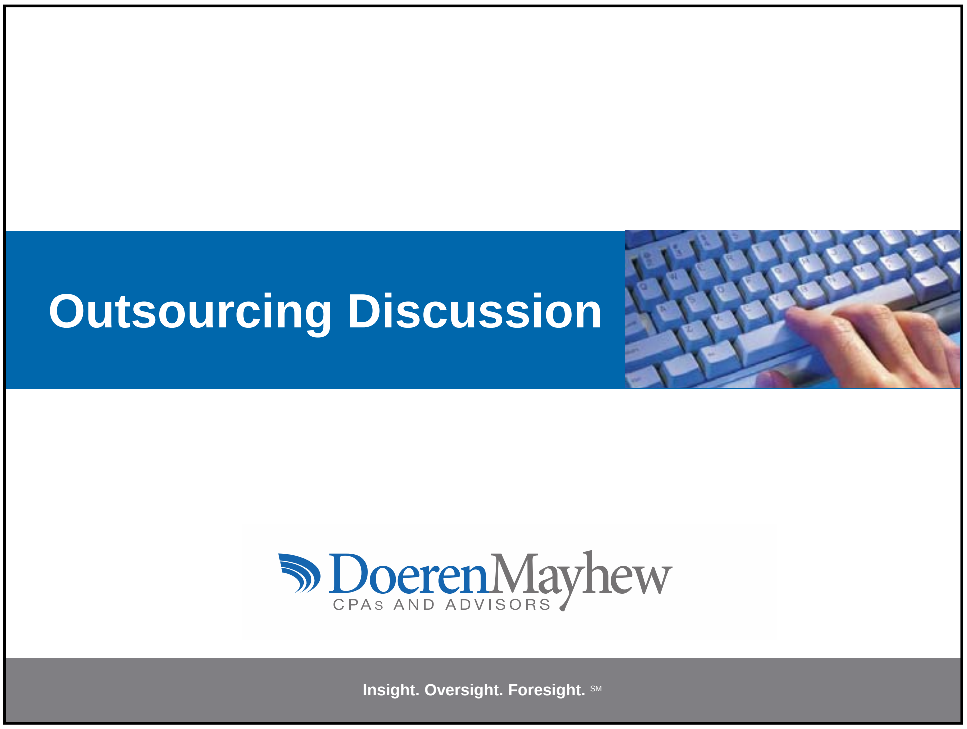
Use

- 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

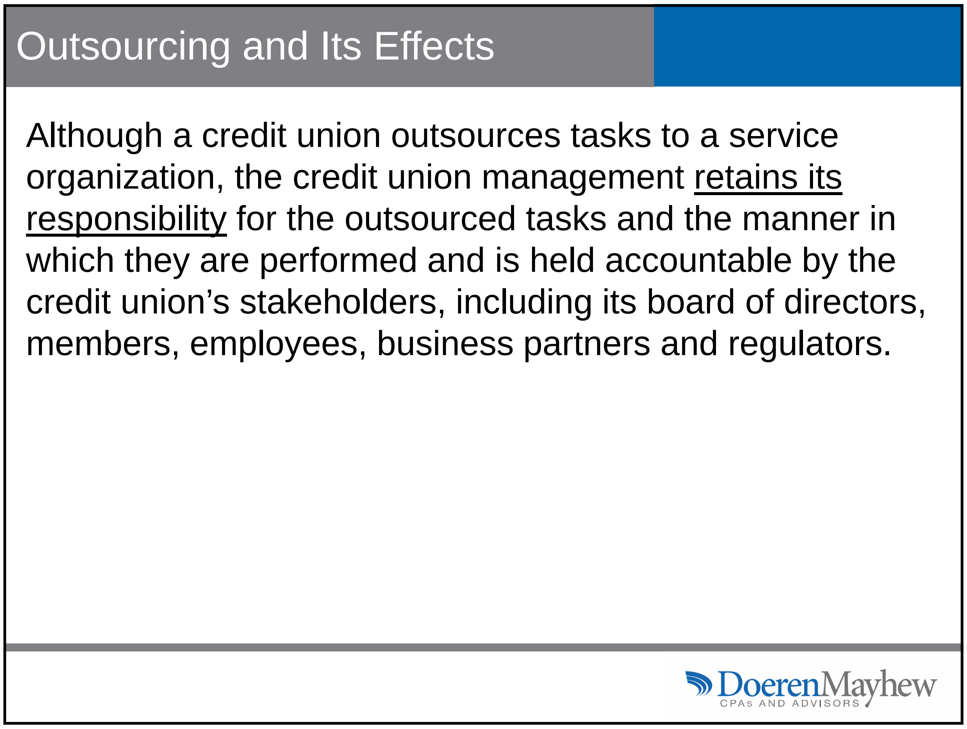
- SOC 3 reports can be issued on one or multiple Trust Services principles (security, availability, processing integrity confidentiality, and privacy)

