Vendor Risk Management (VRM), How Much Is Enough?

Purpose: This paper discusses which vendor relationships should be included in an institution's vendor oversight program and to what level they should be reviewed. Only the vendor oversight component of VRM, not vendor selection or pre contract due diligence, is discussed.

Intended Audience: Any staff member having responsibility for developing or managing a financial institution's vendor oversight program, based on guidance from the Federal Financial Institution Examination Council (FFIEC).

Guidance

VRM programs run the gamut from the collection of a few documents to advanced risk management software tools. What is appropriate for your institution? This discussion will review some of the guidance provided by the FFIEC. Specifically, we will review an excerpt from the FDIC FIL 44-2008:

"Institutions should maintain adequate oversight of third-party activities and adequate quality control over those products and services provided through third-party arrangements in order to minimize exposure to potential significant financial loss, reputation damage, and supervisory action. The board should initially approve, oversee, and review at least annually ***significant*** *third-party arrangements, and review these arrangements and written agreements whenever there is a material change to the program. Management should periodically review the third party's operations in order to verify that they are consistent with the terms of the written agreement and that risks are being controlled. The institution's compliance management system should ensure continuing compliance with applicable federal and state laws, rules, and regulations, as well as internal policies and procedures. Management should allocate sufficient qualified staff to monitor significant third-party relationships and provide the necessary oversight. Management should consider designating a specific officer to coordinate the oversight activities with respect to significant relationships, and involve their compliance management function and, as necessary, involve other operational areas such as audit and information technology, in the monitoring process. The extent of oversight of a particular third-party relationship will depend upon the potential risks and the scope and magnitude of the arrangement. An oversight program will generally include monitoring of the third party's quality of service, risk management practices, financial condition, and applicable controls and reports. Results of oversight activities for* ***material*** *third-party arrangements should be periodically reported to the financial institution's board of directors or designated committee. Identified weaknesses should be documented and promptly addressed."*[1]

[1] FDIC FIL 44-2008

As can be seen, the guidance contains phrases like “adequate quality” and “material change” in their discussions regarding vendor oversight. These terms are not defined by the FFIEC which means it is the responsibility of the financial institution to define them. Of course, if they are not properly defined by the institution, the examiner is likely to point this out. The guidance requires financial institutions to only track those vendor relationships that are deemed to be significant or material. What do the terms significant and material mean? These terms were highlighted above by the author to point out the confusion in the naming convention. Was the intent for these terms to be interchangeable, or do they have different meanings? It is not totally clear. While the author believes that these terms should have different meaning, for the purpose of this paper, he will assume that the FDIC intended to use the term *significant* in both instances. Given this assumption, how does the institution determine which relationship is significant? Consider another excerpt from the same FIL that states:

“A third-party relationship should be considered significant if the institution's relationship with the third party is a new relationship or involves implementing new bank activities; the relationship has a material effect on the institution's revenues or expenses; the third party performs critical functions; the third party stores, accesses, transmits, or performs transactions on sensitive customer information; the third party markets bank products or services; the third party provides a product or performs a service involving subprime lending or card payment transactions; or the third party poses risks that could significantly affect earnings or capital.“ [2]

The first description of “*new relationship or new bank activity*” implies evaluation of new relationships or activities to determine whether they will require ongoing oversight. Certainly, not every relationship or activity will meet this requirement. The determination of which relationships do is accomplished through the same process as any other, by determining its inherent risk to the institution. As the inherent risk increases, so should the frequency and the depth of due diligence. There are typically three levels of inherent risk: Critical, Material, and Minor. The names and the number of levels may vary but the concept does not change. Critical level relationships have the most inherent risk. These relationships should have due diligence conducted no less than once per year. Material relationships may require due diligence every other year and Minor every third year. Using this methodology, the institution invests the appropriate amount of time focused on vendor relationships pursuant to their level of inherent risk. How is the level of inherent risk determined?

The answer to this question may be found within the FIL’s definitions. The three key elements of inherent risk in vendor relationships are: financial loss, loss of customer information, and time needed to replace a vendor should the need arise.

[2] FDIC FIL 44-2008

Multiple items fall into the financial loss category, namely, *"the relationship has a material effect on the institution's revenues or expenses; the third party performs critical functions; the third party provides a product or performs a service involving subprime lending or card payment transactions; or the third party poses risks that could significantly affect earnings or capital."* Financial loss can be determined by answering the following question:

1. **In the event of a vendor outage or a compromise causing an outage, how quickly would the institution need to recover before facing significant financial losses?**

The assumption here is that the loss of vendors providing any of the aforementioned functions would negatively impact the institution's revenues or expenses within a short period of time.

