Mini Vendor Risk Management Handbook

venminder

What is Vendor Risk Management?

Vendor risk management (or third party risk management) is the set of activities associated with identifying the risk that is posed with outsourcing a product or service and then taking all reasonable measures to quantify and reduce the risk.

What is the Importance of Vendor Risk Management?

Proper vendor risk management is essential to protecting your institution, your customers and all proprietary information. In addition to being a sound business practice, it's also a regulatory expectation. During your next regulatory exam, it's a safe assumption that your examiner will expect to see guidance recommendations implemented within your vendor management program.

Framework of Vendor Risk Management

What is a Vendor Management Policy?
The policy is a 5 to 6 page document that broadly outlines the concepts and the structure and also has a focus on regulatory guidance. It should be approved by your senior management team and/or board annually.

What is a Vendor Management Program?
The program describes the concepts laid out in the policy. This can often exceed 25-30 pages and is the fundamental path for all of your vendor management work.

What are Vendor Management Procedures?
The procedures outline the systems and steps you need in order to do every part of the job. These should be very clear and easy to follow, yet comprehensive, so that someone new to the organization could do all of the key tasks of vendor management after reviewing.

Creating a **vendor list**

1. **Establish a threshold** for vendors to be reviewed. This can be determined by setting a targeted expenditure amount (e.g., all payments made to a service provider over $50,000 on a quarterly basis).

2. **Request from accounts payable** a report detailing all expenditures over the threshold amount to include the name of the service provider, the frequency of spend and the amount of spend.

3. **Review the list**, often received in Excel or a custom query format, for accuracy.

4. **Determine which items should be removed**; typically, there are certain expenses that may not actually be forward-looking recurring expenses but anomalies or discontinued service providers which can be removed from the list.

5. **Certain exclusions can be made** if they are mandates by the board or audit committee (e.g., a consultant hired to do a board level recommendation).

6. **Communicate to the senior management team** the need for a detailed review of the list to determine which ones are going to continue to be used.

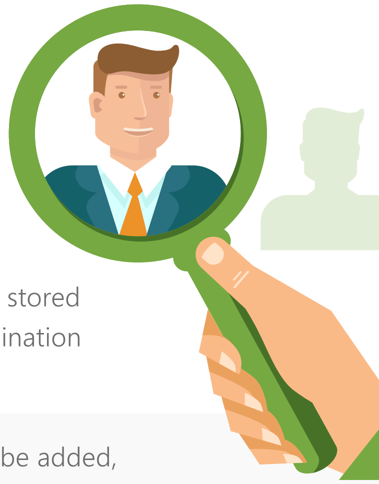
7. Once finalized, this will often pare the Accounts Payable list by 2/3 or more into a list of vendors who need to be actively managed from a risk standpoint.

8. Once finalized, **present to senior management or risk committee for approval**.

9. **Compare the list to the documented scope** in the policy statement and adjust the scope if needed and get approved by the board.

10. **Repeat the entire process at least twice a year.**

Managing
the vendor list



1 Once the final list is determined and approved, the basic list itself should be stored electronically for easy review and examination purposes.

2 Ideally, as new vendors are planned to be added, the business unit follows a formal process to have them added based on a process described in the vendor management program document.

3 The vendors that are to be actively managed need to be risk rated. Consider first if they are a "critical vendor" by asking if a sudden loss of the vendor would cause a material disruption to the business, if the disruption would impact the institution's customers or if the return to normal operations would take greater than a business day. If the answer to any of these is "yes", then they are a critical vendor.

4 Next, consider any possible categories of risk (e.g., but not limited to, operational risk, transaction risk, financial risk, compliance risk, strategic risk, reputational risk, expense risk).

5 Ideally, an objective questionnaire should be applied for each category of risk to arrive at an inherent risk rating for each category and aggregated to a total risk score. These objective questionnaires are typically available through such sources as Shared Assessments SIG, SIG lite or in a scorecard prepared by subject matter experts in the institution, yielding a rating such as high, medium or low for each category.

