Choosing the Right Third Party Risk Operating Model

Choosing the Right Third Party Risk Operating Model

What Model Works Best for Your Organization?

A question we hear often is, "Should my third party risk management program be centralized or decentralized?" We're here to breakdown the different third party risk operating models so that you can determine which one works best for your organization.

Understanding Traditional Third Party Risk Management

Traditional third party risk management involves key disciplines which are found across multiple lines of business. Organizations that have a more mature third party risk management program tend to lean to a more centralized or hybrid vendor management function rather than a decentralized one.

But what does this mean? And for the C-Suite, are there ways which you can implement a system which moves to a centralized third party risk management program that solidifies the risk oversight function and provides valuable data for business intelligence? In short, the answer is yes, but with a hybrid method.

In order to choose the right third party risk operating model for you, let's understand the set-up, advantages and disadvantages of each.

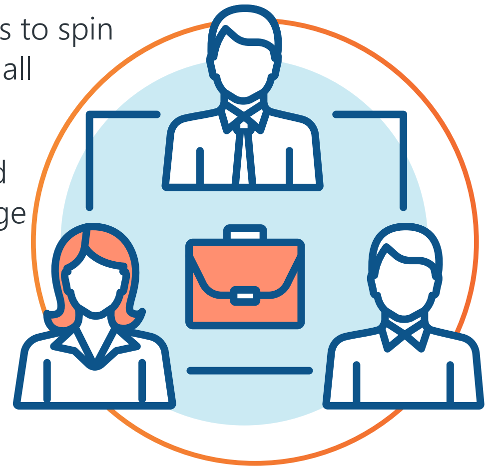
The Stats

According to **Venminder's State of Third Party Risk Management survey**, 57% of programs are centralized, 30% are hybrid and 10% are decentralized. You may be doing some quick math and wondering where the remaining 3% fall. Those programs are fully outsourced.

Centralized Vendor Management

How It's Set Up

With average vendor lists varying from a couple of hundred to tens of thousands on a global scale, there's simply too many plates to spin without an organized system to record, store and manage all third parties.



Third party risk management is becoming more specialized and requires subject matter experts (SMEs) who can manage these various disciplines. Expertise across the enterprise should be identified and a team built around the overall program. If you take a centralized vendor management approach, all responsibilities rest on a single team such as the compliance office or third party risk management department. The team oversees all vendor management activities at the organization (e.g., vendor selection, contract negotiation, due diligence).

Organizations that don't have proper internal resources to execute this outsource to external experts. The external SME isn't there to replace existing staff – they complement the program and do the heavy lifting, when and as needed. When using an external SME, you're still operating a centralized system, but your focus can shift to vendor performance management of service levels or new strategic initiatives.

Advantages

Discipline: The centralized vendor management program allows you to level set the playing field. It brings discipline to a program which by nature requires constant monitoring of cyber risk, fraud, business continuity, disaster recovery, financial strength and potential litigation issues, which may impact your organization both from an operational and reputational standpoint.

Good Communication: Communication in a centralized program is significantly improved over the decentralized model. Creating feedback loops on performance and complaints from your first line of defense, also known as the business units, can go a long way in the overall lifecycle of the vendor relationship. Decentralized systems may allow for disconnects in communication and objectives. There's nothing wrong with a business unit owning the relationship with a vendor, but unless they're committed to the broader risk framework, both in terms of standards and procedures, the decentralized model can cause unnecessary pain points.

Disadvantage

Impractical Components: While a fully centralized vendor management program would certainly be ideal, it can be highly impractical. Impractical in that it often fails to recognize and breakdown the operational silos that may exist within an organization. An operational silo can cause a fully centralized model to fall short when day-to-day relationship managers, in the lines of business, are left out of the vendor management loop completely. That can be a recipe for disaster. While a centralized approach ensures a consistent approach, leaving the business units out of the equation, even unintentionally, means they won't fully understand the risk of doing business with a particular third party.

Consider this example of a centralized approach to vendor management to better understand the process, and where it can fall short at times:

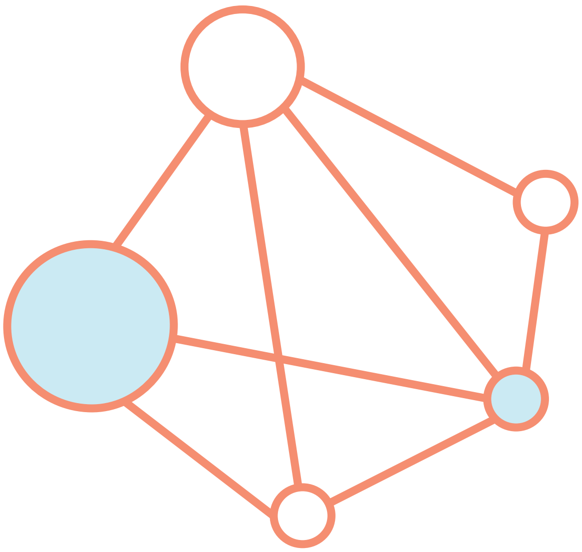
All the vendor management responsibility rested in the hands of the compliance team at an organization. This team was reaching out to vendors to request updated due diligence, looking into new vendor options as needed, reporting on performance, looking into contract renewals/terminations, addressing any vendor concerns and more. All seemed to be going well, until one day, the compliance team realized a new vendor had entered the organization without their knowledge. Upon investigation, the business unit informed the compliance team that they had to make a change; the current vendor was being acquired by a competitor that a member of the senior management team had a very negative experience with in the past.

