



Vendor Due Diligence



Agenda snapshot

Risk
classification

Vendor due
diligence

Vendor
management

What's in store for today?

Vendor Due Diligence

Due diligence is a process related to business decisions to select, implement, and monitor third-party business relationships

- Third-party vendors are playing an increasingly important role in the credit union industry
- In some cases, direct control over one or more business functions is surrendered by the credit union
- A robust due diligence program is necessary!



When to outsource?



- When looking to reduce and control operating costs
- Improve credit union focus
- Gain access to expert capabilities
- Free-up internal resources for other purposes
- Increase efficiency
- Enhance strategy and focus on carrying out value-adding activities
- Share risks with a partner company

Frequently Outsourced Services

- Professional consulting
- Service (lending activities, payroll processing)
- Software development (customization of licensed software apps)
- Maintenance (snow removal, building maintenance)
- Construction (new and/or renovation)
- Supply (materials or goods)



Two of the most common activities in credit unions involving third-party vendors are lending and technology services

What do you think?

What are the most common issues with vendor management?

- Over-reliance on third-party vendors
- Lack of properly trained staff
- Failure to adequately monitor vendor
- Failure to set clear expectations
- No written program for due diligence



Outsourcing Social Media

- Hired third-party to monitor social media platforms
- An individual posted discriminatory comments on the CU's Facebook account that went viral over the weekend
- Many members contacted the CU expressing concerns
- CU reputation took a significant hit
- After review of why the vendor didn't address the post immediately, they found that the fine print only required vendor to perform monitoring **"during business hours between 8 AM–5 PM"**

Consideration:

When reviewing the contract, before signing, it is critical to read everything including the fine print.

The credit union should've verified that 24/7 monitoring was in place as part of the service level agreement. Or, assured that social media networks didn't allow automatic posting until review outside of monitored hours.



Risk Classification

Risk Classification



No access to member PII

No access to
credit union's network



Possible / minimal access
to member PII

Possible / minimal access
to credit union's network



Access to member PII

Access to credit union's
network

Potential to cause major
disruption

Risk Classification

| | Question | +0 | +1 | +2 | +3 | Score |
|----|--|-----|-----------------------------|-------------------------|-------------------------------------|-------|
| Q1 | Will the vendor have access to member / employee data? | No | | Yes – access to non-PII | Yes – Access to full member records | |
| Q2 | Will the vendor have access to the credit union network? | No | | Yes – limited access | Yes – full access | |
| Q3 | Will vendor interact with members? | No | Minimally | | Yes | |
| Q4 | Will member service be affected if the vendor fails to perform as agreed? | No | Minimally | | Yes | |
| Q5 | Will the outsourcing of this service be seamless to our members? | Yes | No, with minimal disruption | | No | |
| Q6 | Will the vendor be outsourcing some or all of the agreed upon services to another third party? | No | | | Yes | |
| Q7 | Is this service susceptible to frequent changes in regulations and laws? | No | | | Yes | |
| | Total | | | | | |

Risk Classification

| | Question | +0 | +1 | +2 | +3 | Score |
|----|--|-----|-----------------------------|-------------------------|--|-----------|
| Q1 | Will the vendor have access to member / employee data? | No | | Yes – access to non-PII | Yes – Access to full member / employee records | 3 |
| Q2 | Will the vendor have access to the credit union network? | No | | Yes – limited access | Yes – full access | 2 |
| Q3 | Will vendor interact with members / employees? | No | Minimally | | Yes | 3 |
| Q4 | Will member / employee service be affected if the vendor fails to perform as agreed? | No | Minimally | | Yes | 3 |
| Q5 | Will the outsourcing of this service be seamless to our members / employees? | Yes | No, with minimal disruption | | No | 3 |
| Q6 | Will the vendor be outsourcing some or all of the agreed upon services to another third party? | No | | | Yes | 0 |
| Q7 | Is this service susceptible to frequent changes in regulations and laws? | No | | | Yes | 3 |
| | Total | | | | | 17 |

Scoring Model



LOW

0-7

MODERATE

8-14

HIGH

15-21

Using a numerical classification method can help identify the risk level

The numerical classification method is just one way to identify the risk level



Vendor Due Diligence

Vendor Due Diligence by Risk Classification

| Required Docs / Review Items | Low Risk Vendor | Moderate Risk Vendor | High Risk Vendor |
|------------------------------|-----------------|----------------------|------------------|
| Ratified Contract | X | X | X |
| Proof of Insurance | X | X | X |
| Required Licenses | X | X | X |
| Ability to Perform | X | X | X |
| References | X | X | X |
| Background Check | X | X | X |
| Financial Review | | X | X |
| Audit Reports | | X | X |
| Data Security Standards | | X | X |
| Industry Affiliations | | | X |
| Organizational Structure | | | X |
| Company History | | | X |

