KnowBe4
Human error. Conquered.

WHITEPAPER

Starting Your Vendor Risk Management Strategy From Scratch

by Roger A. Grimes

Table of Contents

You've heard that vendor dependencies are ripe for malicious abuse and you have read the stories where vendors were used to exploit and infiltrate their customers. Now, you've been put in charge of ensuring your vendors, third parties, contractors, and supply chains are at least as secure as you are: *Welcome to Vendor Risk Management (VRM)!*

Where Do You Start and What Do You Do?

First, recognize that VRM is all about reducing overall risk to your organization, and in particular, cybersecurity risks since much of how we interface with vendors is via digital interactions. Second, recognize that it's going to take a system to do it. VRM isn't a process that scales well using paper and verbal interviews.

Here are the other steps and phases along the way:

Get Executive Management Support

Make sure you have executive management sponsorship. VRM programs will take time, people, and money. You likely have executive support if you are already exploring how to do a VRM program; but if not, it is essential that senior management is on board supporting the program and for the expenses involved. A VRM system can easily lead to a situation where someone's existing or newly selected favorite vendor is being denied access to interoperate with your systems or data. Denials to move forward can strain relationships and bring emotions into the mix. You need solid management support so that if, or when, the tough decisions need to be made, everyone understands the reason for the VRM program in the first place. You want everyone on your team pulling in the same direction—pulling for the vendor to remediate their critical issue instead of blaming you for interrupting an existing or new process. Everyone always claims they are onboard until someone can't get what they want to meet their own project deadlines. You will need the backing of senior leadership to assist in these instances. Don't do it alone.

Make sure you have executive management sponsorship. VRM programs will take time, people, and money. You likely have executive support if you are already exploring how to do a VRM program; but if not, it is essential that senior management is on board supporting the program and for the expenses involved.

Define the Program Scope

You need to define the scope of the VRM program. Will all vendors (and contractors and third parties), regardless of size, be required to participate? Are there any minimum entry-level items that force a vendor to be involved with your program such as revenue/expense thresholds, the involvement of confidential data, etc. Are there industry requirements (e.g., NIST, ISO 27001, HIPAA, PCI-DSS, SOX, NERC, etc.) involved? Can the company do business with vendors and other third parties that haven't undergone the VRM process?

Most VRM programs set revenue/expense thresholds along with a requirement involving the exchange of the organization's confidential information. The goal of any VRM program is to protect the organization from risks caused by vendors. That only occurs when a vendor is using your systems or has your confidential data. For instance, a vendor who scrubs your customer lists or processes employee PII data would be included. But an employee buying something on Amazon or at Walmart where the only confidential information exchanged is payment information and shipping address probably would not be included. How will VRM compliance be measured, questionnaire only, audits, or a combination? Are there independent departments or entities within the organization that need to be treated like a vendor to reduce their risk to the organization? Will potential merger or partnership relationships need to be evaluated within a VRM program? The VRM program scope needs to be determined ahead of time.

Define Resources

VRM programs take people, processes, systems, and time. Define who is in charge and involved in the program starting with senior leadership and spanning across the entire organization. What departments are involved, what are their critical functions, what are the expectations, and what are the required service delivery times? Having an online system involved will save time, money, and resources, especially in an ongoing VRM program.

Define Compliance Requirements

What are the compliance requirements that your involved vendors will be expected to meet? Will they have to meet all the requirements of an industry regulation (e.g., NIST, ISO 27001, HIPAA, PCI-DSS, SOX, NERC, etc.), all of your critical security requirements, or just a subset? What are the Governance, Risk, and Compliance (GRC) requirements that in-scope vendors will be expected to meet? Will vendors be required to meet 100% of requirements to be accepted as a vendor, or is there a risk-based methodology and score a vendor must meet to be able to do business with your organization? Are there critical requirements, such as encrypting PII information at rest and during transport, that will result in an automatic failure? If an issue is found, how long do vendors have to remediate it? Can vendors who promise to remediate do business with your organization now? Will you accept other attestations or certifications (e.g., a SOX compliance report, etc.) as meeting your own requirements?

