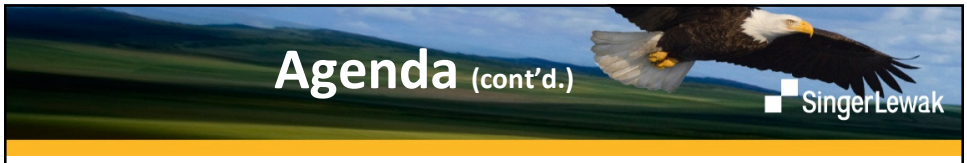
SAS 70 & SSAE 16: Changes & Impact on Credit Unions

John Mason
CISM, CISA, CGEIT, CFE
SingerLewak LLP

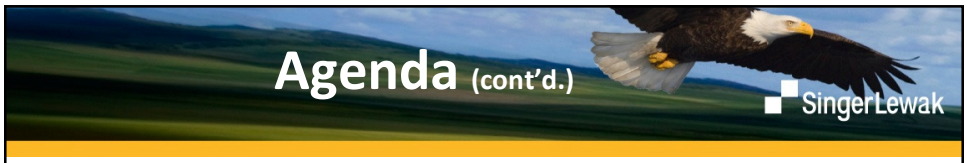
October 19, 2010

Agenda

- Statement on Auditing Standards (SAS) 70 background
  - Background & purpose
  - Types
  - Typical use
- Statement on Standards for Attestation Engagements (SSAE 16) background
  - Definition
  - Intent
- Overview of SSAE 16



- So what has changed?
- Advantages of SAS 70 & SSAE 16
- SAS 70 & SSAE 16 value proposition
- Practitioner considerations
- Decision tree
- So how does this affect my organization?
  - CUSO
  - Management assertion
  - Third-party vendors
  - Use of Internal audit



- Pending issues
- Conclusion & wrap-up

- A bit of history…
  - Statement on Auditing Standards 70
  - First in April 1992 by the AICPA
  - Is used domestically and internationally as a vehicle of auditor-to-auditor communication
  - Focused on unique systems for processing

- A bit of history…
  - Its use is frequently found in third-party outsourcing
    - ✓ Benefits administration (e.g. 401K)
    - ✓ Payroll processing
    - ✓ Insurance/medical claims processing
    - ✓ Hosted data centers
    - ✓ Application service providers (ASPs)
    - ✓ Managed security providers
    - ✓ Security monitoring
    - ✓ Credit scoring/processing organizations

SAS 70 Background (cont'd.)

SingerLewak

- Types of SAS 70s
  - ➢ Type I
    - ✓ Provides an independent auditor's opinion on the
      - – fairness of the presentation of the service organization's description of controls that had been placed in operation
      - – suitability of the design of the controls to achieve the specified control objectives
    - ✓ Is as of a specific point in time (rather than a coverage period)
    - ✓ Sample of 1 to test the design effectiveness
    - ✓ Typical users include marketing organizations and service providers who are preparing initially for a Type II SAS 70

SAS 70 Background (cont'd.)

SingerLewak

- ➢ Type II
  - ✓ Provides an independent auditor's opinion on the
    - – the information provided in a Type I
    - – whether the specific controls were operating effectively during the period under review.
  - ✓ Is for a period of time (minimum 6 months)
  - ✓ Representative samples are drawn from across the SAS 70 period

SAS 70 Background (cont'd.)

SingerLewak

- Type II (cont'd.)
  - ✓ Credit unions: typical organizations that have a Type II SAS 70 performed
    - – Benefits administration
      - » 401K investments performed by third party
      - » Trust administration
    - – Securities custodian investments (e.g. CUSO or benefits)
    - – Payroll (ADP, PayChex, etc.)
    - – IT outsourcing: data processing, item processing
    - – Credit card processing
    - – Loan processing
      - » How many outsource for their loan scoring, credit reports, and/or as a decision tool?
      - » We recently completed the SAS 70 for MeridianLink

SAS 70 Background (cont'd.)

SingerLewak

- Type II (cont'd.)
  - ✓ Key benefits derived from using the SAS 70s
    - – Improved audit coverage since an independent body has evaluated the selected controls at the outsourcer
      - » Less travel
      - » Independent body may have more specialization skills (e.g. trust administration)
    - – Typical reduced audit scope in key areas
      - » Benefits administration
      - » Outsourced IT processing
      - » Payroll
    - – Improved confidence in the services and controls provided by the outsourced organization

SSAE 16 Background

- Definition
  - Statement on Standards for Attestation Engagements (SSAE 16)
    - ✓ Has an international version as well, International Standards for Attestation Engagements (ISAE 16)
- Rather than an auditor-to-auditor communication, the intent now is to focus more on the attestation and the structure surrounding the attestation

Overview of SSAE 16

- Scope
  - Focused on unique systems for processing
  - Type 1 and Type 2 reports
  - Use of subservice organizations (carve-out and inclusive methods)
  - Restricted use report
- Effective Date
  - Service auditor's reports for periods ending on or after June 15, 2011
  - Early adoption is permitted

Overview of SSAE 16 (cont'd.)