SOC3
SysTrust for Service Organizations
DoerenMayhew
CPAs AND ADVISORS



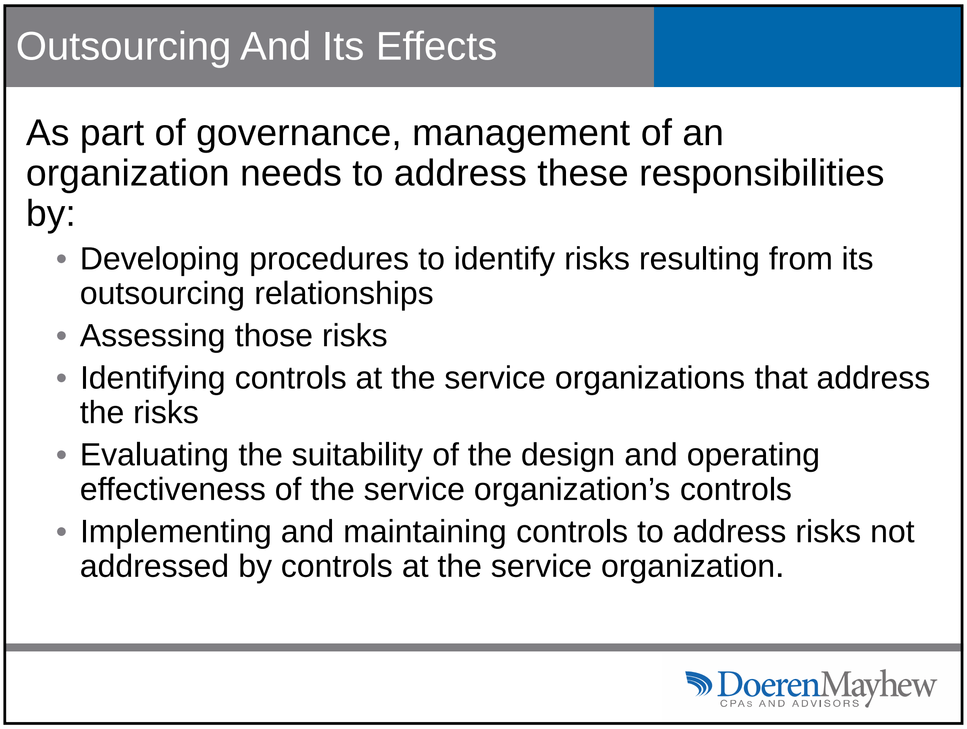
Outsourcing Discussion

DoerenMayhew
CPAs AND ADVISORS
Insight. Oversight. Foresight. SM



Outsourcing and Its Effects

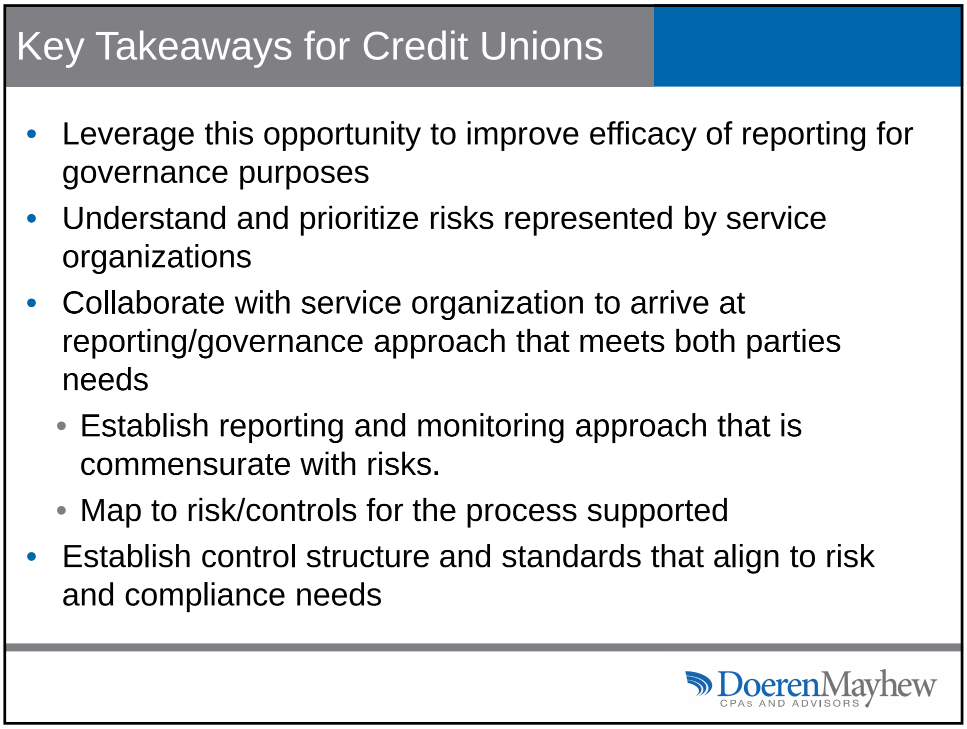
Although a credit union outsources tasks to a service organization, the credit union management retains its responsibility for the outsourced tasks and the manner in which they are performed and is held accountable by the credit union's stakeholders, including its board of directors, members, employees,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