The next item noted, *"the third party stores, accesses, transmits, or performs transactions on sensitive customer information",* may be addressed by the following question:

2. **Does this relationship require the vendor's access to sensitive customer information?**

An additional item that correlates with question # 1 above regards the time required to replace a relationship, should it become necessary to do so. This is vital if the institution is suffering financial loss while the service is not available. One final question linking the determination of close monitoring of relationships is:

3. **How long would it take to replace this service in the event of the vendor's inability to perform?**

These three questions might be utilized as shown in Figure 1:

How quickly would the Institution need to recover this service before facing significant losses?

O Less than 48 Hrs

O Up to 1 Week

O Greater than 1 Week

Does the product/vendor have access to sensitive customer information?

O Definitely has access

O Has potential access

O Has no access

How quickly could a suitable replacement for this product/vendor be identified, selected, and implemented should the need arise?

O 6 months or more

O 3 to 6 months

O 1 to 3 months

O Less than 1 month

Figure 1

Each answer would be associated with a value that represents its level of criticality. Different combinations of responses would yield a *Critical, Material*, or *Minor* inherent risk. This process is called vendor ranking. These questions, and possible responses, may vary slightly from institution to institution depending on their views and requirements. However, in general, these crucial questions will suffice in most cases. The author's opinion is that the relationships which require oversight based on the FDIC FIL 44-2008, are those ranked as *Critical* and *Material* pursuant to the questions and assumptions above. **Institutions should validate this opinion with their respective auditors and examiners**.

In all known instances of this process being utilized, over 120, there is no documented instance of dissatisfaction from any member of the FFIEC. Indeed, the FFIEC appears to be trending toward inclusion of *Minor* relationships in the oversight process based on financial institution feedback received after examination.

Once the ranking is determined, it should be mapped to the institution's Vendor Risk Management Policy in order to determine the frequency, depth, and breadth of the due diligence required. The policy should include, for example, *"those relationships determined to be ranked as Critical, shall be assessed on an annual basis. The assessment shall include completion of the institutions standard Critical ranking due diligence questionnaire in addition to the acquisition and review of the vendor's financials, security review, certificate of insurance, credit rating, and performance metrics."* The policy would also list the requirements for a ranking of Material and Minor which would be subsets of that required for a ranking of *Critical*.

The *Critical* ranking questionnaire might include the following topics:

- Product/Service Description
- General Contract Review
- Financial Review
- Information Security Analysis
- Contract Term and Termination Review
- Physical Security Review
- Software Security Review
- Customer Data Access
- Performance Review

Each section of the questionnaire would contain the questions necessary to determine compliance to the institution's particular requirements and FFIEC's guidelines. Some questions may be answered by the vendor, while others can only be answered accurately by the institution itself. Both responses and supplied documentation should then be reviewed by a third party within the institution. Ultimately, this review should lead to a determination of risk exposure in the aggregate, as well as by risk category. Commonly tracked risk categories include: *Strategic, Credit, Compliance, Operational, Transactional, Reputational*, and *Country*. Since the institution's policy would require less depth of due diligence for material relationships, some questions, and possibly complete sections, would be eliminated from this process.

Common assessment frequencies are every 12 months for *Critical* ranking, every 24 months for *Material* ranking, and every 36 months for a *Minor* ranking.

An obvious question at this juncture is, "Which vendors should be included into the VRM?" Any vendor with whom there is a contract in place or there should be a contract in place. If there is no contract, either it was neglected or a determination has already been made that this relationships poses no risk to the institution.

One key element of a successful, vendor oversight program is the ability to track, report, and proactively notify stakeholders of contract related events. Examples include: contract end-dates, auto renewal dates, anniversary dates, and dates of negotiated price changes. This capability brings the oversight of *Minor* vendors into the program.

Minor relationships pose virtually no risk to the institution based on the criteria above. However, it is helpful to be proactively notified in the event of an approaching contract expiration or renewal. The institution may deem it useful to also perform due diligence on the *Minor*-ranked relationship, even though it may be as simple as tracking the existence of a Non-Disclosure Agreement, or acknowledging that the relationship exists. As a result, the institution is showing that they are on top of their vendor oversight program in the eyes of auditors and examiners. In addition, this approach prevents the institution from overlooking those vendors that began the relationship as *Minor*, but have changed ranking category due to an increase in their product or service offering to the institution.

