


Association of Credit Union Internal Auditors

23rd Annual Conference and One-Day Seminar

Vendor Management Best Practices



Catherine Bruder
CPA, CITP, CISA, CISM, CTGA


CPAs AND ADVISORS

Michigan • Texas • Florida

Insight. Oversight. Foresight. SM


Forbes

TECH | 4/15/2013 @ 9:18PM | 2,677 views

Cloud Computing Gets Deeper and More Strategic, Survey Shows

TECH | 4/16/2013 @ 9:02AM | 4,018 views

The Cloud Hits the Mainstream: More than Half of U.S. Businesses Now Use Cloud Computing



IDC Forecasts

- \$100 billion spent on cloud services by 2016, compared to \$40 billion spent this year
- Represents 5-year compound annual growth rate (CAGR) of >26%
- By 2016, “Software as a Service” will account for 60% of the public cloud



What is changing in the industry?



NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-144

Vendor Management

Why Use a Third Party?

- Credit union's frequently use third-party vendors to:
 - reduce costs
 - enhance performance
 - obtain access to specific expertise
 - offer products directly to members



Vendor Management

Examples Include:

- Outsourcing audits
- Compliance reviews
- Disclosure preparation
- Information technology
- Website development
- More.....



Vendor Management

Vendor Risks

- It is important to emphasize, however, that while day-to-day management of a product or service can be transferred to a third party, ultimate responsibility for all compliance requirements cannot be delegated and remains with the credit union
- Credit union should recognize that using vendors involves significant compliance risk

7

 DoerenMayhew
CPAs AND ADVISORS

Vendor Management Risk

- The use of third-party vendors presents several other risks, the most prominent of which are strategic, legal, operational, reputational, credit, compliance and transaction risk.
- Other risks....



 DoerenMayhew
CPAs AND ADVISORS

Vendor Management Risk

Strategic risk

- Strategic risk is the risk arising from adverse business decisions, or the failure to implement appropriate business decisions in a manner that is consistent with the credit union's strategic goals.
- The use of a third party to perform functions or to offer products or services that do not help the financial institution achieve corporate strategic goals and provide an adequate return on investment exposes the financial institution to strategic risk.



Vendor Management Risk

Legal Risk

- The primary legal risk is that a vendor's operation does not comply with consumer protection laws and regulations.
- Because of the number of complex laws and regulations, the risk of noncompliance has increased significantly. Consequently, credit unions should be especially vigilant in identifying, assessing, monitoring, and mitigating this risk.
- Another legal risk involves legally binding contracts of a fixed duration. If business needs change because of intervening events, "there is a risk that credit unions may be locked into agreements that reflect outdated business realities. The contractual basis of outsourcing coupled with this intrinsic business uncertainty contributes to legal risk."



Vendor Management Risk

Reputational Risk

- A vendor's noncompliance with consumer laws and regulations creates reputational risk for a credit union, including the possibility of a public enforcement action by the institution's regulators, class action lawsuits, and negative publicity.



Vendor Management Risk

Operational Risk

- This is the risk that a vendor's operational system does not perform properly and negatively affects members.
- For example, if a credit union retains a vendor to determine if the institution's loans secured by a building or a mobile home are located in a special flood hazard area for purposes of complying with the flood insurance requirements of Regulation H, and the vendor fails to regularly update its database of special flood hazard areas, the institution could be cited by its regulator and subject to civil money penalties if this results in violations of Regulation H.



Vendor Management Risk

Transaction risk

- Various problems with service or product delivery.
- A third party's failure to perform as expected by members or the financial institution due to reasons such as inadequate capacity, technological failure, human error, or fraud, exposes the institution to transaction risk.
- The lack of an effective business resumption plan and appropriate contingency plans increase transaction risk.
- Weak control over technology used in the third-party arrangement may result in threats to security and the integrity of systems and resources. These issues could result in unauthorized transactions or the inability to transact business as expected.



