Credit Union Service Organization Compliance

How do SOC reporting and PCI requirements affect your overall compliance strategy?

May 15 2012

McGladrey

Assurance ▪ Tax ▪ Consulting

Your Speakers

Dennis Lavin
Credit Union Assurance Partner
Moderator

Kelly Hughes
Technology Risk Advisory Services Director
Speaker

Joe Benfatti
Technology Risk Advisory Services Director
Speaker

McGladrey

PCI Compliance

McGladrey

Assurance ▪ Tax ▪ Consulting

Agenda

- What is PCI?
- Why should I care about this standard?
- Who has interest in our organization's initiatives pertaining to PCI?
- How can I leverage PCI DSS initiatives (i.e. with GLBA; IT General Controls Testing)
- Why is it important to know where cardholder data may be stored?
- What should I consider when starting the PCI initiative?
- Where does the debit card fit in to the process?

McGladrey

What is PCI?

- The Payment Card Industry (PCI) is comprised of:
  - Membership Association/Corporation
    - Visa International
    - MasterCard Worldwide
  - Independent Credit Card Networks
    - Discover Financial Services
    - American Express
    - JCB

McGladrey

PCI Overview

- Payment Card Industry Security Standards Council LLC (PCI SSC – www.pcisecuritystandards.org)
  - Formed in September 2006 to:
    - Allow an open forum for the setting of cardholder security standards
    - Foster broad adoption of cardholder security standards
    - Create a unified, global system that is more accessible and efficient for all stakeholders – merchants, processors, point-of-sale vendors, financial institutions, and payment companies

McGladrey

PCI Overview

- Payment Card Industry Security Standards Council LLC
  - Allow ‘Participating Organizations’ to be members and participate in the standards setting process
  - Responsible for maintaining and enhancing the PCI Data Security Standard
  - Responsible for development of new standards as necessary
  - Responsible for certifying Qualified Security Assessors (QSA) and Approved Scanning Vendors (ASV)

McGladrey

PCI Overview

- The PCI policies, standards and procedures were developed to:
  - Encompass several separate and individual data security efforts
  - Create a common set of data security standards that are critical to the security of the payment infrastructure
  - Ensure a consistent “standard of care” is used to protect payment account, transaction and authentication data

McGladrey

PCI Overview

- The PCI policies, standards and procedures were developed to:
  - Protect the individual card brand trademarks from adverse publicity
    - “x number of Visa/MasterCard/AmEx/Discover/JCB accounts revealed in breach at ABC Corporation”
    - The card brand is usually the first thing in the headline, not the organization that released the information

McGladrey

Why should I care about this standard? It is required…(sort of)

- The PCI SSC has stated:
  - All organizations that store, process, or transmit card holder data must be in compliance with the PCI DSS.
- Typically part of the contract for card services that the organization is PCI compliant
  - Part of the card brands (VISA, MasterCard, etc) operating rules
  - In all new contracts, older contracts may not have requirement
  - Level really only effects the “validation” requirements of the organization

McGladrey

Why should I care about this standard? Card Brand Compromise Penalties

- Organizations proven to be non-compliant or whose merchants or agents are non-compliant will be assessed:
  - Non-compliance fine (egregious violations $500K+)
  - Forensic investigation costs
  - Issuer/acquirer losses
    - Unlimited liability for fraudulent transactions
    - Potential additional issuer compensation (e.g., card replacement)
  - Dispute resolution costs
- Fines are assessed by card brands but passed to merchants and agents via contract terms

McGladrey

Why should I care about this standard? Keep your name out of the paper

- New data breaches are reported daily
  - Stealing credit card numbers has become a business
  - Organized crime groups look for anyway to get numbers for various purposes
  - Loss of customer confidence if breached
- Famous breaches:
  - TJMMAX, Heartland, Hannaford, etc.

McGladrey

Why should I care about this standard? Safe Harbor status

- "Safe Harbor" status provides organizations protection from fines and compliance exposure in the event its merchant or service provider(s) experiences a data compromise
- To attain "Safe Harbor" status:
  - Members MUST be in FULL COMPLIANCE with the PCI DSS at the time of the breach (as demonstrated during a forensic examination)
  - Members MUST have validated FULL COMPLIANCE PRIOR TO the compromise

McGladrey

Why should I care about this standard? Safe Harbor status

- Submission of a Report on Compliance (ROC) alone does NOT provide a member “Safe Harbor” status
  - Compromised members MUST have adhered to ALL of the requirements at the time of the breach

McGladrey

Who has an interest in your organization's PCI initiatives?

- Organizations who have access to cardholder data (credit card numbers, expiration dates, names)
- Organizations that process cards on behalf of others
- Organizations who outsource cardholder related processes, but still have access to the cardholder information
- Organizations who co-brand debit cards with one of the card brands.

