Vendor Management

A Primer to Performing Effective Vendor Due Diligence

Authored by: Jim Vilker, NCCO, VP of Professional Services, CU*Answers

CU*ANSWERS
A Credit Union Service Organization

AuditLink

CONTENTS

LEGAL DISCLAIMER

VENDOR MANAGEMENT

A PRIMER TO PERFORMING EFFECTIVE VENDOR DUE DILIGENCE

Today, every credit union relies on more allies, partners, and vendors than ever before. It's a networked world and keeping track of just the names of all the players who contribute to your credit union's success can be challenging, let alone the key data and information you need to defend them during increasingly complex vendor due diligence audits.

To help with this task, AuditLink has combined its compliance service experts with Trust Exchange's industry-leading platform to offer credit unions a complete vendor management package.

This document will detail the ways in which AuditLink categorizes and assesses each vendor, and to serve as a white paper on sound methodology for public consumption.

THE ASSESSMENT PROCESS

Determining the criticality of specific relationships or vendors is one of the most vital components of a strong vendor management program. The OCC, FDIC, and FFIEC have a number of guidance letters regarding criticality and the underlying theme for them all is the control of reputation risk, financial risk, and compliance risk for the credit union. These letters have served as a basis for emerging and changing regulatory requirements from both the NCUA and state regulatory bodies. These risks are not independent of each other and many times failure of a specific vendor or relationship could have an impact on all three. In the example of AuditLink's work with Frankenmuth Credit Union, when assessing the risk of each vendor the following variables are taken into consideration:

1	• Extent to which the vendor has access to non-public member information • Extent to which the vendor stores non-public member information
2	• Extent to which the vendor has access to the credit union's physical location
3	• Extent to which the vendor has access to the credit union's IT infrastructure
4	• Extent to which the service provided by the vendor is intolerant (disaster recovery/business resumption) to the disruption of member services • Extent to which the service provided is vital to the organization and financially woven into the strategies of the organization

Each vendor is evaluated in accordance with the above variables and based upon this evaluation is assigned a tier level appropriate for the ongoing monitoring and continued due diligence of the vendor.

1. GLBA AND VENDOR MANAGEMENT

Assessing the extent to which a vendor has access to, stores, or transmits member information is the most vital component of any vendor management program. This area of risk management is governed by GLBA and poses one of the most significant compliance and reputations risks facing a credit union. Complying with this rule is very well described by the Federal Trade Commission on their website[1]. The Safeguards Rule transcends throughout all financial institution areas of operation with vendor management being one of the most important in maintaining compliance and mitigating risk.

When assessing a vendor relative to member information it is vital that the organization inventory the amount of member information that vendor has access to, transmits, or stores with a sound knowledge of what information is protected by regulation and which is not. If non-public information is shared the type and amount will then be utilized in categorizing the criticality of the vendor. The spectrum is as broad as sending a marketing firm a member name and address to the transmission of credit card information containing account numbers and PANs.

In the case of working with Frankenmuth, the credit union and AuditLink have built a strong risk-based platform and process for completing this component of the assessment process with a deep knowledge of the Safeguards Rule. It entails evaluating the amount and type of information shared with vendors and identifies the level of risk posed by each relationship. Based upon those findings the vendor is categorized and assigned a tier rating.

Tiers dictate the level of ongoing due diligence, required exchange of information, and monitoring of important events related to the specific vendor. Vendors are granted access to the platform to upload information, and a fully automated system alerts vendors when an item is due and alerts the credit union/AuditLink team when an item is past due.

2. ACCESS TO PHYSICAL LOCATION

Determining the criticality of a vendor who has access to the credit union's physical location is another variable that plays a crucial role in the assessment process. A number of risks come into play including:

- Theft of non-public member information
- Gaining access to the credit union's internal network
- Theft of corporate secrets and money
- Security of the property upon exiting

Not unlike the first variable, vendors that fall under this area must be carefully reviewed and gauged against the internal security requirements of the credit union. For example, it may be the practice of the credit union to have maintenance personnel perform their duties only during credit union hours and never in an area where they are unsupervised. In this case the assessment would categorize this vendor as a low probable risk and assign them to a lower tier (requiring a lesser amount of due diligence). Take the same vendor in another credit union that allows access to the facility at all hours, performs duties unsupervised,

[1] https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying

and/or has access to the credit union's security system. Again, this is as broad of a spectrum as you could find but is necessary to evaluate in the thought process and assessment.

Another consideration to take into account is the credit union's own internal security policies. Is the credit union diligent about maintaining clean work areas and keeping documents containing non-public information under lock and key? Does the credit union have a policy of locking PCs when staff walk away from their workstations and keeping monitors out of public view? These types of protocols must be taken into consideration while evaluating the criticality as vendors do frequently have access to areas that are not open to the public and exposure of this type increases the risks listed above.

3. ACCESS TO IT INFRASTRUCTURE

The third variable in assessing criticality revolves around any vendor that has connections to the credit union's network. To complete this assessment it is wise to have a network diagram describing the topography of connections. Of primary concern are those vendors who have administrative authority (service providers) and those whose connections penetrate the credit union's firewall(s). Generally speaking these vendors have been hired to assist in the running of the network and keeping it patched.

On the other side of the spectrum would be a vendor that has access to the network but lives in the DMZ. An example would be the dreaded HVAC vendor who monitors the credit union from a remote location. Security systems would also be a good example of this.