Vendor Management Risk

Credit Risk

- Credit risk is the risk that a third party, or any other creditor necessary to the third-party relationship, is unable to meet the terms of the contractual arrangements with the credit union or to otherwise financially perform as agreed
- The financial condition of the third party itself
 - In originating loans, the financial condition of the third party is a factor in assessing credit risk
 - Solicit and refer members to other products,
 - conduct underwriting analysis
- Appropriate monitoring of the activity of the third party is necessary to ensure that credit risk is understood and remains within board-approved limits.



Vendor Management Risk

Compliance Risk

- Risk arising from violations of laws, rules, or regulations, or from noncompliance with internal policies or procedures or with the institution's business standards.
- This risk exists when the products or activities of a third party are not consistent with governing laws, rules, regulations, policies, or ethical standards.



Vendor Management Risk

Other Risks

- A comprehensive list of potential risks that could be associated with a third-party relationship is not possible.
- In addition to the risks described above, third-party relationships may also subject the financial institution to liquidity, interest rate, price, foreign currency translation, and country risks.

**The Vendor Management Program
Should Consider Other Risks**



Risk Mitigation

Risk Mitigation

- Credit unions that outsource a service or product must adopt appropriate controls, policies and procedures, and oversight to mitigate outsourcing risks effectively.
- Credit unions should focus on five key areas for effective risk mitigation:
 1. Vendor selection
 2. Vendor contract
 3. Vendor management and monitoring
 4. Human resource management
 5. Contingency planning



Risk Mitigation

Vendor Selection

- Conducting proper due diligence in selecting a vendor is a critical aspect of vendor risk management. Important due diligence steps include:
 - Asking the vendor to provide references (particularly ones from other credit unions) to determine satisfaction with the vendor's performance;
 - Asking questions about the vendor's data backup system, continuity and contingency plans, and management information systems;
 - Researching the background, qualifications, and reputations of the vendor's principals;
 - Determining how long the vendor has been providing the service;
 - Assessing the vendor's reputation, including lawsuits filed against it; and
 - Obtaining audited financial statements to check the vendor's financial health.



Risk Mitigation

- Some credit unions prefer to use other credit unions for outsourcing because they are already familiar with the business.
- Regardless, credit unions should ensure that qualified vendors are chosen after the appropriate level of due diligence is conducted.



Risk Mitigation

Vendor Contract

- Legally binding terms and conditions
- Credit unions should engage experienced counsel to ensure that its interests are protected and potential contingencies are considered
 - Regulatory changes
 - Performance
 - Expectations of both parties
- Given their significance and length, outsourcing contracts must be drafted carefully.



Risk Mitigation

Vendor Contract

In addition to the usual scope of services and terms, other issues need to be addressed in the contract:

- Written procedures;
- Minimum service levels (SLA)
- Approval required for vendor's use of subcontractors;
- Human resource issues (E.G., Outsourced staff);
- Right to conduct audits and/or accept third-party reviews of their operations;
- Retained ownership and confidentiality of data shared with service provider;
- Dispute resolution mechanisms, including service levels to be provided during the dispute, escalation procedures, and arbitration;



Risk Mitigation

Vendor Management and Monitoring

- Performance monitoring controls include:
 - Ensuring that the vendor is complying with consumer protection laws and regulations;
 - Periodically analyzing the vendor's financial condition and performing on-site quality assurance reviews;
 - Regularly reviewing metrics for the vendor's performance relative to service level agreements;
 - Reviewing customer complaints for services or products handled by the vendor and conducting anonymous testing if applicable (mystery shopper);
 - Assessing whether contract terms are being complied with;
 - Testing the vendor's business contingency planning;
 - Evaluating adequacy of the vendor's training to its employees; and
 - Periodically meeting with the vendor to review contract performance and operational issues.



