CU Accelerator

Understanding Vendor Risk And Analyzing the SSAE No. 16

Accelerate your Credit Union's Performance

June 19, 2014

AUSTIN, TEXAS • www.cuaccelerator.com

Agenda – Vendor Management

- Key Outsourcing Risk Areas
- Controls for Different Types of Vendor Risks
  - Operational Reliance
  - Billing/Financial
  - Transaction Processing
  - Management of Confidential Data
- Technical Analysis of the SSAE No 16

CU Accelerator

General Outsourcing Risks

- Business Risks
  - Alignment with Strategy
  - Alignment of incentives
- Contract Risks
  - Enforceability
  - Real options (how do I get out of this?)
- Operational Risks
  - Day to day criticality
  - Processing of transactions
  - Over-reliance on operations (lack of alternatives)
  - Information Security Risk
- Reputation, Compliance & Legal Risk
  - If they are acting on your behalf, you are still responsible!

CU Accelerator

Agenda – Vendor Management

- Key Outsourcing Risk Areas
- Controls for Different Types of Vendor Risks
  - Operational Reliance
  - Billing/Financial
  - Transaction Processing
  - Management of Confidential Data
- Technical Analysis of the SSAE No 16

CU Accelerator

Vendor Specific Outsourcing Risks

- Operational Reliance
  - What would you do without them?
  - How long would it take to switch?
  - Can it be brought in house?
  - How important are we to them (can they decide to drop us)?
- Billing/Financial
  - High dollar value
  - Complex/inconsistent billing practices
- Transaction Processing
  - Accuracy
  - Service Level
- Management of Confidential Data
  - What is the nature of the data the vendor manages?
  - What access to they have?
  - What do they outsource to yet another vendor?
  - *Where* is the data stored?

CU Accelerator

Vendor Risk & Response Summary

Risk Source	Appropriate Response
Operational Reliance	Review of Financial Position Service Level Agreements Dual Sources Identified Perform In-house
Billing/Financial	Contract Terms/Real Options Monitoring of Invoices/Billings
Transaction Processing	SSAE No. 16/Process Audit Enhanced Internal Controls
Management of Confidential Data	Encryption/Security SSAE No. 16/Security Audit Enhanced Internal Controls

Agenda – Vendor Management

- Key Outsourcing Risk Areas
- Controls for Different Types of Vendor Risks
  - Operational Reliance
  - Billing/Financial
  - Transaction Processing
  - Management of Confidential Data
- Technical Analysis of the SSAE No 16

CU Accelerator

Statement on Standards for Attestation Engagements No. 16 (SSAE 16)

- An audit conducted by a CPA firm
  - Once called SAS 70 (replaced by SSAE 16 in June, 2011 in order to comply with international standards)
- Type I includes description and assessment of controls, Type II includes tests of controls
- Three areas of Service Organization Controls
  - SOC 1 for Financial Controls (Accounting)
  - SOC 2 & 3 for Non-Financial Controls (security, availability, etc.)

CU Accelerator

SSAE is Appropriate When

- You already understand the risk in the process, and want to get an assessment of the *controls*
  - Excellent for assessing Information Security or processing timeliness & accuracy
- You need an external assessment to transfer risk
  - Once they perform an SSAE No. 16, the audit firm is *on the record*

CU Accelerator

SSAE No 16 is NOT Appropriate

- For systems/processes performed or maintained *in house* by credit union staff
- When you are the *only* customer using a specific service
- For evaluating the business viability of the vendor
- For obtaining assurance related to invoicing/billing
- For hoping that the vendor will tell you how to manage your risk

CU Accelerator

Weaknesses in SSAE No. 16

- The *auditee* (not you or even the auditor) will identify the review areas
  - Loan application processing, Updates to information systems, Protection of member data, etc.
- The *auditee* (not you) will determine Type I or Type II
  - Type I reports should be heavily scrutinized
- The audit period may not match your reporting period (primarily relevant for SOC 1's)

CU Accelerator

Weaknesses in SSAE No. 16

- Specific controls will be tested based on the *vendor's* procedures
  - *Scope, carve-outs, and Complementary User Entity Controls are extremely important*
  - You need to understand what's covered (and what's not)
    - This means that the reviewer (you) needs to be an expert on the areas of controls being reviewed
    - A clean SSAE No. 16 does *not* mean there is no (less) risk!
- Alternatives for gaining additional assurance
  - Review by customer/Agreed upon procedures
  - Effective internal (credit union) controls

CU Accelerator

Analyzing the SOC – Key Terms

- Service Organization (the vendor)
  - Sets the scope for the audit
  - Creates a description of controls and processes
  - Selects the audit firm and *pays the bill*
- Service Auditor (the audit firm)
  - Audits the controls as defined by the Service Organization (vendor)
  - Issues report summarizing the evaluation
- Audit Period
  - The period of time being reviewed
- Report Type
  - Type I –Review the control description and confirm they are “placed in operation”
  - Type II – Tests the controls to determine if they are operating in a reliable manner
  - This is not always specifically stated – but the opinion letter will contain language