Outsourcing And Its Effects

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

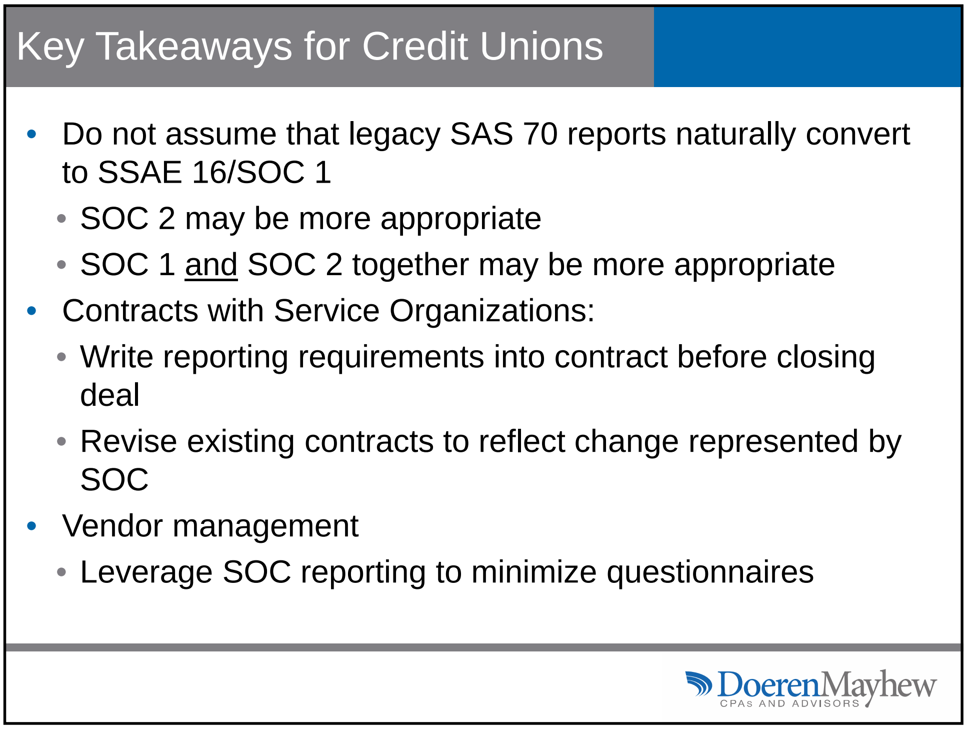
- Developing procedures to identify risks resulting from its outsourcing relationships
- Assessing those risks
- Identifying controls at the service organizations that address the risks
- Evaluating the suitability of the design and operating effectiveness of the service organization's controls
- Implementing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