Risk Mitigation

Human Resources Management

- Effect on credit union's staff
- May result in errors and productivity losses.
- More seriously, they can wound employee morale and lead to loss of desirable or key employees.
- In extreme cases, institutions fear misconduct or retaliatory behavior.”



Risk Mitigation

Human Resources

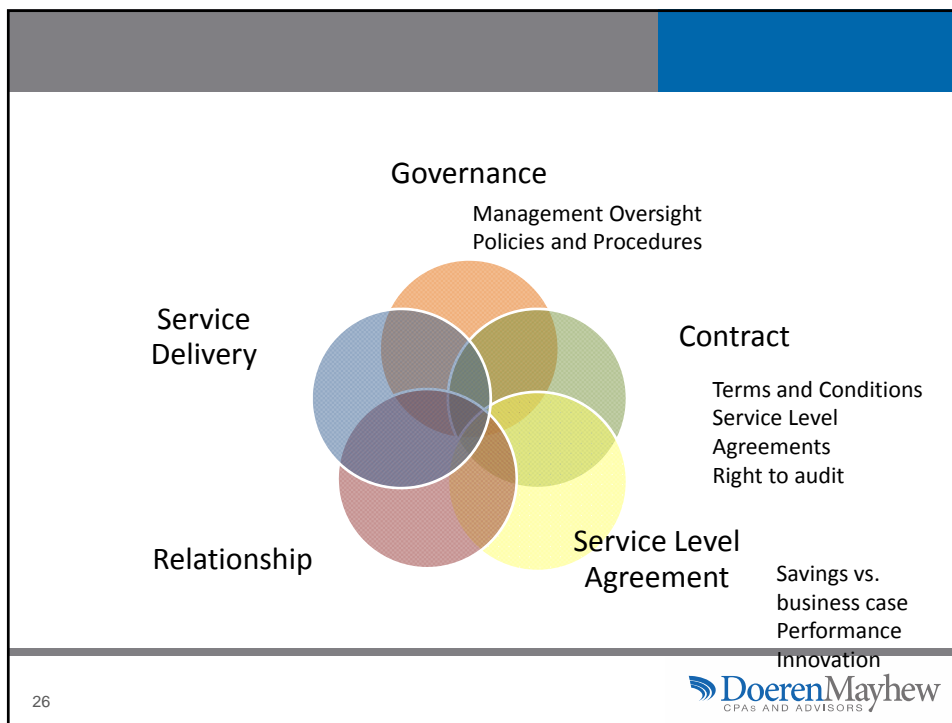
- To mitigate this risk, the Human Resources Department should be consulted early in the process to ensure that appropriate outreach is made to affected employees.
- Will the vendor be required to hire CU staff whose job functions are being outsourced and if so their compensation and term of employment be commensurate?
- Timely communications are very important so that staff are kept apprised and their concerns addressed.
- In addition, if the credit union does not want to transfer staff, it has to adopt contingency plans in the event its staff members are recruited by the third-party vendor.



Risk Mitigation

Contingency Planning

- What is the business continuity plan of the vendor?
- Review the vendors contingency plans on a regular basis
- The CU should have a contingency plan established to address the risk that the vendor may not perform satisfactorily



Service Level Agreements

Again – SERVICE LEVEL AGREEMENTS

- If it matters – include it
- The usual SLAs
 - Availability
 - Performance
 - Support coverage
 - Key performance indicators (and they should be tracked!)



Service Level Agreements

Again – SERVICE LEVEL AGREEMENTS

- SLAs for Security
 - Encryption
 - Access to your data
 - Data retention
 - Data destruction
 - Training
 - Employee background checks
 - Business continuity
 - Support for investigations
 - Control frameworks



Vendor Relationships

Subcontractors

- Subcontractors may be used
- Right of denial?
- Access to subcontractors SOC reports
- Non-disclosure agreements
- Controlling access to CU data
- Protection from viruses or breaches
- Dedicated hosting vs. Segregated databases



Performance Monitoring

Include Key Performance Indicators

- Evaluate the overall effectiveness of the third-party relationship and the consistency of the relationship with the financial institution's strategic goals.
- Review any licensing or registrations to ensure the third party can legally perform its services.
- Evaluate the third party's financial condition at least annually. Financial review should be as comprehensive as the credit risk analysis performed on the institution's borrowing relationships. Audited financial statements should be required for significant third-party relationships.
- Review the adequacy of the third party's insurance coverage.
- Ensure that the third party's financial obligations to others are being met.