An undocumented factor that has an impact on the level of due diligence is the size of the institution. Exactly how does the size of the institution affect the due diligence? When examiners review an institution, they are not only viewing the risk posed to the institution; they are also considering the financial services industry as a whole. The result is that they appear to be more lenient toward smaller institutions, due to the fact that if the institution were to have a catastrophe, the industry at large is not in jeopardy of failure. The abovementioned is the author's opinion based on personal experience and observation. Each institution's examiners and auditors will vary in this area. Care should be taken to understand their views and approach prior to their on-site visit. In general, the level of expected, due diligence effort increases with the asset size of the institution. A visual representation of this specific paradigm is represented in Figure 2.

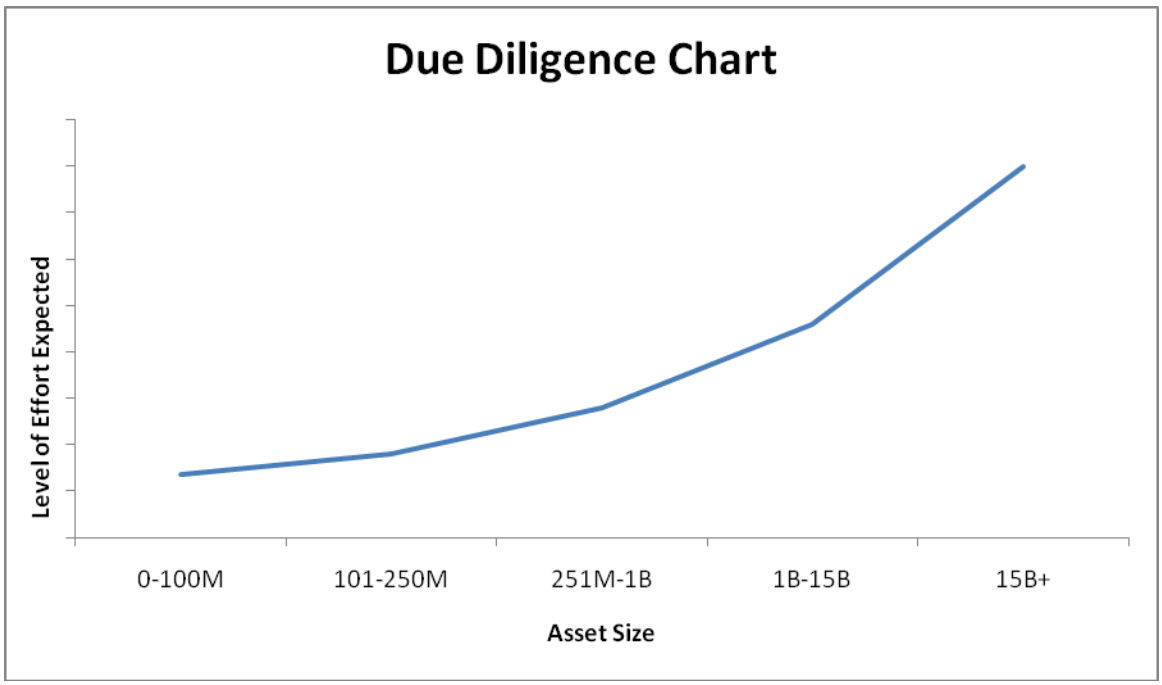
Due Diligence Chart
Level of Effort Expected
0-100M
101-250M
251M-1B
1B-15B
15B+
Asset Size

Figure 2

Conclusions

VRM does not need to be complex although it can require significant effort. Using the simple beforementioned approach will ensure that the correct amount of due diligence is being conducted by the institution.

Summary

FDIC guidance suggests that VRM only applies to critical relationships even though examiners may expect the program to include material and minor relationships as well. However, determination of what is critical can vary by institution. A simple set of questions can be utilized to assist in this determination. The institution's Vendor Management Policy should reflect the criticality definitions as well as the VRM requirements for each. Mapping of the criticality to the due diligence requirements is key to a good VRM program. And finally, the level of due diligence for any given criticality may vary by institution based on its size.

About the author

John M. Edison
CEO
Fortrex Technologies, Inc.

Since co-founding Fortrex Technologies, Mr. Edison has been a key figure in vendor risk management to the financial services community. He designed and prototyped VendorPoint, Fortrex's vendor risk management solution. He obtained patent 7392203 Vendor Security Management System which is the methodology upon which VendorPoint is designed. He has been a featured speaker at OCC training and ABA events.