CU Accelerator

SOC 1 versus SOC 2/3

- SOC 1 Reports will reference “financial reporting” or “accounting” in the opinion
  - Primary concern is accuracy of financial statements
  - Can “pass” controls that fail tests if it can be determined that the control failures would not affect *that year’s* financial statements
  - Certain controls (BCP, Incident Management, User Access Administration, Change Management) can be excluded if there were no events

CU Accelerator

SOC 1 versus SOC 2/3

- SOC 2 & 3 Reports will reference other operational controls in the opinion ("Security & Privacy", "Confidentiality", "Availability of Operations", etc.)
  - Must focus on on-going operations (theoretically)
  - *Should not* allow controls that fail tests to be satisfied by examining the underlying transactions

CU Accelerator

Section One (Usually) – Independent Service Auditor's Report

- 1-2 page report summarizing the results of the audit and opinion of the auditor
- Separate opinions for the design of controls (Type I and Type II) and the test of controls (Type II only)
- Defines the scope of the report as well as SOC 1 or SOC 2/3
- Auditor has three options in writing the opinion:
  - Effective – all controls were designed effectively and the tests were conducted without major problems being noted
  - Effective with exceptions – controls were effective, but some minor problems were noted (your standards for minor may be different than the auditor's)
  - Qualified Opinion - Some part of the audit failed (but probably not all of it)
- Beware - the Auditor and Service Organization may change the scope during the "planning phase" of the project to ensure an unqualified opinion
  - And there is nothing in the report to tell you!
  - It is up to you to determine if the scope is sufficient!

CU Accelerator

Section Two (Usually) – Management's Assertion

- Statement from management stating that the controls are accurately presented to the best of their knowledge
  - SAS 70 did not require this
  - Primarily used to synch to Sarbanes-Oxley requirements (many vendors sell to publicly held companies)
  - Does not allow management to deny responsibility for control weaknesses due to ignorance of the control environment
  - Requires statement that there are no significant omissions (sort of)
- Similar to the auditor's opinion letter
  - Includes management's assessment of the design and operating effectiveness of controls

CU Accelerator

Section Three – Description of Internal Controls Provided by Service Organization

- This section is completed by the vendor and reviewed (not audited) by the auditor
- No set format, but typically includes descriptions of:
  - The organization and its business
  - Its control environment and methodology including industry standards it follows (these can be quite lengthy)
  - Vendor has a lot of flexibility in what is listed and in some cases the description of controls will not match the auditor's testing in section four
- Complementary User Entity Controls (formerly called User Control Considerations)
  - Describes things that are the responsibility of the customer (you)
  - This is the *most important* part of the report
  - Excellent things to include in internal audits

CU Accelerator

Complementary User Entity Controls Can be Very Broad

- Would you expect a loan processing outsourcer to guarantee:
  - Loans are processed according to your parameters?
  - Transactions are complete and accurate?
  - Regulatory updates are implemented?
  - Maintain password controls?
  - Encryption is used?
  - Compliance with their own operating standards?
  - Service levels/availability?

CU Accelerator

Section Four –Information Provided by the Service Auditor

- Provides a list of controls, organized by control objective, that were tested as well as the methods used, and the results
- Testing plans must comply with AICPA standards, but the auditor is given a lot of latitude in developing test plans
- Audits require specific evidence that can be collected through four primary methods
  - *Inquiry* – very light includes asking questions of management
  - *Observation* – watch management execute the process
  - *Re-performance* – redo the control independently with test data
  - *Sampling* – review of a set of transaction to ensure the control worked every time (strongest method – but be careful of the sampling method)
- It's critical to understand the strengths and weaknesses of each based on the risks you are trying to mitigate

CU Accelerator

Section Five – Other Information Provided by Service Organization

- Gives the vendor the ability to describe controls that were not part of the review
  - These may or may not be relevant to your operations
  - The vendor has total flexibility in this section
  - Often includes responses to findings, or descriptions of secondary controls (certifications, etc.)
  - Can be a place to "hide" controls that were not in the audit scope, but that the vendor wants to say they have (BCP/DRP is very popular!)
  - This section is not audited or verified by the service auditor (so you probably don't want to rely on it)

CU Accelerator

What if the vendor fails?

- If the auditor's test or scope was the concern:
  - Audit the vendor's operations yourself
  - Hire an audit firm to conduct an "Agreed Upon Procedures" review
- If still in the selection stage, avoid the risk by canceling the project
- If it is possible to switch, find another vendor (or dual source)
- Bring the process in-house
- Realistically, the most likely scenario is that you will need to strengthen your internal controls
  - Costs of implementing controls should be added to the cost/benefit analysis of the product/service that the vendor is providing
- Other option is to live with the unmanaged risk
  - Some estimation of costs for poorly controlled processes should be added to the cost of the vendor

CU Accelerator

Questions & Contact Information

Alan White, President
alan@cuaccel.com
512-547-1251

CU Accelerator