Contract Review

Key Areas of Issue



Evergreen provisions
(auto renewal)



Indemnification



Service-Level Agreement
(performance to contract)

Evergreen provisions sample / statement



“This agreement shall have an initial term of three years from the effective date. Upon expiration of the initial period of three years, this agreement shall automatically renew for a period of one year unless written notification is received within 30 days of expiration”

Evergreen, or “Automatic Renewal,” provisions in contracts serve to keep contracts in force longer than the initial term

Indemnification



“Vendor shall defend, indemnify and hold harmless Credit Union, Officers and Employees, at the discretion of Credit Union (and their respective successors, assigns and Affiliates) from and against and in respect of any and all losses, damages, deficiencies, liabilities, assessments, judgments, costs and expenses, including attorneys fees (both those incurred in connection with the defense or prosecution of the indemnifiable claim and those incurred in connection with the enforcement of this provision) (collectively, Damages) suffered or incurred by Credit Union, its Officers or Employees which is caused by, resulting from or arising out of, related to, the nature of services provided.”

Service-Level Agreement (SLA)



Goals of a Service-Level Agreement include:

1

Provide clarity for services to be provided, accountability, roles and responsibilities

2

Present a clear, concise and measurable performance of service being provided

3

Require the vendor to comply with all relevant laws and regulations

Key Components of a Financial Review

DUE DILIGENCE

Income
statement

DUE DILIGENCE

Balance
sheet

DUE DILIGENCE

Cash flow

DUE DILIGENCE

Retained
earnings

Tax
Returns

Dunn &
Bradstreet



Business
Model

Business
Credit
Reports

Ask yourself: Would your credit union make a loan to this company?

Legal Review



- Does the third party have adequate legal and compliance programs to allow your credit union to remain compliant?
- Are there any indications of legal issues that may affect the credit union's reputation by doing business with this potential vendor?

Data Security

1 in 5

have experienced a breach of sensitive customer data from third parties²

ONLY 52%

HAVE SECURITY BASELINES OR STANDARDS IN PLACE FOR THIRD-PARTIES¹



75%

breaches involved outsiders

Data Security



PROPRIETARY
INFORMATION



MEMBER'S
PII



EMPLOYEE'S
PII



OTHER THIRD
PARTY DATA



FINANCIALLY AND
STRATEGICALLY
RELEVANT
INFORMATION

If a third-party breach occurs, this information will cause the most harm



Required evidentiary documentation

- Service Organization Control Report
- Synopsis of last independent penetration and vulnerability test
- Business Continuity Plan / Disaster Recovery Plan
- Incident Response Program
- Date and results of last disaster recovery test
- List of data breaches in the last 24/36 months

Data Security due diligence

Contract Provision

Requirement to keep systems and data secure per best practices and industry standards