Key Takeaways for Credit Unions

- 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

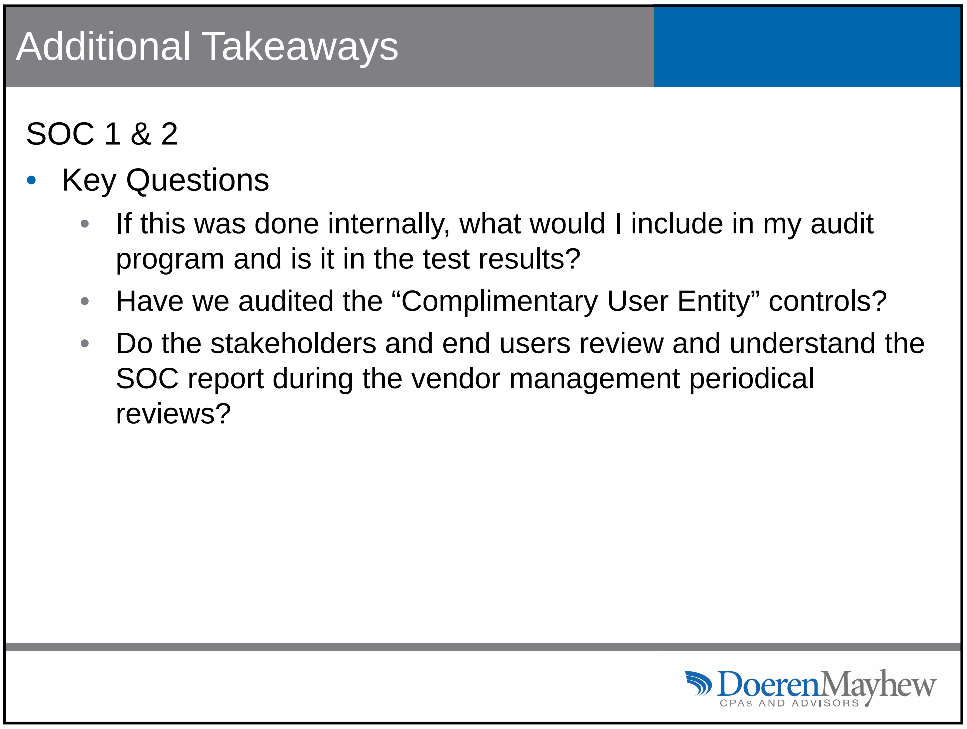
DoerenMayhew
CPAs AND ADVISORS



Key Takeaways for Credit Unions

- 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

DoerenMayhew
CPAs AND ADVISORS

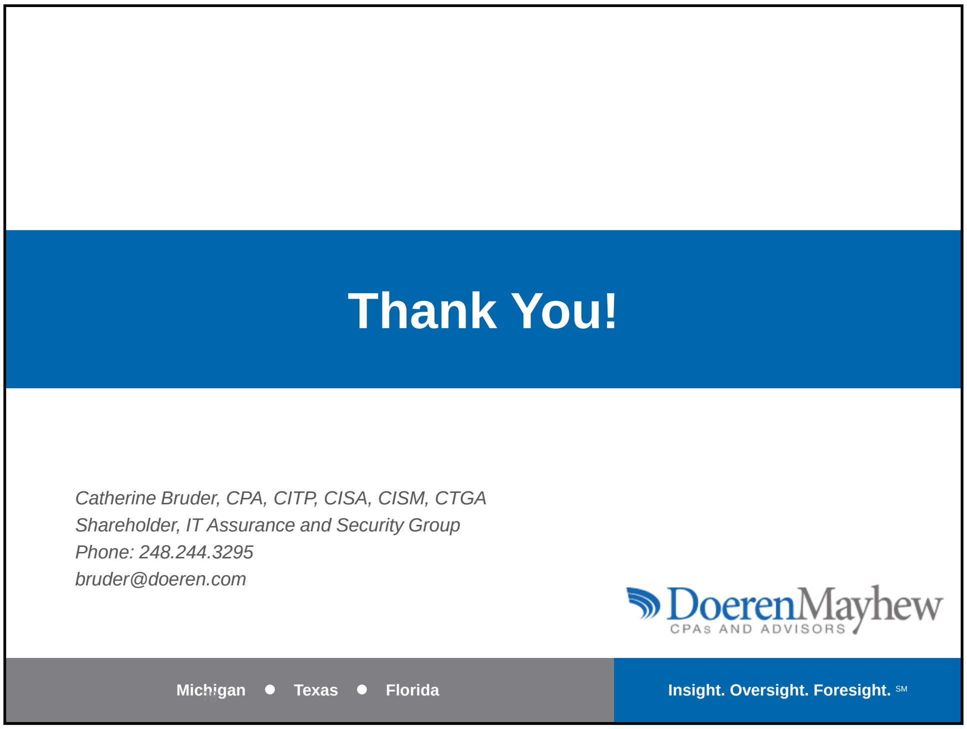


Additional Takeaways

SOC 1 & 2

- Key Questions
  - If this was done internally, what would I include in my audit program and is it in the test results?
  - Have we audited the “Complimentary User Entity” controls?
  - Do the stakeholders and end users review and understand the SOC report during the vendor management periodical reviews?

DoerenMayhew
