CU Accelerator

A Vendor Risk Management Example and Key Lessons Learned

"Driving Credit Union Performance"

June 19, 2018

AUSTIN, TEXAS • www.cuaccelerator.com

Common Mistakes

- Putting the responsibility with departments/people who do not fully understand all aspects of the function
- Creating policies from boiler plates that do not meet the needs of the CU; or putting great policies in place and not following them
- Using the wrong risk matrix strategy
- Failing to offer periodic training for ***all*** people involved in the process
- Failing to address process flow from the onset of the program (or failing to cover all aspects of the program in the flow)
- Implementing inadequate reporting – or no reporting at all
- **Forgetting how much NCUA cares about this**

CU Accelerator

Common Mistakes

- Poor organization
  - Sloppy/inconsistence categorization and retrieval methods
  - Inefficient (i.e. using 10 manual spreadsheets)
  - Weak processes to manage changing methods/versions of retention plans
- Poor follow through
  - Failure to heed legal advice on contract negotiation
  - Failure to receive appropriate information when needed (SOC Analysis, financials, etc.)
  - Poor monitoring of vendor performance and service level standards
  - No advanced planning for termination

CU Accelerator

Making the best practices work

- Determine where responsibility for the program lies
  - Risk
  - Compliance/legal
  - Other unrelated departments
  - Decentralized to individual departments/managers

CU Accelerator

Making the best practices work

Ensure all necessary aspects are adequately covered

- Policy approval/update
- Risk rating of the contract relationship
- Vendor selection/RFP/needs assessment
  - Initial contract review/negotiation
  - Financials, critical data, etc.
  - SOC Analysis review (this is more than User Controls)
  - DRP/BCP
  - Insurance needs
  - Payment

CU Accelerator

Making the best practices work

Ensure all necessary aspects are adequately covered

- Policy approval/update
- Risk rating of the contract relationship
- Vendor selection/RFP/needs assessment
  - Initial contract review/negotiation
  - Financials, critical data, etc.
  - SOC Analysis review (this is more than User Controls)
  - DRP/BCP
  - Insurance needs
  - Payment
- Ongoing monitoring (due diligence)
- Periodic audit/review

CU Accelerator

Ongoing monitoring

- The risk rating should drive the details of the monitoring. Examples:
  - Financials
  - SOC Analysis
  - Updated risk matrix
  - Information Security
- Ensure vendor performance is being evaluated and documented by all departments who are affected by the relationship.
- PLAN for termination!

CU Accelerator

Policy Creation

- Take advantage of your peers and industry resources. There is no need to recreate the wheel, but MAKE SURE the template you choose works for your specific credit union
- You need the “right amount” of complexity and simplicity for your CU. Vendor Risk Management is NOT one size fits all
- Don’t forget NCUA requirements
- NCUA minimum requirements: Planning, Risk Assessment, Due Diligence, Compliance, Vendor Monitoring , Documentation, and Reports
- Keep the Board approved policy simple, limited to NCUA requirements. Put the “meat” into your guidelines/procedures

CU Accelerator

Policy Management Options

Centralized

- Probably pretty easy to manage. One person responsible for the policy upkeep, reviewing any regulatory changes and their impact to your policies, etc.

Decentralized

- Probably a good practice to identify one primary person to be responsible for coordination of policy management

CU Accelerator

Choosing the Right Risk Rating System

Simple rating system: High, Medium, Low

- High – critical to operations; expensive relationship; difficult and costly to replace vendor; high member impact, etc.
- Medium – important to operations; “middle of the road” expense; takes a lesser amount of resources and time to replace the vendor; may have limited member impact, etc.
- Low – not critical to operations; low cost; many vendors available to offer the service; no member impact, etc.

CU Accelerator

Choosing the Right Risk Rating System

More intricate risk rating system:

- Establish tiers based on specific criteria
- Different aspects of the relationship may have different scores (Cost may have a 5 but Information may be a 2…)
- Treatment of various aspects of the contract may differ

CU Accelerator

Making all of the other pieces fit

- Risk rating should drive all other aspects of the process
  - Risk rating should identify which relationships require certain steps, i.e. financial review, legal review of contract, SOC Analysis, etc.
- If the risk rating doesn't drive the review process, then likely all contracts will be subject to full analysis.
- Don't forget to address the process flow and timing of everything!
  - Identify which steps come first, second, third, etc. and who is responsible for those steps

CU Accelerator

Making all of the other pieces fit

- Before even considering a vendor, establish what you need to accomplish through the relationship
- Create a wish list. Start with the “must haves,” then list the “would really like to haves” in order of importance.
  - Usually will span over a few different departments

CU Accelerator

Decisioning

- It's helpful to have standards in place to drive decisioning.
  - What is the plan to manage legal /SOC Analysis/financial review, etc. that reveal concerns?
- Ask the vendor in advance if contract terms are generally negotiable. Try to get a sample contract.
- Management should agree on "deal breakers" in advance. Don't waste time with vendors that can't work within your deal-breaker terms.

CU Accelerator

Vendor/Contract Review

- Don’t forget the details
  - Does this vendor interfere with a non-compete clause you have with an existing vendor?
  - Are you creating a sub-relationship that results in an extended relationship with that vendor?
  - Is this a CUSO? If so, consult NCUA Rules & Regulation Part 712
  - Does this contract change your Privacy Notice?

CU Accelerator

SOC Analysis

- Outsource or review internally?
- Either way, what are you doing with the results?
  - Even an outsourced review will require some internal attention and decisions
  - Don’t forget the User Controls section!
- Don’t forget to consider sub-servicers and their impact on your relationship & review

CU Accelerator

Enforcing Vendor Policy Compliance

- Great Controls:
  - Clean up the A/P Process so that payments cannot be make “outside the lines”
  - Vendor cannot be added to A/P Vendor Master file without due diligence checklist and/or signoff from vendor management specialist
  - Compare A/P Vendor Master file to master vendor list annually
  - Audit of vendor for billing, service level, etc. based on risk profile
  - Escalate invoice approval if billing issues have been identified in the past

CU Accelerator

Questions

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

CU Accelerator