Vendor Centric

HOW TO KICK START YOUR VENDOR MANAGEMENT PROGRAM

A Practical Guide to Standing Up Your Program in as Little as 90 Days

How to Kick Start Your Vendor Management Program: A Practical Guide to Standing Up Your Program in as Little as 90 Days.

Published by Vendor Centric
9841 Washingtonian Boulevard, Suite 200, Gaithersburg, Maryland 20878

Visit us at **www.vendorcentric.com.**

CONTENTS

Getting Started with Vendor Management

Start Here

Vendor management continues to trend upward as a topic of importance to all companies, driven by pressure to reduce expenses, strengthen risk management and comply with an ever-growing set of regulatory requirements. Ever since the infamous Target data breach involving a third-party HVAC company, regulators, boards and the public in general are all pushing companies for more structure and discipline in how they find, vet and manage vendors, suppliers and similar third parties.

There are a variety of goals and drivers for creating more structure to the vendor management function.

Vendor Management Goals

- **Strengthening the management of high-risk relationships such as cloud computing and software vendors**
- **Protecting confidential information shared with vendors and other third parties**
- **Complying with an increasing set of regulations from Federal and State authorities**
- **Managing costs effectively and ensuring vendor performance is optimized**

Many companies already do some form of vendor management; however, most are at a very rudimentary level with no cohesion or coordination to the process. The result? Poor performing vendors, unmanaged risks and compliance requirements and, in the worst cases, significant impacts to operations and data security.

Given headcount and other resource limitations, it's oftentimes a lower priority to get your vendor management program up and running. But it's a critical business function necessary to manage third party risk, compliance and contractual performance.

So, we created this guide to outline practical steps you can follow to get your program off the ground and get traction fast through meaningful action. It's based on the preeminent sets of regulatory guidance and best practices developed across multiple industries, particularly the financial services industry, which has been among the most stringently regulated for many years.

Let's get started!

The Vendors

Be Clear On Who You Are Managing

The term 'vendor' often means different things to different people. It can sometimes create confusion regarding who to include within your vendor management program, especially since most regulators use the broader term 'third-party' when addressing vendor management programs. So, it's important that you design your program to capture all vendors (and other third parties) that are applicable to you.

Generally, a third-party can be any company or individual with which or whom you have entered into a business relationship to:

Provide goods and services for your own use

Perform outsourced functions on your behalf

Provide access to markets, products and other types of services

Companies often have more third parties than they realize. Some of the more common third parties used in multiple types of organizations can include:

Accountants and auditors
Agents and brokers
Attorneys
Banks
Benefits providers
Bill payment solutions
Software applications (cloud and on-premises)
Security software & systems
Call centers
Consultants and independent contractors
Contingent/temporary workers
Credit card processing
Custodians
Fulfillment and mail houses
Insurance companies
IT hardware, services and support
Internet service providers
Lockbox solutions
Meeting/event-related vendors
Payroll companies
Printing and publications
Payment processors
Shredding and records management
Telecommunications hardware and services
Temporary agencies

So, as you get things going, you'll need to be clear about what a 'vendor' looks like in your company, and if your program should be broadened to include other types of third parties that may not fit precisely in the typical vendor definition.