SingerLewak

- Notable Changes
  - Attestation standard vs. auditing standard
  - Management assertion
  - Use of suitable criteria
  - Suitability of design opinion (point in time vs. entire period)
  - Materiality
  - Use of internal audit
  - Opinion format

So What Has Changed?

SingerLewak

- SAS 70 reports will now be renamed to Service Organization Control (SOC) reports
- SSAE 16 is NOT intended to provide assurance on controls as they relate to internal controls over financial reporting (ICFR)
  - New standard on the horizon that will provide assurance on controls regarding ICFR
- Audit standard is now referred to as the attestation standard

So What Has Changed? (cont'd.)

SingerLewak

- The carve-out method (i.e. specific exclusion) likely will be the most prevalent
  - Subservicing organizations (e.g. payroll, outsourced IT processing, premises monitoring, etc.) may not wish to provide an attestation of their service as they may not be prepared for the expense or the effort

So What Has Changed? (cont'd.)

SingerLewak

- Management assertion is required
  - Is similar to that used for SOX Section 302: the CEO and CFO must attest to the effectiveness of the controls
    - ✓ The description of the organization's controls is presented fairly
    - ✓ An explanation of how the controls' design is suitable
    - ✓ Confirmation that the controls were designed and implemented as of the assertion date
    - ✓ Providing information about the controls operating effectiveness (Type II only)

Advantages

SingerLewak

- Advantages of a SAS 70 or SSAE 16
  - ➢ Allows the provider's customers to place reliance on the provider's controls.
  - ➢ The provider determines the scope, control objectives, controls to be tested, and the review period.
  - ➢ Can reduce the scope of internal audits, external audits, regulatory examinations, and required compliance testing
    - ✓ Reducing the scope ➔ saving $, time
    - ✓ Major mortgage servicer essentially recouped its cost

Value Proposition

SingerLewak

INTERNAL VALUE	EXTERNAL VALUE
VALIDITY	THE CONTROLS EXIST & THEIR DESIGN IS EFFECTIVE; FOR A TYPE II ENGAGEMENT, THEY ARE OPERATIONALLY EFFECTIVE
EFFICIENCY	RESOURCES ARE DESIGNED AND DEPLOYED AS PLANNED
MEASURABILITY	QUANTIFIABLE, VERIFIABLE RESULTS
ACCOUNTABILITY	CONTROL OBJECTIVES' CONTROLS ARE FULLY TRANSPARENT TO THE CLIENTS
EFFECTIVENESS	ALL CONTROLS AND PROCEDURES ARE IN PLACE TO ENSURE THE BEST OUTCOME
COMPETITIVE ADVANTAGE	MEMBERS KNOW THAT A CU/CUSO WITH A SAS 70 EXAMINATION HAS STRONGER INTERNAL CONTROLS
COMMITMENT TO EXCELLENCE	CLIENTS UNDERSTAND THAT WITH A SAS 70 AUDIT, YOU ARE COMMITTED TO EXCELLENCE FROM THE TOP DOWN

Practitioner Considerations

- Management's Assertion
  - Written assertion required
    - ✓ Description of system (using criteria similar to SSAE 16)
      - – Control objectives (specified in Guide)
      - – Controls
    - ✓ Risk assessment
    - ✓ Management's basis for asserting controls were consistently applied
  - Service auditor's responsibilities
- Suitability of Criteria
  - Management's use of suitable criteria
  - Controls applied as designed

Practitioner Considerations (cont'd)

- Risk Assessment
  - Formal vs. informal assessment
    - ✓ If the practitioner has performed the audit previously, it must perform a new risk assessment each time it performs the audit
    - ✓ This is intended to
      - – ensure that the auditor takes a fresh look at the service organization's environment and
      - – provide a more current perspective on the service organization's control structure

Practitioner Considerations (cont'd.)

SingerLewak

- Risk Assessment
  - Control objectives
    - ✓ Relevancy to the key areas to be examined and tested
    - ✓ Effects of new legislation or other environmental and economic conditions
    - ✓ Organizational strategic objectives and tactical initiatives
  - Monitoring controls
    - ✓ Changes in key activities
    - ✓ New systems or applications
    - ✓ Changes in economic conditions, both macro and micro

Practitioner Considerations (cont'd.)