Design a Scoping Questionnaire

Design a scoping questionnaire to be sent to all vendors to determine which vendors must be included in the VRM program and undergo compliance to remain or become a vendor. This should include all the factors determined above about what made a vendor's participation become a component of significant risk for your organization. You want to learn from the vendor what type of data and other interaction they have with your organization. Do they connect to your network? Do they have access to your critical data on your network and/or on their own? Ask whatever it is you need to determine if they need to be included in the larger VRM program. If a vendor is excluded, send them a report detailing the thresholds at which if they cross, they must voluntarily self-report and must now become compliant in your VRM program.

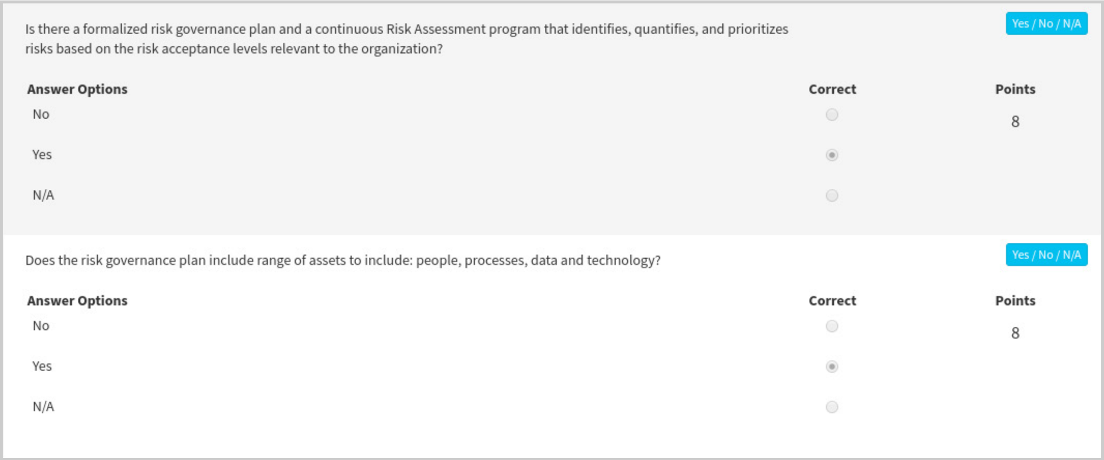
It's important to design the scoping scenario to define and detect between critical and non-critical vendors. Non-critical vendors will typically get less questions and less frequency of questionnaires. Your scoping questionnaire should ensure that your organization spends more time with the critical vendors and less time with non-critical vendors.

Design Compliance Questionnaires

Next, based on the desired compliance requirements vendors must meet, create a compliance questionnaire to send to in-scope vendors. Preferably, you can use an online questionnaire so the vendor's immediate responses are collected and stored for analysis. Second best is an email or electronic document sent with the questions to the vendor and the answers are reviewed and placed into the VRM system. The least desirable option is a system where only paper questionnaires are sent, and answers are collected and stored in a paper-only system.

Overall, you want to minimize the number of questions sent to both your critical and non-critical vendors. Non-critical vendors should get less questions than critical vendors. But even critical vendors only have so much bandwidth to answer questions. The more questions you have, the less compliance you can expect. Multiple questionnaires asking every detailed question possible is going to stress the resources of your vendor. Ask the questions you need to satisfy that a particular risk is covered, but you don't need to necessarily know every detail. For example, perhaps you ask if the vendor uses passwords eight-characters or longer and if they require periodic password changes, but you don't ask about complexity makeup or whether password history issues are prevented, or at what level. Ask enough detail that you feel confident the vendor is mitigating a particular security concern, but you don't have to know every answer to every security detail.

The screenshot below shows a sample of an example vendor survey from the KnowBe4 Compliance Manager GRC platform.



Is there a formalized risk governance plan and a continuous Risk Assessment program that identifies, quantifies, and prioritizes risks based on the risk acceptance levels relevant to the organization?

Answer Options	Correct	Points
No	○	8
Yes	●	
N/A	○	

Does the risk governance plan include range of assets to include: people, processes, data and technology?