Performance Monitoring

Include Key Performance Indicators

- Review audit reports or other reports of the third party, and follow up on any needed corrective actions.
- Review the adequacy and adherence to the third party's policies relating to internal controls and security issues.
- Monitor for compliance with applicable laws, rules, and regulations.
- Review the third party's business resumption contingency planning and testing.
- Assess the effect of any changes in key third party personnel involved in the relationship with the financial institution.
- Review reports relating to the third party's performance in the context of contractual requirements and performance standards, with appropriate follow-up as needed.



Performance Monitoring

Include Key Performance Indicators

- Determine the adequacy of any training provided to employees of the financial institution and the third party.
- Administer any testing programs for third parties with direct interaction with customers.
- Review member complaints about the products and services provided by the third party and the resolution of the complaints.
- Meet as needed with representatives of the third party to discuss performance and operational issues.



Vendor Management Exam

- Documentation supporting the business case for the application
 - Scope and nature;
 - Standards for controls;
 - Minimum acceptable service provider characteristics;
 - Monitoring and reporting;
 - Transition requirements;
 - Contract duration, termination, and assignment; and
 - Contractual protections against liability.



Vendor Management Exam

- The extent to which the institution
 - Reviews the financial stability of the service provider;
 - Analyzes the service provider's audited financial statements and annual reports;
 - Assesses the service provider's length of operation and market share;
 - Considers the size of the institution's contract in relation to the size of the service provider;
- Reviews the service provider's level of technological expenditures to ensure ongoing support; and
- Assesses the impact of economic, political, or environmental risk on the service provider's financial stability.



Vendor Management Exam

- Due diligence considers the following:
 - References from current users or user groups about a particular technology service provider's reputation and performance;
 - The service provider's experience and ability in the industry;
 - The service provider's experience and ability in dealing with situations similar to the institution's environment and operations;
- Shortcomings in the service provider's expertise that the institution would need to supplement in order to fully mitigate risks;
- The service provider's proposed use of third parties, subcontractors, or partners to support the outsourced activities;
- The service provider's ability to respond to service disruptions;
- Key service provider personnel that would be assigned to support the financial institution;
- The service provider's ability to comply with appropriate federal and state laws including GLBA and BSA and Country, state, or local risk.



Vendor Management Exam

- Periodic monitoring of the service provider relationship(s), including:
 - Timeliness of review, given the risk from the relationship;
 - Changes in the risk due to the function outsourced;
 - Changing circumstances at the service provider, including financial and control environment changes;
 - Conformance with the contract, including the service level agreement; and
 - Audit reports and other required reporting addressing business continuity, security, and other facets of the outsourcing relationship.





The Cloud





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


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

39

 **DoerenMayhew**
CPAs AND ADVISORS

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

 **DoerenMayhew**
CPAs AND ADVISORS

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 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

