CU Accelerator

Tactics for Managing Vendor Risk and Analyzing Vendor Information

Accelerate your Credit Union's Performance

June 19, 2018
AUSTIN, TEXAS • www.cuaccelerator.com

Vendor Risk & Response Summary

Risk Source	Appropriate Response
Operational Reliance	Review of Financial Position Service Level Agreements Dual Sources Identified Perform In-house
Transaction Processing	SOC Reports/Process Audit Enhanced Internal Controls
Management of Confidential Data	Encryption/Security SOC Reports/Security Audit Enhanced Internal Controls
Billing/Financial	Contract Terms/Real Options Monitoring of Invoices/Billings

Evaluating the Business Model

- How does this organization make money (margins, fixed costs, *cash flow*, etc.)?
- Who are their customers?
  - How do you compare to most of their customers (size, complexity, concentration, customization)?
- What expertise/advantage do they have that you do not?
- Is what you are buying their primary business?
- Who are their competitors?
- What do they outsource?
  - Do the same steps for any critical outsourcers they have!

CU Accelerator

Evaluating the Financial Position

- Are revenues increasing or decreasing?
- Are margins increasing or decreasing?
  - Are costs are rising faster than revenues?
- What is their cash position?
- How are they financed (equity or debt)?
  - Has this changed recently?
- What are their largest financial commitments?
  - How much revenue/margin reduction can they withstand and maintain these?
- Have any competitors had financial difficulties?
  - This can be a sign of bad industry fundamentals!

Specific Number to Analyze

- Overhead Ratio (Ability to sustain operations)
  - Operating Expense/Operating Income
  - Lower is better
- Interest Coverage (Ability to cover their borrowing costs)
  - Operating Income/Interest Expense
  - 10 or above is preferred
- Current Ratio (Short term liabilities vs short term assets)
  - Current Assets/Current Liabilities
  - The higher the better – but you may allow for timing differences (they collect faster than they pay)
- Debt to Equity (Financial flexibility)
  - Total Debt/Total Equity
- *Would you buy their stock if you could?*

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
Transaction Processing	SOC Reports/Process Audit Enhanced Internal Controls
Management of Confidential Data	Encryption/Security SOC Reports/Security Audit Enhanced Internal Controls
Billing/Financial	Contract Terms/Real Options Monitoring of Invoices/Billings

Top 10 Issues Identified in Vendor Audits

1. Early Payment Discounts
2. Balance Payments To Billings
3. Estimated Payments Not Reconciled to Actual
4. Billing rates not in accordance with those in contract
5. Intentional rounding in the suppliers billing process
6. Benefits rate is overstated and not adjusted to actual
7. Billed for services or materials that are not part of the contract
8. Inadequate billing controls resulting in wrong quantities billed
9. Inadequate security over confidential credit union data
10. Supplier fraud

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
Transaction Processing	SOC Reports/Process Audit Enhanced Internal Controls
Management of Confidential Data	Encryption/Security SOC Reports/Security Audit Enhanced Internal Controls
Billing/Financial	Contract Terms/Real Options Monitoring of Invoices/Billings

Assess Risk *Before* Reading the SOC

- The vendor's risks become your risks as soon as you engage then
- The approach is similar to a process risk assessment ("deep dive") for an in house process
- Identify risks that would be in your process if it were in house
- Add risks that are created by outsourcing
- Outsourced processes have *more* risk - not less
  - Risk in outsourced processes needs to be managed *better* that in internal processes
  - You (or someone in your credit union) will need to become an expert in relevant controls (IT, processing, etc.)

CU Accelerator

Identifying Process Risks

- Risks exist where:
  - The process begins
  - Data needs to be captured or processed (follow the data)
  - Money or transactions are processed (follow the money)
    - Incentive for fraud, abuse, or misuse exists
  - There is reliance on/interaction with external parties
    - Incentives may not be aligned
    - Never discount lunacy
  - Systems do not interface
  - Compliance requirements exist
  - The process ends

Options for Managing Risk

- Insurance
- Internal Processes
- Internal Audit/Compliance Review of Vendor Control Information (procedures, network security, etc.)
- Agreed Upon Procedures
- Service Organization Control (SOC) Reports

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 SOC, the audit firm is *on the record*

SSAE no 18 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

Confessions of a Service Auditor

- 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

Confessions of a Service Auditor (con't)

- Specific controls will be tested based on the *vendor's* procedures
  - *Scope, carve-outs, and Complementary User Entity Controls are key*
  - 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 SOC does *not* mean there is no (less) risk!
- Several alternatives for gaining additional assurance
  - Review by customer/Agreed upon procedures
  - Effective internal (credit union) controls

Statement on Standards for Attestation Engagements No. 18 (SSAE 18)

- 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 and again updated with SSAE 18 in May, 2017)
- Originally intended to give assurance related to financial reporting of transactions processed by outsourcers
- Gives outsourcers the ability to only audit a process once rather than have audits conducted by customers
- Very common for IT, Payroll, Claims, Collections, etc.
- 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, transaction processing, etc.)