Contract Provision

Confidentiality and privacy requirements

Contract Provision

Requirement to notify you of security breaches, incidents, and vulnerabilities

Contract Provision

Requirement to undergo independent penetration and vulnerability assessments

Contract Provision

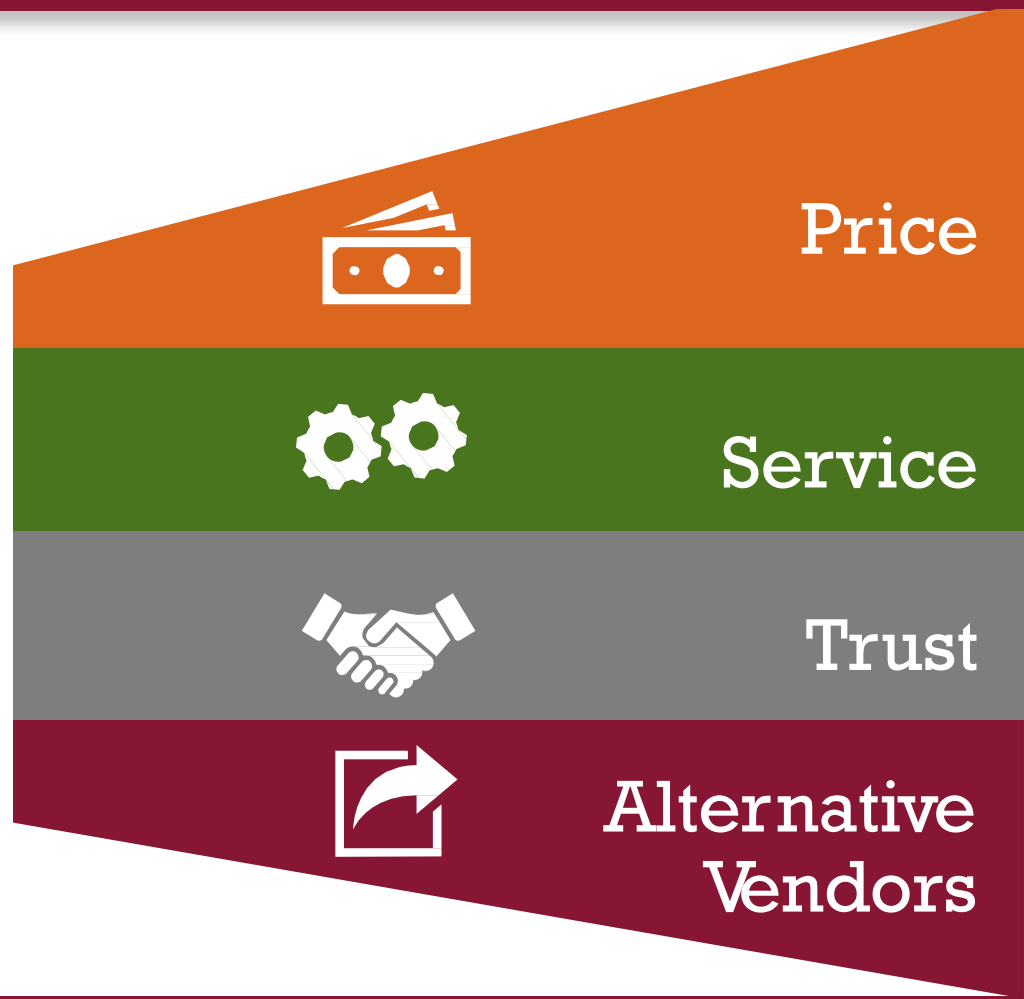
Requirement to provide you access to audit documents



Vendor Management

Evaluating Vendors

Look for a partner,
not just a vendor.



Vendor Management - Scorecard Method

- Used to measure the performance and effectiveness of vendors
- Measure the key performance indicators (KPI)
- Corresponding timeline and set of milestones that are in sync with KPI
- Use consistent and regularly-scheduled evaluations that are agreed to by both sides
- Make it easy to use in order to keep traction!

