BUILDING AN EFFECTIVE VENDOR RISK MANAGEMENT PROGRAM

Have you considered what it takes to develop an effective vendor risk management (VRM) program? The good news is that you don't always need a large team or unlimited resources. Organizations of all sizes can build an effective program that will satisfy regulators and manage vendor risk.

It takes a holistic and scalable approach with the following key steps:

Step One

Create Your Third-Party Vendor Inventory

Your organization must first determine the scope of the program by defining what a third party or vendor means to your organization and determining which of these relationships will be included in your VRM program. This generally excludes clients, customers, and specific business types that won't need to go through the VRM process, like government entities. From there, work with your accounts payable department to create your full third-party vendor inventory.

PRO TIP
Determining the scope of your VRM program helps you know where to focus your efforts. To help you determine scope, keep in mind that it'll depend on the product or service's scale and dollars spent, complexity, and significance to your organization.

Step Two

Define Roles and Responsibilities

VRM is a team effort, so it's important to clearly define the roles and responsibilities of those involved.

Here are some typical roles to consider:

- **A dedicated VRM team** might have one or more people who perform activities such as identifying emerging risk issues, reporting VRM information to senior management and the board, and preparing for regulatory exams.
- **Internal or external subject matter experts (SMEs)** should provide qualified opinions about the sufficiency of a vendor's controls. They should also identify any gaps or issues that can expose you to greater risk. SMEs are qualified to assess risk in different areas such as privacy, cybersecurity, financial, legal and compliance, and more.
- **Vendor owners** should handle the required daily vendor relationship activities. This individual should be responsible for completing risk assessments, monitoring the vendor's performance, and ensuring due diligence is completed on time.
- **Senior management and the board of directors** should be involved in setting the tone-from-the-top and developing the overall strategy of your VRM program. These individuals should assign roles and responsibilities and be actively involved in critical and high-risk vendor activities.

You may also want to identify other VRM roles such as internal or external auditors, regulators, and oversight and accountability.

Step Three

Develop Governance Documentation

An effective VRM program will include well-written governance documentation that enforces rules and communicates responsibilities throughout your organization.

Consider developing these standard documents:

- **Policy** – This should spell out the rules and requirements for VRM at your organization. A policy will generally include minimum requirements regarding roles, responsibilities, enforcement, and oversight. Your policy should reflect your VRM program in its current state, even if it's not fully developed or mature.
- **Program** – This document can supplement your policy but doesn't need to be created right away just in case you need to revise your processes. A program document can provide specific details about how different departments should collaborate. It can also contain information about reports, deliverables, or functions that are needed for your processes to operate smoothly.
- **Procedures** – These step-by-step instructions can also be delayed until your processes are stabilized. Procedures should be simply written so anyone can understand the day-to-day operations.

PRO TIP
These documents are never just a one-and-done process. They'll need to be updated at least annually or when there are important regulatory or process changes. Always keep a thorough change log.

Step Four

Follow the VRM Lifecycle

The VRM lifecycle is a tried-and-true process of onboarding, ongoing, and offboarding activities. This process is scalable and simple to follow, which enables any type of organization to effectively manage vendor risk.

These fundamental elements set the foundation of the VRM lifecycle: oversight and accountability, documentation and reporting, and independent review.

The following VRM lifecycle stages guide your vendors through each step:

Onboarding a vendor includes tasks such as planning, performing an initial risk assessment and due diligence, and negotiating and executing the contract.

Ongoing activities refer to periodic risk re-assessments and due diligence, monitoring a vendor's risk and performance, and reviewing and renewing contracts.

Offboarding a vendor generally includes formal notification of contract termination, executing the exit plan, and closing any VRM activities like paying open invoices and archiving vendor documents.

Step Five

Create an Issue Management Strategy

Vendor issues can range from minor inconveniences to major disruptions, so it's important to have a strategy in place that identifies, tracks, monitors, and remediates them. This strategy should be formally documented in your policy, so every stakeholder understands the process.

PRO TIP
Issues should be reported regularly until they reach closure, either through remediation or exiting the relationship. The reporting cadence depends on the issue's severity, risk, and lifecycle stage.

Step Six

Generate VRM Reporting

Regular reporting to senior management and the board will help ensure your VRM program remains effective. You may want to report program metrics such as:

- Number of critical vendors
- Number of vendors that require due diligence reviews
- New risks that are emerging within your industry

Remember to report data that drives action and decision making from senior management and the board.

As long as you understand these basic steps, building an effective VRM program doesn't have to be an overwhelming task.

Once you find a specific strategy that works for your organization, you'll realize that effective VRM can become second nature.