SingerLewak

- Criteria
  - Description of the system
    - ✓ Types of services and classes of transactions
    - ✓ Procedures (automated and manual)
    - ✓ Related accounting records
    - ✓ Significant events and conditions
    - ✓ Specified control objectives and controls and as applicable, complementary user entity controls
    - ✓ Other relevant COSO components (e.g., control environment, risk assessment, info and communication, control activities, monitoring)

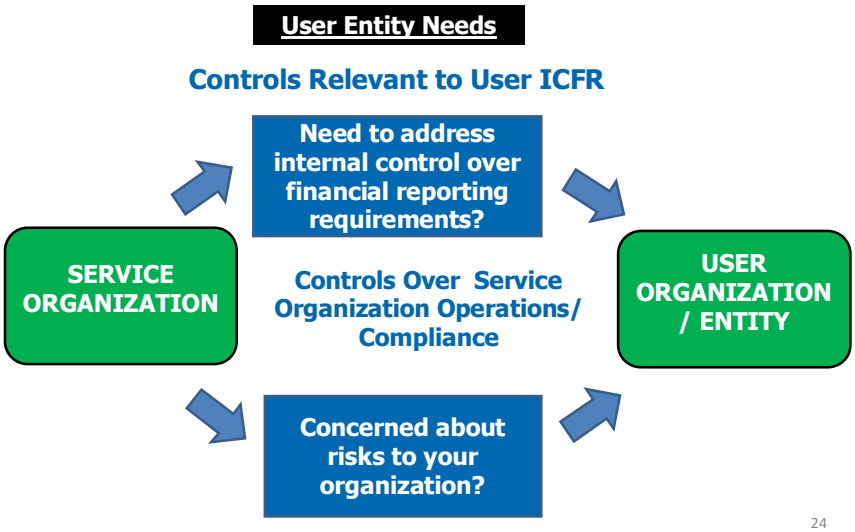
Practitioner Considerations (cont'd.)