The Fundamentals

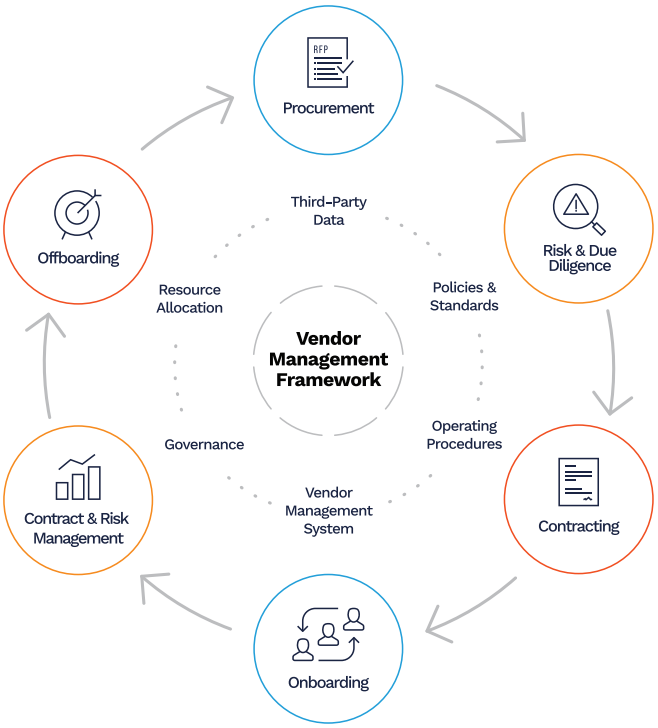
Follow a Proven Framework

Establishing a single, repeatable framework is necessary for the long-term success of your vendor management function. There are fundamentals to follow – you can't make it up as you go along.

Best practice is to take a lifecycle approach to managing vendor relationships. Perhaps the gold standard for this lifecycle approach can be found in a bulletin issued by the Office of the Comptroller of the Currency – OCC Bulletin 2013-29 – which establishes the fundamental blocks every successful program should include and regularly update with all actively managed vendors.

Adopting a lifecycle approach means your program should incorporate all activities involved in managing vendors throughout the lifetime of their relationship with you – from finding them to offboarding them. There are costs, risks, performance and compliance requirements to be managed along the way, and they all need to be considered. The lifecycle includes:

- **Procurement**
  Selecting the right vendor and solution for each unique set of requirements.
- **Risk & Due Diligence Assessments**
  Identifying risks and evaluating controls.
- **Contracting**
  Negotiating terms and allocating risks between you and the vendor.
- **Onboarding**
  Integrating new vendors into operations in a consistent, controlled manner.
- **Contract Management and Risk Monitoring**
  Managing costs, performance, risks and compliance requirements during the term of the relationship.
- **Offboarding**
  Formally ending and de-risking the relationship, including a formal exit strategy for critical vendors.



To ensure activities are performed consistently throughout the lifecycle, you also need to align your people, processes and systems to support these activities. These include:

Governance & Oversight

Provides vision, direction and accountability for the vendor management function.

People, Skills & Training

Ensures the right level of vendor management resources, subject matter expertise and stakeholder knowledge.

Third-Party Profiles

Organizes data and documents so you have clear profiles of your third-party relationships.

Policies & Standards

Establishes the scope and guidelines for the program, and defines key roles and responsibilities.

Operating Procedures

Defines the day-to-day activities stakeholders will undertake to execute the program.

Supporting Technologies & Systems

Centralizes information, facilitates workflow, provides reporting and ensures an audit trail of activities.

The scope of vendor management activities and infrastructure should scale to your company's size, needs and overall risk appetite. But you need all of the fundamentals to be in place for your program to be effective. You also need to ensure you establish a clear owner of the program's day-to-day operations, which can be done via a single individual or a working group/committee.

The Approach

Take a Phased Approach to Building Your Program

Implementing a vendor management function doesn't happen overnight. But you don't want to spend months putting it together - you want to start with the basics to get traction and some quick wins under your belt.

You can do this by taking a practical, risk-based approach to building your program. We recommend that you get the fundamentals in place and start getting those riskiest vendors under control (and some wins), and then start maturing your program to get it where you ultimately want it to be. Your riskiest vendors include those that are critical to your day-to-day operations, as well as those that present other types of higher risks such as access to your sensitive data. (***See Criticality vs. Risk – What's the Difference for additional guidance***.)

We've broken the process down into three phases. It looks like this.

Phase 1:
Establish Your Foundation

Start by establishing your fundamentals with support from senior leadership. This ensures alignment and the right tone-from-the-top.