Regardless of how the vendor is connected to the network each one must be evaluated relative to the total topography. It is important to understand that once they are on the network they may have the capability to scan for vulnerabilities or worse if their network has been compromised and they are being used as a vector from other bad actors.

Like physical security, the credit union's internal IT expertise and security policies come into play. Credit unions that have locked down their firewalls, are diligent applying patches, and consider all connections to the network with a cyber security mindset are less likely to be compromised from a vendor having access to their networks.

The credit union and AuditLink Vendor Management have built a strong platform and process for completing this component of the assessment process with a strong technical knowledge to ask the right questions and guide non-technical people through this assessment. Based upon those findings the vendor is categorized and assigned a tier rating. Tiers dictate the level of ongoing due diligence, required exchange of information, and monitoring of important events related to the specific vendor.

4. INTOLERANCE TO DISRUPTION OF SERVICE OR PRODUCT

Consider the difference between a vendor that provides the credit union with paper products versus one that provides hundreds of loan applications through an indirect dealer network. Several considerations come to mind including:

- Number of members impacted
- Balance sheet and income statement implications
- Difficulty replacing the vendor in a short amount of time
- Disruption in the strategic plans and goals of the credit union
- Member facing intolerance and reputational risks
- Potential legal liability relative to loss of service
- Implications on the disaster recovery/business resumption plans

Vendors who are deeply woven into the fabric of the credit union's operations must be managed at a much higher level and the amount of due diligence increases based upon depth of their involvement with the credit union and its member services. This would generally include increasing the due diligence requirements including the review of disaster recovery testing results.

These vendors are typically easy to spot and always include the credit union's data processor, debit/credit/ATM provider, indirect lending channels such as Route One and DealerTrak, and corporate credit unions. The assessment and amount of ongoing due diligence depends upon the credit union's ability to replace these vendors in a reasonable amount of time.

CATEGORIZING VENDORS

After evaluating vendors on how they interact with and impact the credit union, the final step of the assessment process is to categorize them using a risk-based approach. The categorization is used to determine the level of ongoing due diligence that must continuously be performed by the credit union and AuditLink staff. Five tier levels were developed and vendors are assigned a level where Tier I would require the largest amount of due diligence and monitoring and Tier V requiring the least.

Listed below are the descriptions of each tier and the required due diligence to monitor.

TIER I

Tier I vendors pose the highest degree of risk and require the largest degree of ongoing due diligence. Vendors that fall under this tier generally meet one or more of the following criteria:

1. Have access to, transmit, or store a large amount of non-public member data;
2. The service provided has a high degree of activity which is visible to members;
3. Would have a significant impact on income and expense statement in the event of its dissolution or contract termination;
4. Would be difficult to replace in a reasonable period of time while seriously disrupting member service;
5. Have high level access to credit union's IT infrastructure behind the firewalls where corporate secrets and member information reside;
6. Have access to the credit union's facilities in an unescorted manner and in doing so may also have access to member data;
7. Owned CUSOs requiring oversite in accordance with NCUA guidelines.

Tier I vendors have the highest level of due diligence on the vendor management system. Based upon categorization will require some or all of the following events tracked:

- News feeds
- Annual or audited financial statements (or quarterly financials if it is an owned CUSO)
- Publicly available control audit
- Insurance/bond
- Internal network infrastructure audit or penetration test
- Disaster recovery/business resumption policies and annual testing

TIER II

Public Companies that provide a service technical in nature that may house member data, such as FISERV

There is very little difference between Tier I and Tier II vendors. The biggest difference is that these companies are generally found in the Fortune 500. These companies do have a higher amount of access to member data and can be deeply woven into the credit union's service offerings and income statement. They may be difficult to replace quickly, and could have a high degree of member related activity visible to members. A Tier II company may also have a significant impact on income and expense statements.

Tier II vendors do pose a high level of risk and based upon this categorization will require some or all of the following on-going due diligence

Tracked Events:

- News feeds
- Annual report or financial statements
- Control audit
- Insurance if warranted

TIER III

Financial servicing companies

Tier III vendors generally will have some degree of access to non-public member data, they are not as difficult to replace quickly, and have no access to the credit union's network or physical locations. Typical vendors that fall into this category would be private mortgage and credit life and disability providers.

Tracked Events:

- News feeds
- Annual report or audited financial statements
- Publicly available control audit
- Insurance

TIER IV

These vendors would consist of public companies that could be viewed as vital to the community infrastructure. If a company of this type were to fail it would have regional catastrophic effects. Companies that fall into this category generally are the public utilities. These companies are considered critical, however the failure of these types of companies is highly unlikely as they are vital for the community or region to survive. Contingency and disaster recovery plans or more important in this case to manage the impact of their failure vs. the management of the vendor relationship. Examples of these type of companies would include DTE Energy or Consumers Energy.

Tracked Events:

- News feeds
- Annual report

TIER V

Companies that fall into this tier may come into contact with member data or have physical access to the facility. Generally these companies would have very little direct access to information, can be replaced very quickly, and would have little if any impact on the ongoing business operations of the credit union if they fail.

Tracked Events:

- News feeds
- Insurance

TRACKED EVENTS SUMMARY

	TIER				
TRACKED EVENTS:	I	II	III	IV	V
New feeds	✓	✓	✓	✓	✓
Annual or audited financial statements (or quarterly financials if it is an owned CUSO)	✓	✓	✓	✓	
Publicly available control audit	✓	✓	✓		
Insurance/bond	✓	✓	✓		✓
Internal network infrastructure audit or penetration test	✓				
Disaster recovery/business resumption policies and annual testing	✓				