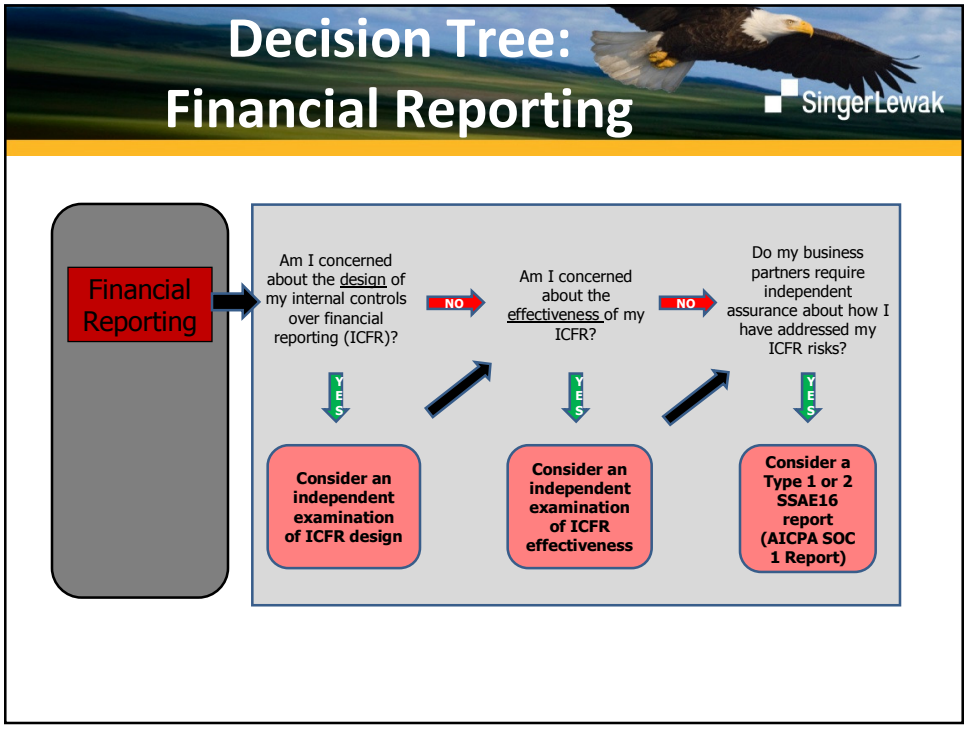
SingerLewak

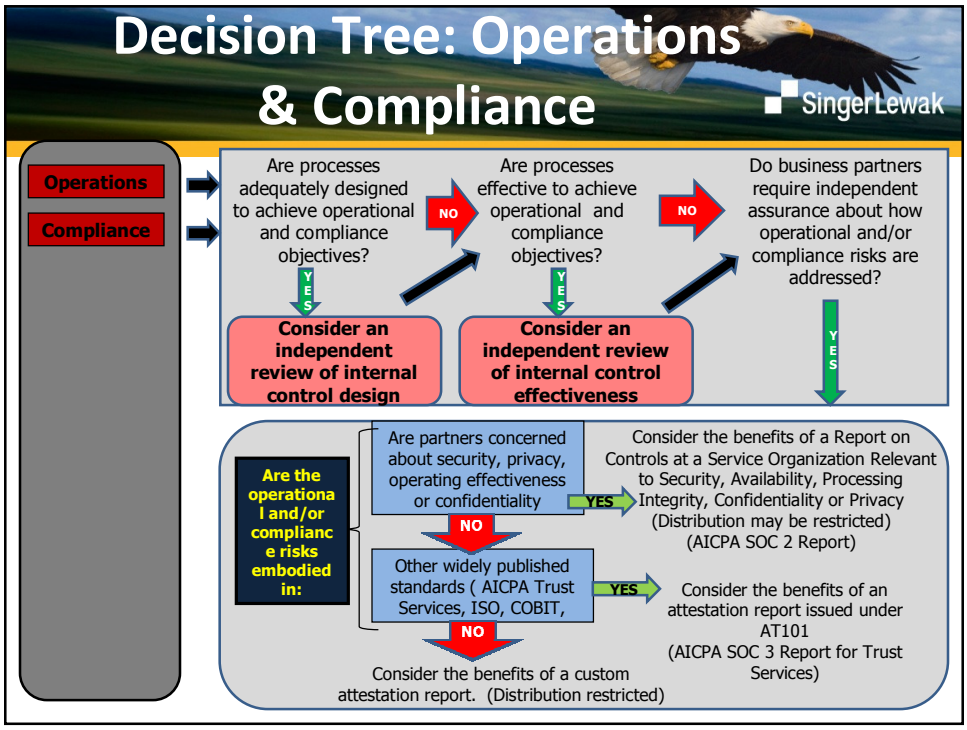
- Criteria
  - Changes to the service organization system during the period (in the case of Type 2 report)
  - Management's description does not omit or distort information while meeting common needs of a broad range of user entity/user auditor needs

SAS 70 / SSAE 16 Decision Tree

SingerLewak




Decision Tree:
Financial Reporting
SingerLewak
Financial Reporting
Am I concerned about the design of my internal controls over financial reporting (ICFR)?
NO
Am I concerned about the effectiveness of my ICFR?
NO
Do my business partners require independent assurance about how I have addressed my ICFR risks?
YES
YES
YES
Consider an independent examination of ICFR design
Consider an independent examination of ICFR effectiveness
Consider a Type 1 or 2 SSAE16 report (AICPA SOC 1 Report)


Decision Tree: Operations & Compliance
SingerLewak
Operations
Compliance
Are processes adequately designed to achieve operational and compliance objectives?
NO
Are processes effective to achieve operational and compliance objectives?
NO
Do business partners require independent assurance about how operational and/or compliance risks are addressed?
YES
YES
YES
Consider an independent review of internal control design
Consider an independent review of internal control effectiveness
Are the operational and/or compliance risks embodied in:
Are partners concerned about security, privacy, operating effectiveness or confidentiality
YES
Consider the benefits of a Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy (Distribution may be restricted) (AICPA SOC 2 Report)
NO
Other widely published standards (AICPA Trust Services, ISO, COBIT,
YES
Consider the benefits of an attestation report issued under AT101 (AICPA SOC 3 Report for Trust Services)
NO
Consider the benefits of a custom attestation report. (Distribution restricted)

So How Does This Affect My Organization?

- Using the SSAE 16 or SAS 70 when scoping and performing an audit
  - ➢ May be able to reduce the scope of the audit if the outsourced provider has a current SAS 70 or SSAE 16
    - ✓ Payroll
    - ✓ Data processing
    - ✓ Item processing (e.g. WesCorp or other providers)
    - ✓ Loan scoring/processing
  - ➢ Need to ensure the user (or client) control considerations are being reviewed periodically and are documented
    - ✓ Legal aspects to consider

So How Does This Affect My Organization? (cont'd.)