- Develop your policy
- Inventory your vendors
- Clarify roles and responsibilities
- Create your core assessment tools

Phase 2:
Get Traction and Some Quick Wins

With your fundamentals in place, get traction by beginning to assess your most critical and riskiest vendors.

- Risk assess and categorize vendors into risk tiers
- Start conducting due diligence with your highest-risk vendors
- Begin tracking and remediating issues you identify
- Start with some basic monitoring activities around performance, cybersecurity, financial health and negative news.
- Rinse and repeat with the rest of your vendors, starting with the next riskiest group and working your way down

Phase 3:
Create a Roadmap to Mature Your Program

Finally, once you are consistently doing the basics, create a path for enhancing and maturing your program. These can include:

- Automate business processes with technology
- Identify and assess 4th parties
- Enhance standards for contracting, termination and offboarding
- Audit contracts and consolidate spend with fewer vendors
- Assess concentration and geographic risk
- Plan for new products

If you're committed, you can establish your foundation (Phase 1) in 90 days or less. The rest of this guide is going to be your playbook for getting it done.

Building Block #1. Create Your Vendor Management Policy

Creating the Foundation for Your Program

The starting point for any new vendor management program is the policy. It's the blueprint you'll follow to roll out your program and mature it over time. The policy itself does not need to be elaborate, but it does need to set a "tone from the top" – senior management [or other governance structure that has oversight of your organization's risks and controls] should set firm direction on expectations and lay out the ground rules for full adherence.

The policy document itself can be simple in structure – perhaps 7 or 8 pages – but should include the following key elements.

1. **Governance** – Define the role of the governing body (individual, working group or committee) over this function. Determine which functional group within the company will own the vendor management function (more on that later).

2. **Ownership** – Be clear in the policy that each vendor will be assigned a relationship owner that is responsible for managing performance, risk and compliance with the vendor.

3. **Stakeholders** – Identify all key stakeholder roles that must be filled to support an effective line of defense for your program. In addition to the relationship manager, key roles include risk management, information security, compliance, business continuity and legal.

4. **Categories of Risk** – Describe the types of risk your program is being designed to manage with your vendors. Align with your enterprise risk function if you have one. Common categories to define include strategic, financial, operational (including information security risk, concentration risk, 4th party risk), reputational, compliance and legal risks.

5. **Risk Classifications** – Clarify the 'tiers' you will be using to categorize vendors by level of risk. Most common is a three-tiered classification – high, medium and low – though some companies use other tier structures to align with broader enterprise risk policies.

6. **Critical Activities** - Criticality refers to how significant a vendor is to your organization's operations – If your vendor failed or was suddenly not operational, would your organization be able to function, or would there be serious financial impacts? Your policy should define what a critical vendor looks like for your company. (See callout on next page.)

7. **Program and Vendor Scope** – Define which activities are in-scope for your program (i.e. risk assessments, due diligence, monitoring, etc.) along with which types of vendors/third-parties are in-scope. The latter will help you create your in scope vendor inventory.

8. **Applicable Laws and Regulations** – If your industry has third-party regulatory requirements you need to follow, reference them here.

The policy should work hand-in-glove with other policies where risks are also defined – like enterprise risk and information security risk. It should also be reviewed and refined on a periodic basis. Best practice is also to have the policy approved annually by whomever has oversight responsibilities (i.e. Board of Directors or Executive Committee), and that there is periodic testing of the program's procedures and controls to ensure documentation is complete and accurate, and procedures are being performed according to policy.

Criticality vs. Risk What's the Difference?

It is a common misnomer that a 'critical vendor' and a 'high-risk vendor' are one in the same. They are not, and it's important to delineate between the two when establishing your program.

Critical Vendors

A critical vendor is one that you rely on heavily to support the most important activities (ie. 'critical activities') within your company; that is, those that are necessary to support the work you do. Critical activities often include:

- Support of financial operations via an outsourced vendor (i.e. payment processor)
- Infrastructure provider that powers back-up servers and remote access to daily activity for critical employees.
- Vendors whose systems store, restrict or protect access to client information (ie. Firewalls, data warehouses, etc).