| NAME OF VENDOR | | | | | | | | | | | | | | | | | | | | | | | | |
|---|--|-------------|-------------|--------------|-------|---|-------|--------|--------------|------|------|-------|-------|-------|------|-------|-------|-------|-------|------|-------|-------|------|------|
| Description of Content and / or Services Provided | | | | | | | | | | | | | | | | | | | | | | | | |
| A brief paragraph about the vendor, their business, what services they provide, and Abbott's history with the company. | | | | | | | | | | | | | | | | | | | | | | | | |
| Another brief paragraph about the vendor relationship, including ease or difficulty of negotiations. | | | | | | | | | | | | | | | | | | | | | | | | |
| Three-Year Spend History (\$000) | | | | | | | | | | | | | | | | | | | | | | | | |
| | 2010 Act | 2011 Act | 2012 UPD | 2013 Plan | | | | | | | | | | | | | | | | | | | | |
| Total LIR Content | \$12,221 | \$12,475 | \$15,026 | \$14,696 | | | | | | | | | | | | | | | | | | | | |
| Acquisition | | | \$104 | | | | | | | | | | | | | | | | | | | | | |
| Total This Supplier | \$222 | \$202 | \$301 | \$324 | | | | | | | | | | | | | | | | | | | | |
| % of LIR Content | 1.8% | 1.6% | 2.0% | 2.2% | | | | | | | | | | | | | | | | | | | | |
| YOY Trend | 25% | -9% | 49% | | | | | | | | | | | | | | | | | | | | | |
| LIR Allocation Methodology / Top Users | | | | | | | | | | | | | | | | | | | | | | | | |
| Statement of how this vendor cost is allocated to Abbott divisions. | | | | | | | | | | | | | | | | | | | | | | | | |
| Statement of which divisions use this vendor content. | | | | | | | | | | | | | | | | | | | | | | | | |
| Statement of what usage statistics are available from the vendor and in what timeframe. | | | | | | | | | | | | | | | | | | | | | | | | |
| Current Contract Terms & Conditions | | | | | | | | | | | | | | | | | | | | | | | | |
| License expires MMDD/YYYY. | | | | | | | | | | | | | | | | | | | | | | | | |
| Statement of what the vendor pricing is based on (e.g. number of sites, R&D headcount, set global price) | | | | | | | | | | | | | | | | | | | | | | | | |
| Statement about whether the vendor accepted Abbott's license terms. | | | | | | | | | | | | | | | | | | | | | | | | |
| Billing Frequency | | | | | | | | | | | | | | | | | | | | | | | | |
| Statement about how often Abbott is billed (e.g. annually, quarterly, monthly) and during what timeframe (e.g. beginning of the quarter). | | | | | | | | | | | | | | | | | | | | | | | | |
| Products (\$000) / Competitive Landscape and Supplier Pricing Models | | | | | | | | | | | | | | | | | | | | | | | | |
| | Product Name | 2012 UPD | Sole | Comp | Other | Pricing Models | | | | | | | | | | | | | | | | | | |
| 1) | Name of first product with optional brief description | \$301 | | X | | Description of pricing model for that product | | | | | | | | | | | | | | | | | | |
| 2) | Name of second product with optional brief description | \$0 | | X | | Description of pricing model for that product | | | | | | | | | | | | | | | | | | |
| Contract Price Increase Trending | | | | | | | | | | | | | | | | | | | | | | | | |
| YOY Trend vs. Industry Average | | | | | | | | | | | | | | | | | | | | | | | | |
| <table border="1"> <caption>YOY Trend vs. Industry Average Data</caption> <thead> <tr> <th>Year</th> <th>Inflation</th> <th>Other</th> <th>Volume</th> <th>Industry Ave</th> </tr> </thead> <tbody> <tr> <td>2010</td> <td>2.5%</td> <td>10.0%</td> <td>12.0%</td> <td>12.0%</td> </tr> <tr> <td>2011</td> <td>-0.1%</td> <td>-8.0%</td> <td>-9.0%</td> <td>-9.0%</td> </tr> <tr> <td>2012</td> <td>15.0%</td> <td>32.0%</td> <td>2.0%</td> <td>2.0%</td> </tr> </tbody> </table> | | | | | Year | Inflation | Other | Volume | Industry Ave | 2010 | 2.5% | 10.0% | 12.0% | 12.0% | 2011 | -0.1% | -8.0% | -9.0% | -9.0% | 2012 | 15.0% | 32.0% | 2.0% | 2.0% |
| Year | Inflation | Other | Volume | Industry Ave | | | | | | | | | | | | | | | | | | | | |
| 2010 | 2.5% | 10.0% | 12.0% | 12.0% | | | | | | | | | | | | | | | | | | | | |
| 2011 | -0.1% | -8.0% | -9.0% | -9.0% | | | | | | | | | | | | | | | | | | | | |
| 2012 | 15.0% | 32.0% | 2.0% | 2.0% | | | | | | | | | | | | | | | | | | | | |
| Pricing Trend / Other Comments | | | | | | | | | | | | | | | | | | | | | | | | |
| 2010 - Comments about any notable pricing trend for this year, such as one-time purchases which may have impacted fees for one year or packages purchased which reduced overall spend. | | | | | | | | | | | | | | | | | | | | | | | | |
| 2011 - Comments about any notable pricing trend for this year, such as one-time purchases which may have impacted fees for one year or packages purchased which reduced overall spend. | | | | | | | | | | | | | | | | | | | | | | | | |
| 2012 - Comments about any notable pricing trend for this year, such as one-time purchases which may have impacted fees for one year or packages purchased which reduced overall spend. | | | | | | | | | | | | | | | | | | | | | | | | |
| Historic Inflation Rates / Abbott Headcount | | | | | | | | | | | | | | | | | | | | | | | | |
| | 2010 | 2011 | 2012 | | | | | | | | | | | | | | | | | | | | | |
| Abbott | X.X% | X.X% | X.X% | | | | | | | | | | | | | | | | | | | | | |
| CPI (past year's average) | 3.7% | 3.2% | 3.4% | | | | | | | | | | | | | | | | | | | | | |
| Journal Publishers | 10.0% | 8.0% | 5.0% | | | | | | | | | | | | | | | | | | | | | |
| Outsell | 8.0% | 5.0% | 5.7% | | | | | | | | | | | | | | | | | | | | | |
| Industry Average | 9.0% | 6.5% | 5.4% | | | | | | | | | | | | | | | | | | | | | |
| Abbott HC +/- | X.X% | X.X% | X.X% | | | | | | | | | | | | | | | | | | | | | |
| Abbott R&D HC +/- | X.X% | X.X% | X.X% | | | | | | | | | | | | | | | | | | | | | |
| (Rev MMDD/YY) | | | | | | | | | | | | | | | | | | | | | | | | |