CPAs AND ADVISORS



Thank You!

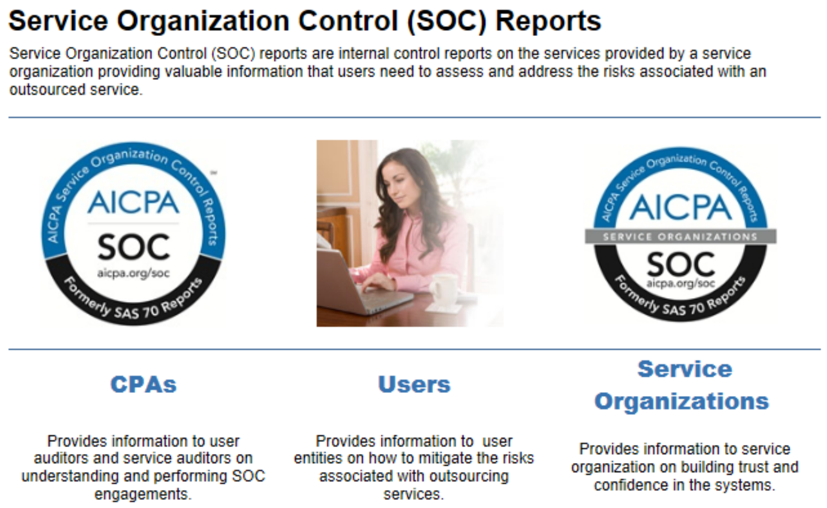
Catherine Bruder, CPA, CITP, CISA, CISM, CTGA
Shareholder, IT Assurance and Security Group
Phone: 248.244.3295
bruder@doeren.com

DoerenMayhew
CPAs AND ADVISORS

Michigan ● Texas ● Florida

Insight. Oversight. Foresight. SM

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.

DoerenMayhew CPAs AND ADVISORS

Additional Resources

- AICPA – IMTA Section Membership
  - Open to non-CPA's
  - Access to tools and whitepapers
  - www.aicpa.org
- ISO Store – ISO 31000 – 2009
- The IIA – IPPF Practice Guide, Assessing the Adequacy of Risk Management Using ISO 31000

DoerenMayhew CPAs AND ADVISORS