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



More than SAS 70

Trust Services Principles & Criteria

- Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy



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




 **DoerenMayhew**
CPAs AND ADVISORS

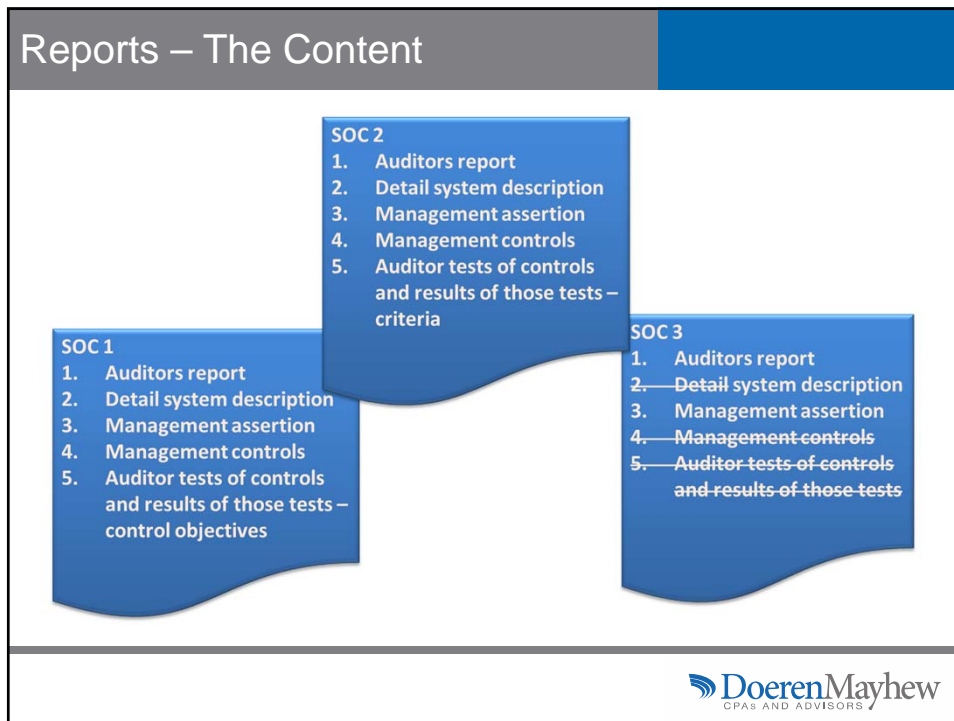
SOC Reports

- 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

 **DoerenMayhew**
CPAs AND ADVISORS

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 Reports


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*


CPAs AND ADVISORS

New Requirement for Assertion

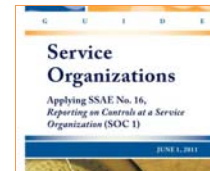
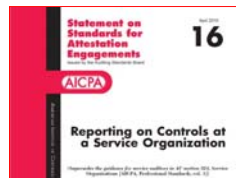
Service auditor must obtain written assertion from service organization's management about the fairness of the presentation of the description of the service organization's system and about the suitability of the design



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**



SOC 1

Internal Controls over Financial Reporting

- ICFR is the specific criteria for SOC 1

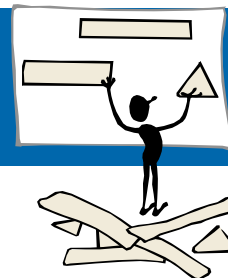
These reports are intended to meet the needs of entities that use service organizations (user entities) and the CPAs who audit the user entities' financial statements (user auditors) when evaluating the effect of controls at the service organization on the user entities' financial statements

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 2



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



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.



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:

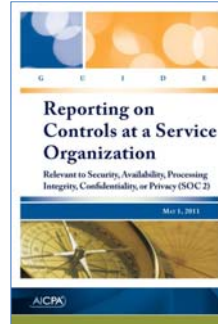
- Determine whether the controls implemented by the service organization address the user organization's risks
- Identify the complementary user entity controls that must be in place to meet the control objectives



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



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

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?



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?



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**



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.

Internal Audit



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.



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



SOC 2 – What To Look For

1. Type 2 Report
2. 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
3. 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



SOC 3



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



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



Outsourcing Discussion



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



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



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?





Thank You!

Catherine Bruder
Shareholder
IT Assurance and Security Group
Phone: 248.244.3295
bruder@doeren.com



Michigan • Texas • Florida

Insight. Oversight. Foresight. SM