Have a back-up plan
Long before the contract matures



Annual Due Diligence / Managing the Relationship

Perform to
Contract /
SLA

Insurance

Litigation

Financials

Audits

10 Vendor Due Diligence Checkpoints

1

Risk
Classification

2

Financial
Review

3

Legal Issues

4

Evergreen
Clause

5

Indemnification

6

SLA
(performance
to contract)

7

Information
Security / Data
Management

8

Tracking
Methods -
Scorecards

9

Alternatives

10

Annual Due
Diligence

Looking for additional assistance



CUNA Mutual Group
**Risk & Protection
Response Center**

800.637.2676

Select you're a credit union, then choose option 4

riskconsultant@cunamutual.com

[Ask a Risk Manager](#) interactive form


Stay on top of emerging risks

- RISK Alerts – **Warning** ♦ **Watch** ♦ **Awareness**
- Loss Prevention Library (whitepapers, checklists)
- Webinars & Education
- Risk Assessments
- Peer Data

Protection Resource Center @ www.cunamutual.com

RISK Alert

ACTIONABLE INSIGHTS FOR BOND POLICYHOLDERS.




Alert Type: Awareness | **Watch** | Warning

Mitigate Emerging Risks Related To Cash Advances

While stolen card data has continued to wreak havoc on gross fraud losses, the primary method used by fraudsters has been isolated to point-of-sale and ATM terminals. Recently, however, reported credit union losses suggest a shift to in-branch cash advance machines.

[Read Full Alert](#)
User ID and Password required


[Download PDF >](#)
File is available for 30 days.



Protection Resource Center
Access risk management resources to identify and manage credit union risks including access to the full RISK Alert Library.

[Learn More >](#)

© CUNA Mutual Group
PO Box 391 | 5910 Mineral Point Road
Madison, WI 53701-0391
608.238.5851 | 800.356.2644 | www.cunamutual.com



If this email was forwarded to you from a colleague, [find instructions](#) on requesting access to the Protection Resource Center.

If you received this message in error or wish to decline further emails on this subject, [unsubscribe](#) from CU Protection Resource Center.

You can also manage all your CUNA Mutual Group email subscriptions [here](#).



CUNA MUTUAL GROUP

This presentation was created by the CUNA Mutual Group based on our experience in the credit union and insurance market. It is intended to be used only as a guide, not as legal advice. Any examples provided have been simplified to give you an overview of the importance of selecting appropriate coverage limits, insuring-to-value and implementing loss prevention techniques. No coverage is provided by this presentation/ publication, nor does it replace any provisions of any insurance policy or bond.

CUNA Mutual Group is the marketing name for CUNA Mutual Holding Company, a mutual insurance holding company, its subsidiaries and affiliates. Insurance products offered to financial institutions and their affiliates are underwritten by CUMIS Insurance Society, Inc. or CUMIS Specialty Insurance Company, members of the CUNA Mutual Group. Some coverages may not be available in all states. If a coverage is not available from one of our member companies, CUNA Mutual Insurance Agency, Inc., our insurance producer affiliate, may assist us in placing coverage with other insurance carriers in order to serve our customers' needs. For example, the Workers' Compensation Policy is underwritten by non-affiliated admitted carriers. CUMIS Specialty Insurance Company, our excess and surplus lines carrier, underwrites coverages that are not available in the admitted market. Data breach services are offered by Kroll, a member of the Altegrity family of businesses. Cyber liability may be underwritten by Beazley Insurance Group.

This summary is not a contract and no coverage is provided by this publication, nor does it replace any provisions of any insurance policy or bond. Please read the actual policy for specific coverage, terms, conditions, and exclusions.

10007678-0518 © CUNA Mutual Group 2018 All Rights Reserved.



www.cunamutual.com