6 Once this inherent risk assessment has been created, carefully consider what steps can be taken to reduce any areas of high or medium risk; for example, if they are a high transaction risk, perhaps set up ongoing transaction monitoring to quickly catch any anomalies. Or if they are a high compliance risk, consider gathering a copy of their regulatory compliance policies as part of due diligence.

7. Once these controls are in place, review and determine if they more satisfactorily answer the questions; if so, their residual risk may be lower than their inherent risk.

8. The result of these risk assessments and accompanying narrative should be stored.

9. Typically, Excel spreadsheets or Word documents are not sufficient since they lack the ability for mass updates or for easy tracking. More sophisticated programs require a software platform specifically designed for vendor management purposes.

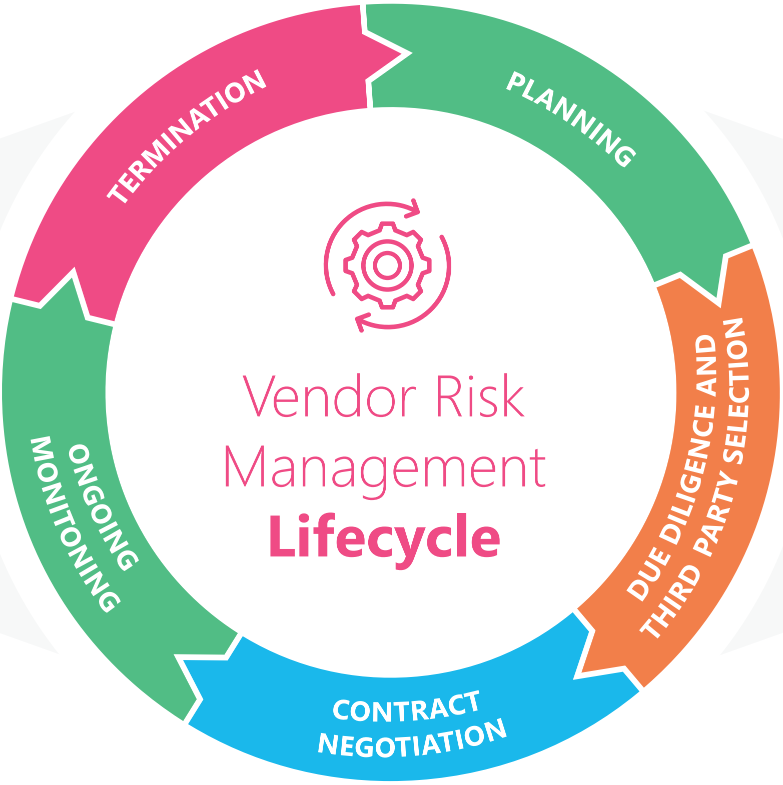
10. The results of the risk assessment, in aggregate, should be included in reports to senior management and the board.

11. The information learned in the risk assessments should be refreshed on a regular basis; a best practice would be to do critical or high risk vendors annually, medium risk every other year and low risk in advance of a contract renewal.

12. The results of the risk assessment inform the depth of due diligence review or frequency and type of ongoing monitoring.

Keeping the **list** and **process current**

1. Establish, with the assistance of the institution's compliance or legal function, a requirement that all new potential vendors follow the documented process.
2. Be prepared to report any deviations from the process to the appropriate senior management team.
3. Not all vendors must go through the full risk assessment and due diligence process, as some will be determined to be one time use or materially insignificant (e.g., office supply provider, a one time use consultant). These that are readily apparent should not be added to the actively managed vendor list.
4. At least twice a year, review the entire list as described above through accounts payable and involve senior management in the determination.
5. At least annually, present the vendor management policy and program to the board for renewal and, if new regulatory guidance is issued, update and present for approval.
6. In advance of a vendor coming up for renewal, follow the same process as a new vendor, except bring in any sort of experience-based information that may result in either a non-renewal or a need to change relevant terms, such as required reporting or contractual provisions. Ideally, this is done at least a full quarter prior to the timeframe required for notification of non-renewal.