High Risk Vendors

On the other hand, a high-risk vendor is one that presents a heightened level of risk to your company regardless of how critical they are to your operations. A common example is a vendor that has access to your data. These vendors are higher risk due to the type of information to which they have access, but they may not have a significant role in supporting your critical activities. Other factors that can elevate the risk of a vendor include:

- Access to your building/offices and direct contact with your employees
- Support of your own compliance with laws and regulations
- Direct interface with your customers (i.e. investor portals / data rooms, outside counsel)
- Use of downstream contractors or service providers (i.e. 4th parties) to provide the good or services to you.

Is a Critical Vendor Always a High-Risk Vendor?

No. Every company has a subset of vendors that are both critical but also lower risk. Your internet services provider is a good example. Clearly, your internet connection is critical to your day-to-day operations, but the risks associated with most internet service providers are relatively low.

Identifying Your Critical Vendors

So, defining your critical vendors begins with being clear on your own critical activities. A good place to start is with your company's business continuity plan (BCP) which should already define critical activities for you. From there, it's about identifying and segmenting the vendors that are critical to supporting those activities. Here are three, key questions that will help.

1

Does the vendor provide a key technology that supports the critical activity?

2

Did we outsource a component of the critical activity to the vendor?

3

Does the vendor provide crucial data, models or other products we rely on to perform the critical activity?

As you get your program up and running, focus your energy on these critical vendors to start.

Building Block #2. Inventory Your Vendors

Compiling Your Source of Truth

Now that your policy is in place, how do you create the actual inventory of your vendors? The best practice is to simply *follow the money!*

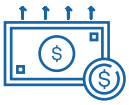
There are generally two main sources of data. The first, and your primary source, will be your accounts payable system. It lists everyone you pay. The second, supplemental source are your credit card statements if your company has a commercial card program. They house information on vendors you use that does not typically show in your accounts payable system.

Getting data exports from both is relatively easy; however, it can be overwhelming if your company works with a lot of vendors. So, you may want to cull down the list and weed out vendors that have negligible risk or fall outside the scope of your policy.

The most common approach to doing this is to pick a dollar threshold. While certainly helpful, simply knowing how much you spend does not tell the whole story. As an example, you may find that you don't spend much money with a particular attorney but you may be sharing highly confidential information with her. In this example, the financial risk is not high but the information security risk sure is.

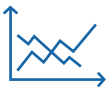
You need to strike a balance of creating an accurate inventory while not having to slog through hundreds or thousands of vendors. The best approach is to create gating criteria you can use to help narrow down the list. We recommend these five:

Vendor name



Spend amount

(use the most recent 12 months)



Spend frequency

(to eliminate one-time vendors)

Category

Vendor names, spend amount and frequency should all come from your systems. You can generally get the category too, but sometimes you may need to append the list with the category. The categories are really important as they'll help you eliminate vendors who fall outside the scope of your policy or present negligible risk. These might include caterers, memberships and subscriptions and sponsorships. They can also include things like tax payments to government agencies or payments to utility companies.

One additional data point you'll want to append to this list is the name of the employee responsible for the vendor relationship. The employee name is also critical because that's the person who can give you some insight into how you are using the vendor. Once you've identified them, you should review the inventory with them to further scrub the list and then carefully compare it back to the policy for anything that may need to be adjusted in your inventory or in the scope of the policy.

Tip:

When first doing this, you may find that several of your vendors don't have a clear owner. This can be due to turnover as well as the vendor being utilized across multiple departments. Creating your inventory is a great opportunity to assign or reassign the owner for each of your vendors.

Building Block #3.
Define Roles and Responsibilities

Clarifying Your Team

Writing your policy and inventorying your vendors are fundamental to getting your program off the ground; however, the rubber meets the road when you start doing the actual work. So, this building block is all about identifying and aligning your team.

Here are the core roles you'll need to define.

