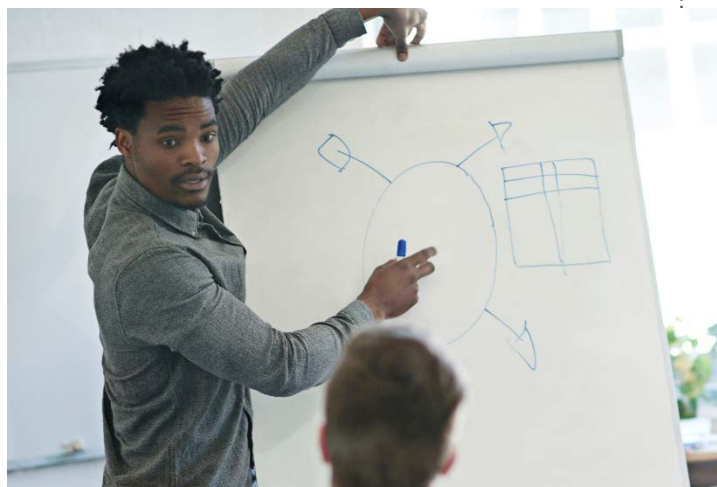


Vendor Due Diligence

Organizations today are not simply comprised of one internal team. Credit unions, small and large alike, collaborate with partners, vendors, and other third parties.

While you can outsource the service; remember, you still own the responsibility of this critical business practice.



Navigating Vendor Relationships

It's inevitable that credit unions will work with vendors or third-party providers to deliver various products and services to their members. Third-party vendors play an important role as you strive to become more competitive and expand member services. But, partnering with these vendors doesn't come without risk. Managing risks associated with these relationships is a critical aspect to maintaining a successful operation.

Your decision to outsource a product or service should be dependent on a risk / reward, including cost benefit, analysis. Before you begin the vendor selection process, it's important to determine if outsourcing is the right decision for your credit union.

If your risk / reward analysis points to outsourcing, consider classifying the product or services that you are looking to outsource. There are a few methods you can use – numerical designations or a high-medium-low scale. Classifying the risks allows you to rank the importance of the product or service, and in turn, determine the level of initial and ongoing due diligence necessary to maintain the relationship.

These activities should happen independent of the actual request for proposal and vendor selection process; and, instead are intended to help identify the level of risk associated with outsourcing an activity.

Credit unions should establish processes to evaluate and manage associated risks before entering, during, and even after the vendor relationship ends.

Remember, third-party and vendor risk management is an ongoing process. The initial data and information only provides you with a snapshot in time.

Vendor risk management can seem like a daunting task.

Following these vendor risk management best practices can be a great first step:

- **Risk / Reward Analysis** – develop a thorough understanding of what the proposed will and won't accomplish for the credit union.
- **Vendor Classification** - substantiate and document the rationale behind what third parties are selected for closer analysis. Review the classification example using a numerical scale.
- **Vendor Due Diligence** – gather information to prevent surprises down the road.

For additional insights, contact
CUNA Mutual Group Risk Consultants at
800.637.2676 or **riskconsultant@cunamutual.com**

A risk / reward analysis can help determine the desirability of entering a relationship with a third party. It's important to consider both short-term, long-term costs, and risks along with benefits associated with outsourcing the function.



Key Questions to Ask When Assessing Vendors

In today's complex business environment, vendors play a key role in your success. However, relying on vendors can also introduce added risk, and managing these relationships is important. It is key for management to develop a thorough understanding of what the proposed relationship will accomplish for the credit union, and why the use of a third party is in your best interests.

A risk / reward analysis, including a cost-benefit analysis, should be performed for significant matters, comparing the proposed third-party relationship to other methods of performing the activity or product offering, including the use of other vendors or performing the function in-house.

Use these key questions to assist in your risk / reward analysis:

- Is the proposed vendor relationship consistent with the credit union's strategic plan and overall business strategy?
- Does the credit union have the ability to provide adequate oversight and management of the proposed third-party relationship on an ongoing basis?
- Do we currently have someone on staff that can or already does perform this service?
- What is the cost of hiring and training someone vs. the cost of outsourcing the service / work?
- Does outsourcing the service offer benefits that could not be realized by keeping the service in house? For example, increase member base, increase loans, etc.
- Who will benefit from the outsourcing of this service? Credit union, member, or both?
- Are there additional anticipated costs associated with the ongoing management of the relationship? For example, network / infrastructure upgrades, licensing fees, etc.
- Does outsourcing introduce additional legal, regulatory and social ramifications that would not exist if the function was performed in-house?
- What operational or reputational risks could be introduced with this particular vendor relationship?

Carefully estimate the long-term financial effect of the proposed third-party relationship, including taking into account all aspects of the long-term potential of the relationship, as well as the managerial expertise and other associated costs that would result from the decision to use a third party.

Remember, it is critical that you are not solely influenced by short-term cost savings.