How did they get the vendor through the process unnoticed? They used the "emergency" clause in the vendor management program and the member of the senior management team with the issue signed off on it! Worse yet, when the compliance team asked the business unit about renewing the existing vendor – many months prior to this drama – the business unit responded they were going to continue with the current vendor. The emergency clause is often found in centralized programs for true emergency situations where a vendor needs replaced and fast; however, more often it's used when someone doesn't want to go through the expected vendor selection process. Unfortunately, emergency clauses often become the real path, not the exception. In the scenario at hand, the organization now has two vendors for the same function; one being used and one being paid but going unused.

Decentralized Vendor Management

How It's Set Up

Various lines of business select and work with the vendor directly. This is common in organizations who run multiple branches and have branch managers responsible for their own profit and loss. With the business units essentially managing the vendor relationships, and likely making decisions, there can be room for error and duplicate vendor types across the organization.



Advantages

Lighter Workload: A decentralized model has its advantages — many hands make lighter work.

Strong Monitoring: The lines of business are in constant contact with the vendor. Why not utilize their relationship to help monitor the performance of a vendor, and perhaps, serve as an early warning system for a potential problem with the vendor? The business units will also be able to give you information you can use when it's time for contract renewal.

Disadvantages

Inconsistencies: The larger the organization, the more risk there is of having radically disparate disciplines related to vendor management. It's up to the vendor management office to establish routine procedures for checking up on a vendor, with each line of business, to be sure SLAs are being met and the terms and conditions in the contract are being adhered to, by both parties. There's a real risk of allowing inconsistencies to occur unless routine processes and procedures help the vendor management team and the lines of business work closely together.

Lack of Discipline: If vendor selection is based on relationships over and above cold hard facts, then there's negligible risk assessment evidence performed at the branch level. This model may offer little in terms of working through a disciplined risk management framework and third party risk management professionals are often the last to know about a new vendor onboarding.

Take this example where a decentralized approach proved to be subpar:

A vendor management professional was asked to approve an invoice for Accounts Payable who didn't recognize the vendor invoice. Given the increase in phishing attacks and wire and invoice fraud that organizations are exposed to, imagine the shock of the vendor management team when there was no record of an approved vendor at the corporate level. The branch manager had entered into a contract without corporate approval and the relationship was impacted when the service levels declined. Legal support was required and made for a messy experience for all parties since the contract was written in favor of the vendor and not the organization. Shortly afterward, the organization made the move to adopt a more centralized vendor management program.

A Hybrid Approach

How It's Set Up

It's nearly impossible to take vendor management and place it in one central area with the centralized model when the organization is very large. It just becomes too much to manage the expectations and essentially creates a black hole where everything will implode.

We feel **THE BEST APPROACH** is a hybrid of the centralized and decentralized model. This means a well-organized and disciplined vendor management office setting the guidelines and checking the results while working very closely with the business units to ensure consistency and timeliness of practices.

With this approach you can expect a centrally led operation, yet a very involved group of business units.

Advantages

Consistency: Baking vendor management into day-to-day practices and annual performance goals with the hybrid model will ensure that the expectations of vendor management are closely adhered to and given the appropriate amount of attention.

Communication: The hybrid model promotes efficiency as there is an open line of communication between the vendor management office and first line of defense.

Support: If the vendor management office has the backing of senior management and accountability to the board, that makes the task all that much better. It's important the board and senior management set the tone and reinforce that everybody has a role in vendor management and compliance in order for it to go well.

Take this example of the hybrid model to better understand the set up and workflow efficiencies created:

A mid-sized organization was operating with a centralized vendor management approach, but as they grew it was becoming too cumbersome to manage. The organization decided to opt for a hybrid approach. By doing so, the compliance team dedicated to overseeing vendor management still developed and managed the policies and processes; however, with their new approach, SMEs within the business units became more actively involved. The business units understood and complied with the implemented policies and procedures. The business units also reported any due diligence findings, SLA reporting, etc. to the compliance team. The compliance team would review and address any concerns or escalate pressing matters regarding critical and/or high-risk vendors to their senior management and the board. As you can see, with a hybrid approach there is a steady workflow with strong communication throughout the entire organization.

One other thing to consider...even if you use a hybrid approach, you need a robust vendor management software platform, like Venminder, to help promote consistency and clarity while gathering all of the documents in the same place.

Want to learn more about Venminder's software and services? **Schedule a demo today!**

REQUEST A DEMO

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.