- CUSOs
  - ➢ Amendment to SEC Rule 206(4)-2, the custody rule under the Investment Advisers Act
    - ✓ Became effective March 12, 2010
    - ✓ Qualified custodian can use a SSAE 16 to provide the report on internal controls relating to the custody of client assets
      - – Advantages include having the examiners, external auditors, and internal auditors able to rely on the attestation
      - – Reduced scope, time, effort for the other audits and examinations
      - – Credit unions can ask that their servicers have a SSAE 16

So How Does This Affect My Organization? (cont'd.)

- Amendment to SEC Rule 206(4)-2, the custody rule under the Investment Advisers Act (cont'd.)
  - ✓ This report is prepared by an independent PCAOB-registered public accountant
  - ✓ This would not take the place of the required surprise examination

So How Does This Affect My Organization? (cont'd.)

- Management Assertion
  - Justifying the management assertion can be time-consuming
    - ✓ Wording has not been finalized yet
    - ✓ Can include that management's monitoring can support its assertion that through ongoing activities, e.g. periodic reviews or internal audit activities
  - Assertion's evaluation should include whether the review activities are being performed by someone with appropriate training
    - ✓ Most likely, the depth and extent of training will need to be detailed

So How Does This Affect My Organization? (cont'd.)

SingerLewak

- Third-party vendors (subservice organizations):
  - Current method: informal verification
  - New: if the service organization's system description includes a third party's control objectives and controls (e.g. payroll or physical security monitoring), need a written assertion as part of the service organization's report
    - ✓ This may be difficult for many smaller third-party providers to prepare and furnish

So How Does This Affect My Organization? (cont'd.)

SingerLewak

- Use of internal audit
  - Current: Internal Audit's work is not used; some sampling may overlap with Internal Audit
  - New: Can use some of internal audit's testing
    - ✓ Must specify the extent that the controls relied on internal audit
    - ✓ This is disclosed in Section 3's report of tests of operating effectiveness

So How Does This Affect My Organization? (cont'd.)

- Cost factors
  - Will vary according to
    - ✓ Type of audit (Type I or Type II)
    - ✓ Coverage period length (Type II only)
    - ✓ Number of control objectives
    - ✓ Number of controls overall
    - ✓ Number of locations in the organization
    - ✓ Complexity of the controls
    - ✓ Number and type of clients who will use the SAS 70
    - ✓ Number of application controls vs. the number of IT general controls

So How Does This Affect My Organization? (cont'd.)

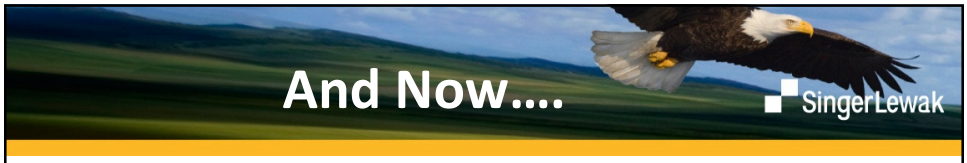
- How much will it cost?
  - Based on the variables, we have seen Type II SAS 70's vary from $25,000 to $45,000+
  - Wide variance in the number of controls and complexity
    - ✓ Some users have primarily IT general controls; some efficiencies are available
    - ✓ Application controls are specific to the organization and its IT environment
      - – Custom applications require more due diligence and effort to determine the key controls and the critical points in processing/handling
      - – Can also occur with a less common commercial off-the-shelf application

Pending Issues

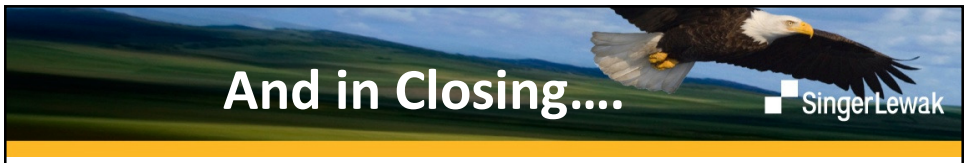
- Key Issues Pending Resolution
  - Guidance from AICPA expected in early 2011
  - Management assertion's prescribed wording has not been finalized yet
- If a significant piece of info is missing, the auditor must determine if that would change the use of the SSAE 16 by the typical user

Conclusion

- In summary,
  - SAS 70 is being updated and enhanced
  - Requires a new risk assessment for each audit (not just updated)
  - Need to determine if the carve-out method (i.e. exclusionary) will be used regarding subservicer organizations
  - Can now leverage Internal Audit's work
  - Management assertion now will be required
  - Several pending issues are to be resolved and clarified by the AICPA in 2011



Questions / Comments???



Thank you for your time!

Contact information:

John Mason
SingerLewak LLP
310.477.3924 x1451
jmason@singerlewak.com