Interested in learning more about Vendor Due Diligence and related risks?

Contact CUNA Mutual Group Risk Consultants at 800.637.2676 or riskconsultant@cunamutual.com

Vendor Classification

When outsourcing services, the criticality of the service should be classified. Using numerical classification method (shown below) can identify the risk level of outsourcing services. “Low” risk suppliers typically can be moved to the approval process with no further action, to be re-evaluated when conditions change. “Medium” or “high” risk third parties generally qualify for an additional due diligence deep-dive to provide more detailed analysis of the risks identified. By having a clear process, you can substantiate and document the rationale behind what third parties are selected for closer analysis.

Answer each question with only one response and related score per row. Enter the points in the last column and tally the scores after completing all questions. Total scores falling within **0-7 points are considered Low; 8-14 Moderate; and 15-21 High.**

| | 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 | | | | | |

Example: a credit union looking to outsource custodial services may fill out the classification table as follows: Q1-No (0); Q2-No (0); Q3-Minimally (+1); Q4-Minimally (+1); Q5-Yes (0); Q6-No (0); Q7-No (0). By tabulating the scores, the vendor classification is 2 which falls within the low classification.

Risk levels are not static, as the business, security or financial practices of your third parties may evolve at anytime. You are responsible for detecting when a third party moves within the classifications.

Interested in learning more about Vendor Due Diligence and related risks?

Contact CUNA Mutual Group Risk Consultants at 800.637.2676 or riskconsultant@cunamutual.com

Vendor Due Diligence

After performing a risk / reward analysis, including a cost-benefit analysis, you will need to perform due diligence on potential vendors, commensurate with the level of risk associated with the relationship. For example, due diligence performed on an outsourced service that will not have access to the credit union network, not have access to member personal identifying information (PII), and not heavily regulated will not be as deep as the due diligence performed if it has network access and is heavily regulated.

When performing due diligence, it is imperative to dig deep and gather as much information about vendors so you can make apple-to-apple comparisons in the decision-making process. Insurance, licensing, financials, litigation, previous audits, security standards and references are some of the things that need to be reviewed prior to reaching an agreement and signing a contract with a specific vendor. The bottom line is that you want to gather as much information to prevent surprises down the road that could have been learned previously.

NEWLY CONSIDERED THIRD-PARTY / VENDOR

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

Additionally, remember that the level of initial due diligence performed on a vendor may vary from that of the ongoing due diligence. The ongoing due diligence to manage the relationship will consist of getting some updates on information reviewed in the initial due diligence such as insurance (to ensure it hasn't expired, and limits haven't changed), litigation, audits etc. The most important thing that will be done during ongoing due diligence - that was not part of the initial due diligence - is to determine if the vendor performed to contract.

Interested in learning more about Vendor Due Diligence and related risks?

Contact CUNA Mutual Group Risk Consultants at 800.637.2676 or riskconsultant@cunamutual.com

ONGOING VENDOR MANAGEMENT

| Required Docs / Review Items | Low Risk Vendor | Moderate Risk Vendor | High Risk Vendor |
|----------------------------------|-----------------|----------------------|------------------|
| Proof of Insurance | × | × | × |
| Required Licenses | × | × | × |
| Performance to Contract | × | × | × |
| Legal Check | | × | × |
| Financial Review | | × | × |
| Audit Reports | | × | × |
| Data Security Issues (Breaches) | | × | × |
| Organizational Structure Changes | | | × |

KEY TERMINOLOGY

Ratified Contract: Outlines performance expectations, roles and responsibilities, indemnification, liability limits, insurance requirements, term length, exit clauses, pricing, etc. Contracts should be created by an attorney on behalf of your credit union, or at least reviewed by a qualified attorney on your behalf. Access the [Contract Provision Checklist](#) for additional details on information to be included in contracts.

Proof of Insurance: Active, valid and adequate insurance limits are in place. The type of service or product being purchased will dictate the type of insurance coverages required (i.e. document transportation services should have adequate auto or truck insurance in place).

Background Check: Background review on the vendor and its principal's partners and executives can help to prevent. This analysis could include a review of prior criminal offenses, insurance claims, internet presence and other lawsuits or legal history.

Financial Review: Consider including a review of the third parties Dun & Bradstreet Report or Business Credit Report, especially if financial statements are not available. Ask yourself, would we make a loan to this vendor?

Data Security Standards: Take necessary steps to understand the vendors data security standards. When applicable, contractually require adequate protection of member information and review appropriate security documents to ensure compliance.

Risk & Compliance Solutions • 800.637.2676 • riskconsultant@cunamutual.com

This resource is for informational purposes only. It does not constitute legal advice. Please consult your legal advisors regarding this or any other legal issues relating to your credit union. 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. CUNA Mutual Group Proprietary and Confidential. Further Reproduction, Adaptation or Distribution Prohibited.