McGladrey

How can I leverage PCI DSS initiatives? (with GLBA, FFIEC IT controls reviews)

- Map out the control requirements for the various compliance type of initiatives (PCI, GLBA, IT GCC testing).
  - DSS Requirement 12 (12.1.2) can map to GLBA's IT risk assessment requirement
    - Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment.
- Analyze where overlap may exist (there are many).
- Determine how to best leverage the controls so data is gathered once, but used across requirements, when possible.

McGladrey

Why is it important to know where cardholder data may be stored?

- It becomes the scope
- Remember, the assessment scope applies only to the **card holder data environment (CDE)**
  - Card holder environment: systems that **store, process or transmit** cardholder data
- No segmentation? Then you *must* include *everything* in scope.
  - This is where most organizations start
  - This approach rarely (never?) leads to a clean ROC

McGladrey

Why is it important to know where cardholder data may be stored?

- Generally speaking, most organizations don't do well the first time through
  - Costs money
  - Wastes time
- It's an opportunity for improvement:
  - By learning from the mistakes of others, you can be better prepared
- Most often, the issues are one of a few preventable issues that could help make compliance an easier process

McGladrey

Why is it important to know where cardholder data may be stored?

- Difficulty in compliance is normally in one or more of these areas:
  - Inappropriate scope
  - Insufficient documentation
  - Unnecessary (or inappropriate) data storage
  - Application issues (particularly legacy applications)
  - Compensating controls (that don’t compensate)
  - Bad timing

McGladrey

Cardholder data at credit unions

- Debit card processing - is your core application provider PA-DSS approved?
- POS terminals at branches, i.e. cash advances
- Paper records at branches and locations, i.e. loan applications, credit reports, etc.
- New card set up (debit card/ATM) involves card holder data
- Inactivated card stock
- Any information exported to end user apps

McGladrey

Summary – Top Things to Prepare for PCI

- Identify the repositories and data flow of card holder data in your organization
- Implement segmentation where feasible
- Determine if vendors that access card holder data are addressing PCI compliance
- Application providers are PA-DSS certified
- Physical security of paper records containing cardholder data
- Control of exports, extracts or transfers of data to less secure environments

McGladrey

Service Organization Control (SOC) Reporting

McGladrey

Assurance ▪ Tax ▪ Consulting

Agenda

- SAS 70 History and Need for Change
- Internal Control Reporting Options
- New Guidance
- New Terminology
- What Does this Mean for Service Organizations?
- What Does this Mean for User Entities?

McGladrey

History and Need for Change

- SAS 70 issued in 1992
  - Overview
  - Purpose
- Effects on SAS 70's caused by SOX:
  - "Stakeholders grew, and grew, and grew…"
    - Procurement agents requiring SAS 70 in RFPs
    - Salespeople promising SAS 70s to customers
- 2011- service organizations and user organizations often request them for non-financial controls

McGladrey

History and Need for Change

- Need for realignment of guidance with market uses and perceptions
  - "…no, we can't do SAS 70 to assess how 'green' your company is…"
  - Additional reporting options
- Convergence with international standards
- Emerging needs, complexities and types of service organizations

