6 Elements
of a Successful Vendor Risk Management Program

venminder

6 Elements of a Successful Vendor Risk Management Program

It can be challenging to keep all the elements of a vendor risk management program straight. Let's cover more about six of the elements we consider critical to a successful vendor risk management program.

1. Reviewing the **Regulatory Guidance**

First and foremost, remember that all the regulators compare and share notes as they all have a seat at the table of the Federal Financial Institutions Examination Council (FFIEC). Therefore, even if one of these governing regulatory bodies isn't whom oversees your organization, it's still worth your time to review their expectations.

Read and understand guidelines around vendor management. **Here are the major regulators we see most often and the guidance you should check out:**

Office of the Comptroller of the Currency (OCC) – Bulletins 2013-29, 2017-7 and 2017-21

Federal Deposit Insurance Corporation (FDIC) – FILs 44-2008, 3-2012 and 19-2019

Federal Reserve (the Fed) – Supervisory Letter 13-19

Consumer Financial Protection Bureau (CFPB) – Bulletin 2012-03

U.S. Securities and Exchange Commission (SEC) – Examination Priorities for 2019

National Credit Union Administration (NCUA) – Supervisory Letter 07-01

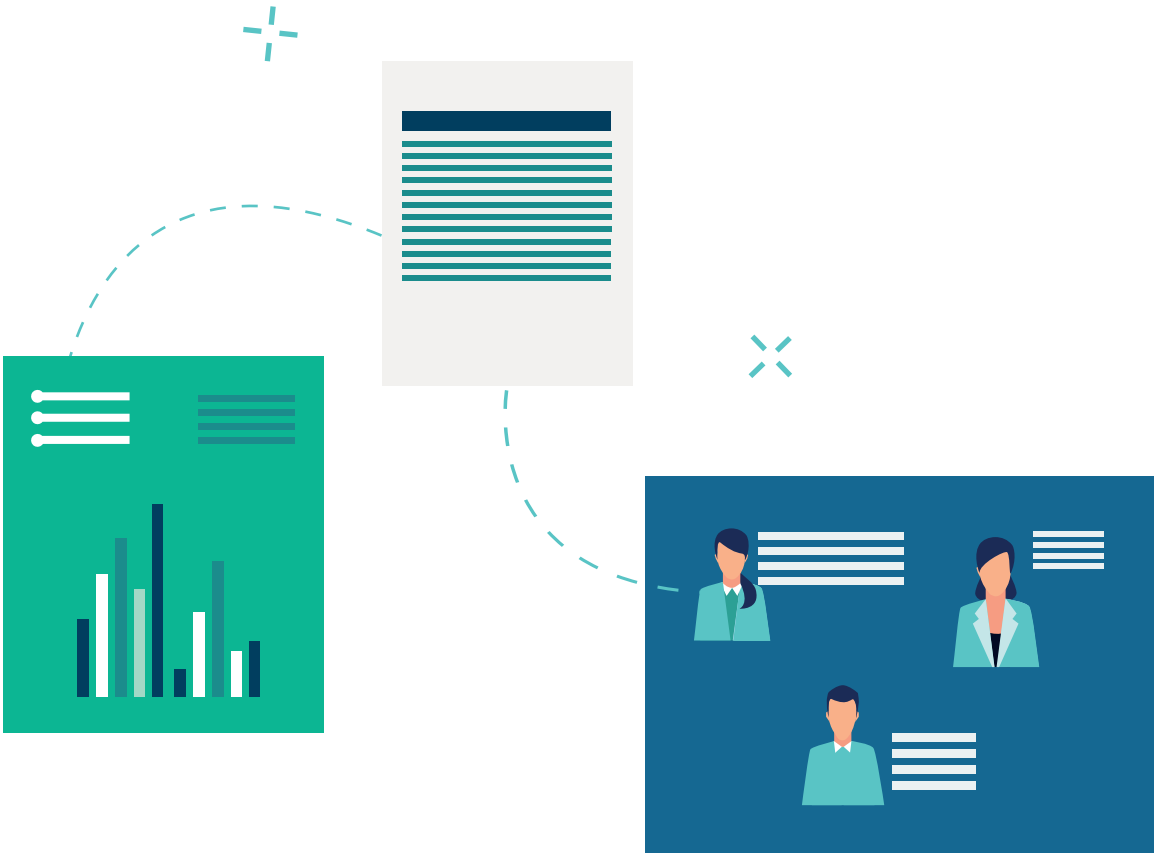
2. Creating a set of **Policy, Program and Procedures**

These are **fundamental documents** that highly influence the success of a vendor risk management program. Here's a little more about each:

The Policy – A high-level overview outlining how vendor risk management will be handled at your organization. The policy is instructive to the board.