- **Relationship Managers**
  Responsible for day-to-day interaction with vendors, and provides first-line oversight and management of the relationship.
- **Vendor Management**
  Responsible for the facilitation and execution of vendor management activities in support of the policy.
- **Information Security**
  Sets information security standards, develops/advises on risks and due diligence and evaluates controls of your third parties.
- **Risk Management**
  Advises on third-party risk standards and practices, and ensures alignment with enterprise risk management policies and procedures.
- **Legal**
  Sets contractual standards and advises on contracting with vendors.
- **Compliance**
  Marries the policy standards to other elements of regulatory guidance
- **Senior Management**
  Sets expectations for the overall vendor management policy, and ensures adherence to policy within their departments.
- **Internal Testing / Control Group**
  Tests and reports on the adequacy and effectiveness of the program. This function may fall to your organization's compliance or risk team(s), and when applicable, an Internal Audit function.

Many companies maintain a lean, small staff. It's possible that one person may be responsible for many of these roles, and may not have necessary subject matter expertise in areas like information security, risk management or compliance. So, your resourcing plan should include identifying your internal 'quarterback' for the program (i.e the person that will run point and fill some of these roles), the subject matter experts you already have on your team (i.e legal, information security) and any external partner(s) you can rely on to fill roles and, when appropriate, manage many of these activities on your behalf.

Another important consideration is where the vendor management function is going to sit. In smaller organizations, this responsibility is often added to an existing business unit like legal, compliance, risk or IT. In larger organizations, you'll generally find a Vendor Management Office that operates autonomously.

Regardless of your size, however, there is no one place where the function should always sit. Placement of the function should really depend on answering three questions:

1

What is the primary driver for creating a vendor management function?

2

What does your company consider to be its greatest vendor risk factors?

3

Who is the Executive Sponsor?

Answers to these questions will guide you towards the right home for you vendor management program.

Building Block #4. Create Your Core Assessment Tools

Developing Your Toolkit

The last building block you need to tackle is creating the tools you'll need to begin assessing and managing your vendors. These consist mainly of the forms and templates you'll use to asses and monitor your vendors.

While the scope and breadth of each tool can differ widely between companies (mostly based on their risks and program maturity), the tools themselves consist of the following:

Inherent Risk Assessment Form

The Inherent Risk Assessment Form is in internal form, completed by the Relationship Manager, that is used to assess potential risks with a vendor before entering into a contract and again when there are material changes to an existing relationship. The goal is to tease out the types of risks that are naturally inherent in the relationship being considered, and to determine what type of diligence you need to perform. At a minimum, key questions you should be asking include:

- Do you outsource critical services or operations to the vendor, and/or do you rely on them to effectively run a critical business function?
- Will the vendor have access to personal or confidential information?
- Will your vendor have access to your building/offices, and potentially direct contact with your employees?
- Do you rely on the vendor for revenue generation, or will there be hefty costs if a contract is terminated early?
- Is the vendor an integral part of your compliance with laws or regulations?
- Does your vendor rely on downstream contractors or service providers (i.e. 4th parties) to provide the goods or services to you?

Due Diligence Assessment Form(s)

The Due Diligence Form(s) are external forms, completed by your vendors at relationship inception and on a routine basis thereafter, and that are used to assess the systems, processes and controls your vendor has employed. For a company just starting out with a new program, the forms typically consist of a series of vendor-facing questions that you use to spot potential red flags and issues that need to be remediated before entering into a contractual relationship (and also identify new issues that may arise during the course of the relationship.)

The scope of due diligence performed is truly personal for every company. While some standard due diligence questionnaires exist, the scope of your due diligence questions should align with your company's own risk appetite. With that said, there are common categories of diligence questions that are asked which include questions about:

Risks to Evaluate as Part of Vendor Due Diligence

- **Financial health**
- **Lawsuits and litigation**
- **Bankruptcies**
- **Insurance**
- **Business continuity**
- **Compliance with laws and regulations**
- **Information security**
- **4th parties**

For any company just starting out with vendor management, we recommend starting with the basics but doing them consistently well. Then mature your diligence over time. You want diligence to be a substantive program, not a check the box process.