McGladrey

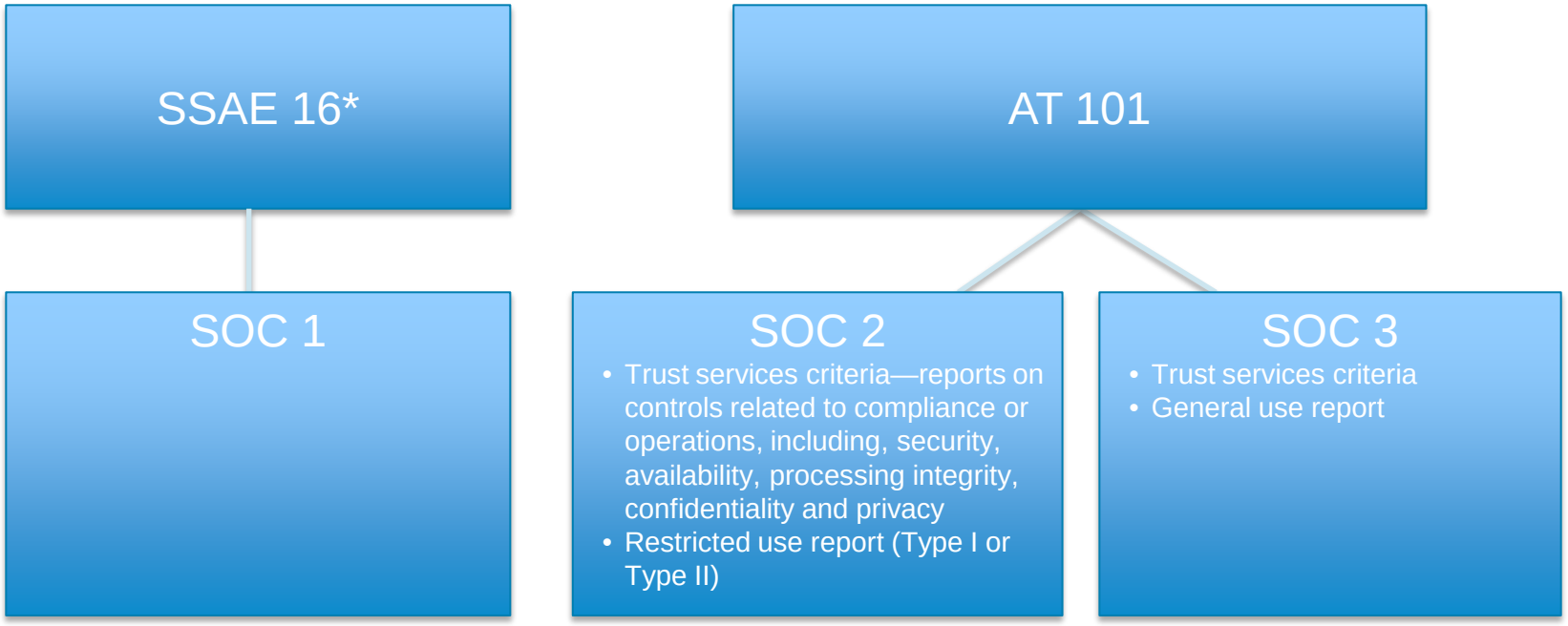
Internal Control Reporting Options

	SSAE16 (SOC 1)	SOC 2	SOC 3	Other Reports
GUIDANCE	AICPA Attest Standards (SSAE 16)	AICPA Attest Standards (AT101) Trust Services Principles	AICPA Attest Standards (AT101) Trust Services Principles	AICPA Attest Standards (AT101)
EXAMPLE PROJECTS	• Auditor to auditor opinion report for financial reporting controls • Audit entity meets definition of service organization • CPA firm responsible for the adequacy of the procedures	• Opinion report on system security, availability, processing integrity and confidentiality/or privacy • Detailed like SOC1 • CPA firm responsible for the adequacy of the procedures	• Opinion report on system security, availability, processing integrity and confidentiality/or privacy • Client description is not audited • CPA firm responsible for the adequacy of the procedures	• Doesn't fall under SSAE 16 or Trust Services Principles • Reporting on the design of internal controls • CPA firm responsible for the adequacy of the procedures
REPORT DISTRIBUTION	• Report distribution to service organization users • Issued by licensed CPA	• Intended for non-auditor audience (e.g., CIO) • Issued by licensed CPA	• Intended for non-auditor audience (e.g., CIO) • General use report • Issued by licensed CPA	• May be issued for general or restricted use • Issued by licensed CPA

McGladrey

Service Organization Controls Reports

The hierarchy of available reporting standards is depicted below:

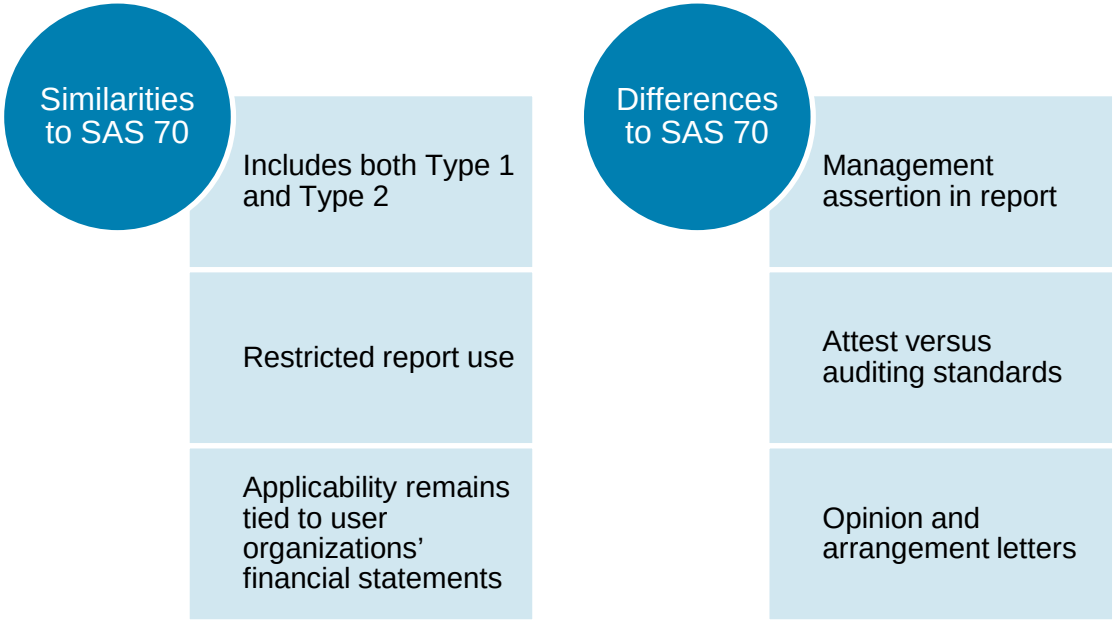


**ISAE3402 is the corresponding international standard*

McGladrey

SSAE 16

- Governed by Statement on Standards for Attestation Engagements No. 16 (SSAE 16)
- New terminology - Service Organization Control Report 1
- Effective for periods ending on or after June 15, 2011



McGladrey

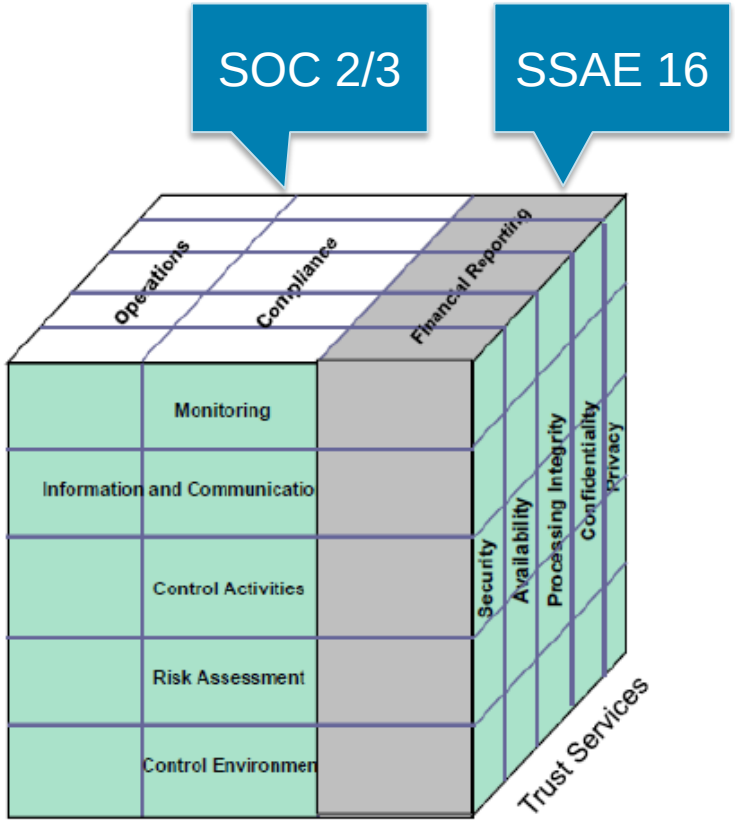
User Considerations for SOC Reports

- How are the reports used by financial statement auditors?
- What is of interest to financial statement auditors?
- What is required by financial statement auditors?
- Can a SOC 2 or SOC 3 report be used by a user financial auditor to satisfy any of its audit requirements?
- Other considerations?

McGladrey

SOC 2 and SOC 3 Overview

- Cloud Computing / SaaS / PaaS / IaaS outsourcing
- Subject Matter
  - Operational
  - Compliance
  - Non-Financial
- Better “fit”



McGladrey

Trust Principles and Criteria

- AICPA framework which included high level principles and related detailed criteria
- Principles include
  - Security
  - Availability
  - Processing Integrity
  - Confidentiality
  - Privacy
- Criteria include detailed control standards that need to be achieved

McGladrey

What does this mean to service organizations?

Engagement activity	What clients will notice
Arrangement Letter	• Updated wording for the letter to align with the new guidance
Planning	• Enhanced validation of the control objectives included in the report • Discuss the need for subservice organizations to sign a management representation letter (for inclusive method reporting)
Fieldwork	• No significant changes
Management Representation Letters	• Addition of management's assertion relating to the design and effectiveness of relevant internal controls will be included in the representation letter • Obtain a management representation letter from subservicers included in opinion
Reporting	• The new report format will include management's assertion and the opinion's language will be changed to align with the new standard

McGladrey

What does this mean to credit union user entities?

Engagement activity	What user entities will notice
Report Sections I and II	• Updated wording for the opinion and formal management assertion appears in the report to align with the new guidance • Subservice organization requirements
Report Section III	• Enhanced validation of the control objectives included in the report
Nature, Timing & Extent of Testing	• No significant changes
Report Use for CU User Entities	• SOC 1 (support of financial statement audit) • SOC 2/3 (support of resident objectives)
User Control Considerations	• Internal/external requirements

McGladrey

McGladrey LLP

800.274.3978
www.mcgladrey.com

McGladrey

Assurance ▪ Tax ▪ Consulting