The Program – Taking the policy into consideration, the program goes into much more detail and is instructive to senior management and the lines of business.

The Procedures – A step-by-step guide that should be so comprehensive that anyone who reviews them should be able to understand the general responsibilities of their role. Many organizations call these "desktop procedures."



3. Hiring Subject Matter Experts (SMEs) or Outsourcing

SMEs are a critical component of any successful vendor risk management program. They bring a level of expertise that will be valued by your organization, customers, shareholders, examiners and the board.

Consider the following examples:

- A financial analyst or CPA should review vendor financial statements.
- An IT professional or someone certified – such as a CISSP – should review SOC reports, business continuity plans, disaster recovery plans and cybersecurity reports.
- A legal analyst or paralegal should review contracts related information.

Disclaimer: *This is not an all-inclusive list.*

4. Focusing on the 6 Pillars of Vendor Management

The 6 pillars of vendor management are as follows:

1 **Selecting a Vendor** – There should be a defined process in place for vetting a vendor and it should be followed prior to any contract's execution. This will give your organization and your preferred vendor the strongest possible start as you'll know you're choosing the company that aligns best with your overall strategy, goals and needs.

2 **Risk Assessment** – A detailed risk assessment process is critical to any vendor risk management program. As you assess a vendor's risk, you're determining their business impact to the organization – critical or non-critical – as well as their overall risk level – low, medium or high risk – to fully understand the level of risk they pose to your organization.

3 **Due Diligence** – Remember when we mentioned SMEs? This pillar of vendor management is especially why. Not only is it important to request and gather essential documentation such as SOC reports, financial statements, etc., but it's also just as important to have a SME analyze the documentation and report findings. If you don't do this, you're forgetting half of the step.

4 **Contractual Standards** – Ensure your contract outlines what both parties are setting out to accomplish by entering the contractual relationship. That means the vendor's responsibilities and your organization's responsibilities..

5 **Reporting** – You need proper tools to produce comprehensive and standardized reporting, as needed. Your board, senior management and examiners will all expect this. Honestly, Excel spreadsheets make customizable and board ready reports very difficult to produce and are nearly impossible to manage for hundreds – possibly thousands – of vendors. What if the regulations change? You'd potentially have to open up hundreds, if not thousands, of the spreadsheets one by one. A robust tool, such as software, can assist with this and create efficiency.

6 **Ongoing Monitoring** – Often forgotten, but very important, ongoing monitoring is an overall expectation in vendor risk management. You must continue to monitor vendor relationships as they progress to verify the level of risk posed to your organization hasn't increased. With ongoing monitoring, you're on the hunt to catch any negative changes before they impact your organization, such as a decline in service levels, faulty security controls, a sudden dip in financials or any other potential or "risky" areas of concern.

5. Having a **Proper Budget**

Ultimately, vendor risk management is a strategic advantage and investing in your program greatly behooves all involved. It's your **best defense** against weaknesses and risks that arise at your organization. By allocating the right funds to the program, you can do the following:

Eliminate redundancy in vendor use as you'll have greater visibility to easily see if there are similar vendors providing like products/services to different areas across your organization. As you can imagine, eliminating redundancy can lead to an overall cost savings.

Save your customer reputation by contracting with reputable vendors who provide high quality work product.

Satisfy examiners, regulators, senior management and the board as you'll have taken the appropriate steps to address risk and solidify a process.

6. Developing **Internal Audit Procedures**

Introducing an internal audit element to your overall program works as a catch-all. The audit group will look for gaps and inconsistencies in your vendor risk management program to evaluate the effectiveness. Going through internal audit reviews should help identify any weaknesses in your program before an examiner arrives on-site.

Considering these elements greatly yields a vendor risk management program's success.

Download free work product samples and see how Venminder can help 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.