SSAE no. 18 – What's New

- New Requirements related to subservice providers
  - In the past, vendors could use the "carve out" method to essentially de-scope activities of subservice providers (their vendors)
    - This forced customers (us) to obtain and review documents from each subservice provider that the vendor used.
  - Now, they must include controls to analyze their key subservice organizations and perform periodic assessments
    - Does not remove the risk, but it is an improvement

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
  - Issues report summarizing the evaluation
- Report Type
  - Type I – Includes a review of the control description and confirms they are placed in operation
  - Type II – Tests the controls to ensure they are operating in a reliable manner within audit guidelines
  - This is not always specifically stated – but the opinion letter will contain language that can help determine the type
- Audit Period
  - The period of time being reviewed

CU Accelerator

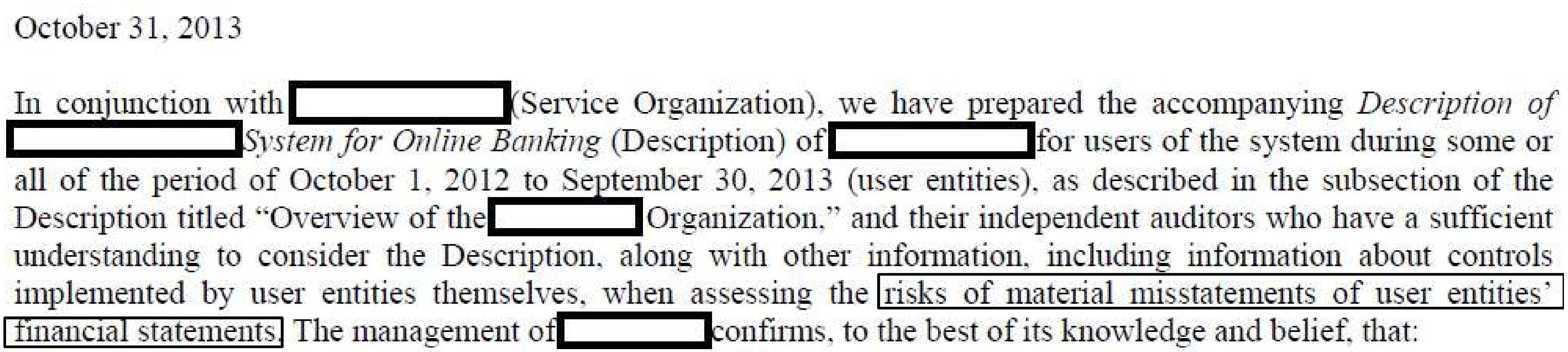
Analyzing the SOC – Cover Page

- Type I or Type II (may or may not be on the cover page)?
  - A Type I does not include a test of controls
    - Often means the controls are new or the vendor knows they will not pass if tested
  - Type II includes everything in a Type I plus tests of controls
- What is the Audit Period?
  - Usually period of at least six months (many are now 12 months)
  - For operational purposes, ensure the period is sufficiently long
  - For accounting purposes, the entire period should be within your financial reporting period or your reliance can not be as strong
- Who is the Auditor?
  - There is wide variation in competency among and within firms (even among the big firms)
  - Think of the auditor as another vendor

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

SOC 1



October 31, 2013

In conjunction with [redacted] (Service Organization), we have prepared the accompanying *Description of* [redacted] *System for Online Banking* (Description) of [redacted] for users of the system during some or all of the period of October 1, 2012 to September 30, 2013 (user entities), as described in the subsection of the Description titled "Overview of the [redacted] Organization," and their independent auditors who have a sufficient understanding to consider the Description, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. The management of [redacted] confirms, to the best of its knowledge and belief, that:

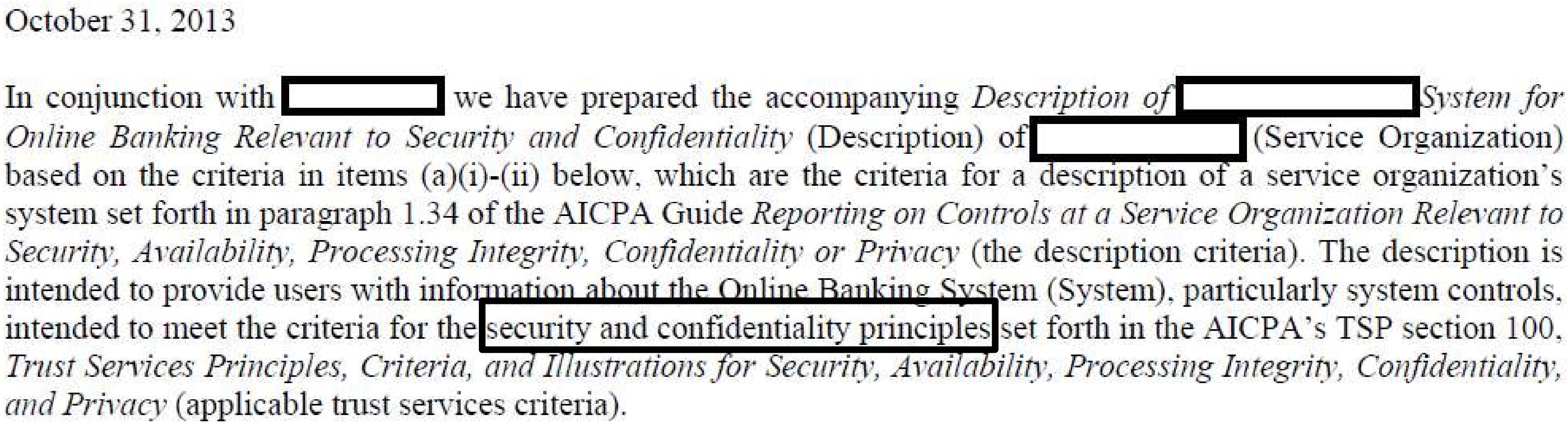
SOC 1 versus SOC 2/3

- SOC 1 Reports will reference “financial reporting” or “accounting” in the opinion
  - Primary concern is accuracy of financial statements
  - Can “pass” controls that fail a test if it can be determined that the control failures did not affect *that year’s* financial statements (substantive testing)
  - Certain controls (BCP, Incident Management, User Access Administration, Change Management) can be excluded if there were no events.
  - The auditor also has some latitude in assessing control testing issues.

SOC 1 versus SOC 2/3

- SOC 2 & 3 Reports will reference the controls in scope in the opinion (Security, Privacy, Confidentiality, Processing Integrity, Availability)
  - Security is always required
  - *Should* focus on on-going operations
  - *Should not* allow controls that fail tests to be satisfied by examining the underlying transactions

SOC 2



October 31, 2013

In conjunction with [redacted] we have prepared the accompanying *Description of* [redacted] *System for Online Banking Relevant to Security and Confidentiality* (Description) of [redacted] (Service Organization) based on the criteria in items (a)(i)-(ii) below, which are the criteria for a description of a service organization's system set forth in paragraph 1.34 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy* (the description criteria). The description is intended to provide users with information about the Online Banking System (System), particularly system controls, intended to meet the criteria for the security and confidentiality principles set forth in the AICPA's TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

SOC 2 and SOC 3

- SOC 2 Reports will list the specific controls performed, organized by control objective
- In many cases, these controls will overlap (so the reports can be longer than necessary)
- Control testing exceptions are included
- Security is always required, but the vendor can choose to only focus on other specific areas of the standard (Availability, Privacy, Confidentiality, Processing Integrity)
- SOC 3 does not list controls, but the vendor must comply with a strict interpretation of the standard and can have no testing exceptions

SOC versus Type

SOC Number and Objective	Type 1	Type 2
SOC 1: Financial Statement information	Controls Exist	Controls Operating
SOC 2: Security, Availability, Privacy, Confidentiality, ***and/or*** Processing Integrity	Controls Exist	Controls Operating
SOC 3: SOC 2 – without control listings, but all controls must pass	No such report	Controls operating but not disclosed

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

- Brief (1-2 pages) report summarizing the results of the audit and the option of the auditor
- Separate opinions for the design of controls (Type I and Type II) and the test of controls (Type II only)
- Auditor has three options in writing the option:
  - 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)

Type 1 or Type II?

- From the Service Auditor’s Report:

  a. The description fairly presents the system related to the ABC System, (“ABC”), developed by XYZ and relevant general computer controls over application change management at its Anytown, Anystate facility that was designed and implemented throughout the period October 1, 2011 to September 30, 2012.

  b. The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period October 1, 2011 to September 30, 2012, and user entities applied the complementary user entity controls contemplated in the design of XYZ’s controls throughout the period October 1, 2011 to September 30, 2012.

  c. The controls tested, which together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period October 1, 2011 to September 30, 2012.

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

- Brief (1-2 pages) report summarizing the results of the audit and the option of the auditor
- Separate opinions for the design of controls (Type I and Type II) and the test of controls (Type II only)
- Auditor has three options in writing the option:
  - 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!

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
- Similar to the auditor's opinion letter
  - Includes management's assessment of the design and operating effectiveness of controls

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)
  - Its Vendor is given a lot of flexibility in what is listed and in some cases the description of controls will not match what is tested by the auditor in section three (e.g. system availability)
- Complementary User Entity Controls (formerly 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

Complementary User Entity Controls Can be 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?

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

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
  - This section is not audited or verified by the service auditor (so you probably don’t want to rely on it)

When assessing risk in an outsourced process:

- First evaluate the process risks *regardless* of who performs what functions within the process
- Identify controls that are important to you to mitigate those risks *regardless* of who performs what functions within the process
- Review the SOC to determine which of those controls are performed by the vendor, and which are your responsibility
  - Those in Section Three of the report are the *vendor's* responsibility
  - The Complementary User Entity Controls are *your* responsibility
  - Those listed as a carve-out may be some other vendor's responsibility and you will need to review those separately

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

Questions & Contact Information

Alan White, President

alan@cuaccel.com

512-547-1251