Tip:

As you create the questions to include in your due diligence questionnaire(s), make sure to put some thought into how you want vendors to answer each question (i.e. your organization's preferred responses). Doing this work up front will provide you with some standards to follow as you evaluate vendor responses (and will result in a more consistent evaluation process). For example, let's say that your due diligence questionnaire asks vendors about the types of background checks they perform on their employees and contractors. If the vendor's answer does not meet your minimum requirements/preferred response, you can easily flag the vendor's response as an issue that needs to be remediated.

Issue Remediation and Management Tool

Lastly, as you identify issues with vendors and develop plans for how you want them to be remediated, you'll need a tool to track them to ensure they get resolved. Auditors and regulators are very focused on issue management, so make sure you have a way to not only track issues but also document that they've been resolved.

One final point. Technology is going to be critical to manage all of this as you scale and grow your program. While you can certainly use Word and Excel as the basis for your tools when managing a handful of vendors, it is not going to be sustainable as you scale. You will need a good vendor management system that automates your risk assessment, due diligence and issue management process. The earlier you can get this established, the more efficient and effective your program will be.

Ready, Set, Go: Your Kick Start Checklist

A Reference Checklist to Stand Up Your Program Quickly and Efficiently

Policy

- ◯ Overarching goals and objectives for the program
- ◯ Governance and oversight structure (committees, senior management)
- ◯ Program ownership (which department will own the program)
- ◯ Framework you are following for the program
- ◯ Types of risks you will be assessing and managing with your third parties
- ◯ Risk tiers/classifications (i.e. low, medium and high)
- ◯ In and out of scope third party categories
- ◯ Documentation and record retention requirements
- ◯ Handling of exceptions and deviations
- ◯ Responsibility for annual policy review and refinement

Inventory

- ◯ Accounts payable system data – recent 12 months of spend
- ◯ Credit card / expense management system (name, transactions, spend, categories)

Roles & Responsibilities

- ◯ Identification of stakeholders to fill each required role (internal + external)
- ◯ Outline of responsibilities for each stakeholder

Toolbox

- ◯ Inherent risk assessment form
- ◯ Due diligence questionnaire(s) covering questions related to:
  - ◯ Corporate and contacts
  - ◯ Information security
  - ◯ 4th parties / vendor management
  - ◯ Business health/financial
  - ◯ Employment screening
- ◯ Issue management tracking tool

About Vendor Centric

Vendor Centric is a national consultancy that specializes in all three pillars of vendor management: procurement, contract management and third-party risk. We provide advisory services and managed solutions that enable organizations to take a systematic, risk-based approach to creating more value and less risk with their vendors.

5 Reasons Our Clients Hire Us

We are Vendor Management Specialists

We are Independent – You Can Trust Our Advice

We Guarantee Quality Outcomes

We Provide No Surprise Pricing

We Make Your Job Easier – Really, We Do.

Kick Start Services and Solutions

Kick Start Package	Implementation & Operational Support
Our kick-start package will enable you to get your fundamentals in place in 8-12 weeks. We follow our proven approach - and leverage our library of compliant, best-practice based tools and templates – to help you quickly get the four building blocks in place. • Vendor management policy • Inventory of in-scope vendors • Roles & responsibilities inclusive of your staff and external resources • Toolbox of personalized forms and questionnaires You get everything in this package for one fixed fee.	Once the fundamentals are in place, we can further support you in rolling it out and managing it for long-term success. • Staff Onboarding & training • Software implementation & training • Vendor due diligence support • Dashboard and report development • Program compliance testing • Program maturity & continuous improvement We offer options for every budget including project-based support, staff augmentation and co-sourced solutions.

Ready to kick-start your vendor management program?
Schedule a free consultation to get a personalized plan on how we can help.

letstalk@vendorcentric.com