

Creating a third party risk scoring system

Vendor Risk Processes

1. Create a scoring system/template
2. Score vendor & based on the risk, decide what steps are needed to analyze the vendor
3. Review the outcome & make a risk decision

Types of Risk

- ▶ Strategic
- ▶ Reputation
- ▶ Transaction
- ▶ Credit
- ▶ Compliance
- ▶ Financial
- ▶ IT
- ▶ Billing/Accounting
- ▶ What else??

Important factors in risk weighting

▶ Criticality

▶ Cost

▶ Compliance

▶ Data/information
sharing

▶ WHAT ELSE??

Creating a Risk Matrix

DETERMINE THE BEST SCORING SYSTEM FOR THE CREDIT UNION'S SIZE, COMPLEXITY, AND PROGRAM VOLUME

- ▶ High, Medium Low method
- ▶ Matrix, based on risk factors
- ▶ Third party software program (which will need to be evaluated per your vendor management program...)

High/Medium/Low Method

ADVANTAGES

- ▶ Simple
- ▶ Fairly easy to track
- ▶ Easily understood by examiners/auditors

DISADVANTAGES

- ▶ May be too simple for credit unions with complex third party relationships
- ▶ Often creates too much or too little due diligence than is actually necessary

High Risk Indicators

- ▶ Critical to operations
 - ▶ Without them, may not meet RPO and RTO standards
- ▶ Difficult to replace in a reasonable period of time
- ▶ Direct Member impact
- ▶ High cost
- ▶ Access to confidential/proprietary data and/or NPI
- ▶ Highly sophisticated with somewhat limited competitive options
- ▶ Significant compliance implications
- ▶ What else???

Medium Risk Indicators

- ▶ Important to operations but not essential
- ▶ Lower cost compared to Net Worth
- ▶ Able to replace in a reasonable period of time
- ▶ Indirect member impact but not reputation-damaging
- ▶ Access to limited or no confidential/proprietary data and/or NPI
- ▶ Few or insignificant compliance implications
- ▶ What else???


Low Risk Indicators

- ▶ Not important to operations
- ▶ Low cost
- ▶ Able to replace quickly
- ▶ Little to no member impact
- ▶ No access to internal/confidential/proprietary data
- ▶ Multitude of replacement options
- ▶ Little/no compliance implications
- ▶ What else???



BUILD YOUR RISK MATRIX

Vendor Risk Process

1. Create a scoring system/template 
2. Score vendor & based on the risk, decide what steps are needed to analyze the vendor
3. Review the outcome & make a risk decision



DUE DILIGENCE

BASED ON THE RISK OF THE VENDOR!!

DUE DILIGENCE – HIGH RISK

- Reference checks
- Background checks
- Public database searches
- Review of financial condition
- Compliance analysis

DUE DILIGENCE – HIGH RISK

- Insurance coverage
- Business continuity/disaster recovery (BCP/DRP)
- Legal review of contract
- Software escrow
- Senior or exec level approval of contract

DUE DILIGENCE – HIGH RISK: DATA

What data? What exactly is used/stored/shared and how is that data categorized?? (confidential, public, sensitive, etc.)

- Data storage
- Data retention
- Complete, timely access to your information
- Subcontractors
- Software escrow
- SOC REPORTS (SOC I, SOC II, SOC III, Type I, Type II...)
- Physical and application safeguards

Due Diligence

LOW RISK

- ▶ OFAC
- ▶ Public Records
- ▶ Background checks

MEDIUM RISK

- ▶ All of Low-risk AND:
- ▶What?



Apply the same or
similar standards to
monitoring



RISK RATE YOUR
VENDOR

INSTRUCTIONS

- ▶ Score your vendor based on the matrix you created
- ▶ Be ready to share why you scored the way you did
- ▶ Based on the score, define the due diligence requirements and why you selected those requirements

VENDOR 1 FACTS:

- ▶ Card processing vendor
- ▶ Considering using them for debit and credit cards
- ▶ Annual spend approximately \$1.7M
- ▶ They will handle daily processing and fraud disputes as well as drive the ITMs/ATMs
- ▶ Real-time data transfer or batch data transfer available

VENDOR 2 FACTS:

- ▶ Collections assistance agency
- ▶ Will make collection calls if needed, assign repossessions, and assist with auction activities
- ▶ Data is shared via individual account upload to the vendor's portal
- ▶ Cost is \$250 per account plus 30% of collected funds

Vendor Risk Process

1. Create a scoring system/template ✓
2. Score vendor & based on the risk decide what steps are needed to analyze the vendor ✓
3. Review the outcome & make a risk decision
 - ▶ Full steam ahead!
 - ▶ Go, but cautiously or in limited capacity
 - ▶ Go, but put internal controls in place to supplement
 - ▶ Pause, need some additional verification
 - ▶ Run away as fast as you can

Evaluating the data

- ▶ Strategic alignment
- ▶ Credit union expertise
- ▶ Functional fit
- ▶ Financial fit
- ▶ Integration with any other existing systems (core, card processor, AML, fraud, lending, doc prep)

Evaluating the data

- ▶ Experience with credit unions of your size and complexity
- ▶ Comparison shopping
- ▶ Cost/benefit analysis
- ▶ RESULTS OF REVIEWS

Evaluating the data – Results of Reviews

- ▶ Records search
- ▶ Reference checks
- ▶ Financial
- ▶ Data/SOC
- ▶ BCP/DRP



Now make a risk
decision on this
vendor

FACTS:

- ▶ Operational units LOVE them – satisfy needs of 5 different departments, meet a strategic need
- ▶ Over 400 credit union clients; grew from 50 to 400+ in 3 years
- ▶ Five reference consultations gave positive feedback
- ▶ Price ranges in mid-risk level
- ▶ Contract
 - ▶ Missing some key protections for the credit union
 - ▶ Dynamic privacy notice
- ▶ SOC II – Company says SOC II compliant but the SOC you received is expired
- ▶ Financials
 - ▶ Over 80% of their income is from an influx of new investor capital
 - ▶ Personnel expenses increased by over \$800,000 in the past two years
 - ▶ Do not have audited financials, working on it
- ▶ BCP/DPR processes seem to be sufficient for CU needs

Homework/Project Vendor Assignment

- ▶ Small Dollar Loan Vendor
- ▶ Cost:
 - \$35,000 implementation
 - \$10,000 annual
 - \$13 per loan application
- ▶ In business 10 years, started the small dollar loan portion of business 3 years ago
- ▶ CEO former bank lender
- ▶ Company unable to produce audited financials
- ▶ New business line (small dollar loans) is supported by excess capital of existing business lines
- ▶ All data housed at CU with vendor access to core systems