PLANNING
DUE DILIGENCE AND THIRD PARTY SELECTION
CONTRACT NEGOTIATION
ONGOING MONITORING
TERMINATION
Vendor Risk Management Lifecycle

These are the stages of the vendor risk management lifecycle.

Planning: Build out the third party policy and program documentation. Having a good plan in place to manage the relationship is essential.

Due Diligence and Third Party Selection: Develop a vendor vetting process for pre-contract due diligence. By completing risk-based due diligence prior to the contract, you will prevent unwanted pitfalls and risk in selecting the wrong vendor.

Contract Negotiation: Define third party expectations and responsibilities early on. This will set the tone for the relationship.

Ongoing Monitoring: Continue to monitor third party relationships on an annual basis to remediate against any undisclosed risk such as a data breach or litigation.

Termination (or Renewal): Develop and implement a plan for terminating relationships. These should include notice periods, transition and exit strategies and the return of assets.

10 Best Practices in Vendor Risk Management to Follow

1. **Actively inventory** all vendors
2. **Confirm with the lines of business** that the vendor list is accurate
3. **Clearly document a policy and program** to govern vendor management
4. **Set clear standards** for selecting and onboarding a new vendor
5. **Establish guidelines** for risk assessing all vendors, not just the new ones
6. **Determine** and **implement** clear due diligence standards
7. **Provide a venue** for ongoing monitoring of vendors
8. **Establish contractual standards** for vendor management
9. **Create a clear line of communication** to senior management and the board
10. Stay abreast of industry **best practices**

venminder

Vendor Risk Management Regulations

FDIC FIL-49-1999 Bank Service Company Act

FIL-81-2000 Risk Management of Technology Outsourcing

FIL-22-2001 Security Standards for Customer Information

FIL-50-2001 Bank Technology Bulletin:
Technology Outsourcing Information Documents

FIL-68-2001 501(b) Examination Guidance

FIL-23-2002 Country Risk Management

Outsourcing Technology Services

FIL-121-2004 Computer Software Due Diligence

FIL-27-2005 Guidance on Response Programs

FIL-52-2006 Foreign-Based Third Party Service Providers

FIL-105-2007 Revised IT Officer's Questionnaire

NCUA 08-cu-09 Evaluating Third Party Relationships Questionnaire

NCUA 2007-cu-13 Evaluating Third Party Relationships

FIL-44-2008 Guidance for Managing Third Party Risk

FIL-127-2008 Guidance for Payment Processor Relationships

Supervision of Technology Service Providers

FIL-3-2012 Managing Third Party Payment Processor Risk

CFPB 2012-03 Service Providers

OCC-2013-29 Guidance on Third Party Relationships

Federal Reserve SR 13-19/CA 13-21 Guidance on Managing Outsourcing Risk

FFIEC Social Media Guidance

FFIEC IT Handbooks (espAppendices E & J)

OCC-2017-7 Supplemental Examination Procedures for Risk Management of Third Party Relationships

OCC-2017-21 Frequently Asked Questions to Supplement OCC Bulletin 2013-29

NCUA SL-17-01 Evaluating Compliance Risk

OCC-2017-43 Risk Management Principles

SEC Statement on Cybersecurity

OCIE Observations from Cybersecurity Examinations

The information in this handbook is not intended to replace a fully documented vendor management policy and program. It needs a well-documented program and policy to support it.

Download free due diligence samples and see how Venminder can help you reduce your vendor management workload.

Download **Now**

venminder

Manage Vendors. Mitigate Risk. **Reduce Workload.**

(270) 506-5140 | venminder.com

About Venminder

Venminder is a leading third party risk management provider dedicated to helping the financial services industry mitigate vendor risk.

Venminder's team of due diligence experts offer a suite of services that can significantly reduce the workload by addressing the tactical challenges of vendor management tasks. Venminder's vendor management software can guide a user through critical processes such as risk assessments, due diligence requirements and task management.