Answer Options	Correct	Points
No	○	8
Yes	●	
N/A	○	

Select a GRC/VRM System

Anyone involved in VRM management is going to want to manage the entire process, from beginning to end, using a system built for that purpose. Some companies offer stand-alone VRM systems or external services, but even more companies use their existing GRC system's functionality to run a VRM program. The latter choice more easily allows all the risks, both inherent to the organization's own issues and those relevant to vendors to be accounted for and managed in one place. After all, the whole reason VRM is important to an organization is to manage risk to the organization, so why not manage all risk in one place using one system? If two systems are an external system or a service is used, the organization is faced with how to collectively measure and compare risk from two or more systems. For example, how does a critical risk in a vendor's system equate to risk to the organization overall? With a common GRC system tracking all risks, internal and external, all risks can be seen together and evaluated at once.

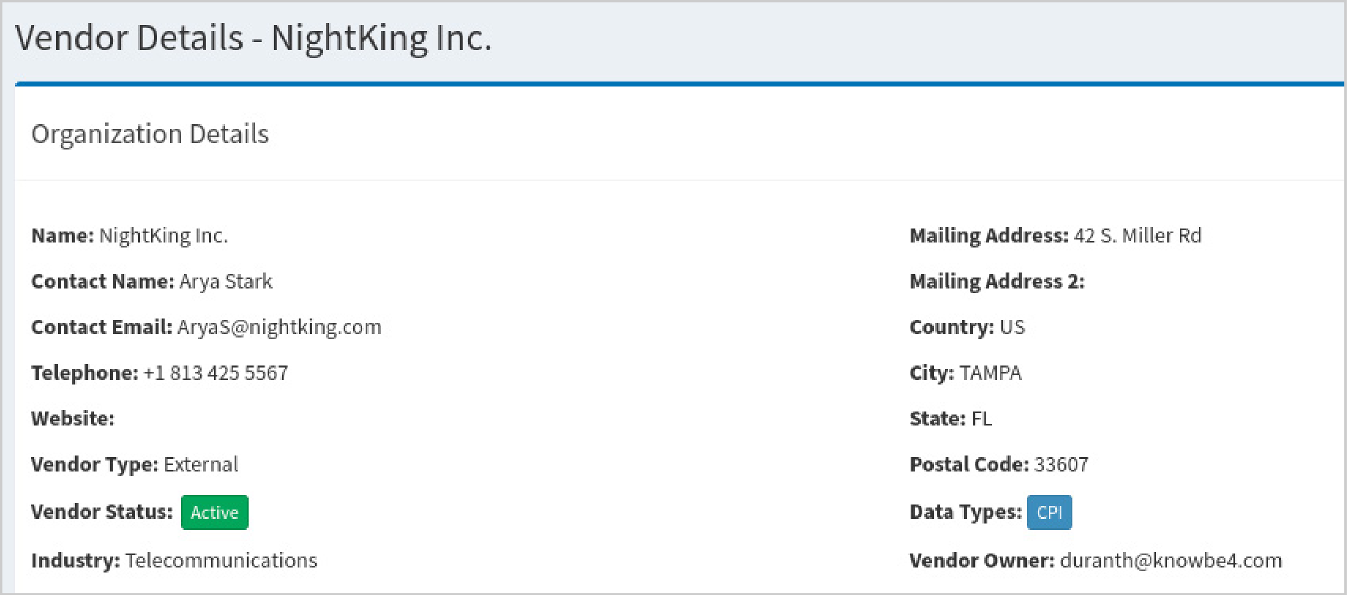
Communicate the Program to Organization

Next, the VRM program needs to be communicated throughout the organization so that all employees dealing with vendors, third parties, contractors, etc. know that your organization has a formal VRM program to which all vendors and other external entities must submit and understand how it functions. Normally, this is done using email communications and potentially a slideshow presentation to show impacted co-workers how it works, including pathway flow and example questionnaires. You should prepare for multiple instances of communication if a VRM program is new to your organization. Change is never easy.

Collect Vendor Information

Collect the names, services provided, contact information, and other details to be able to put all the possible vendors, who will be sent scoping questionnaires, into the system. Any collected or learned information should be put into the system. A good place to start is in Accounts Payable. Most active vendors will be accounted for in Accounts Payable, although not always. Include any department, such as IT, who regularly deals with vendors, third parties, and contractors. Decide how "inactive" a vendor must be before they are not sent a scoping questionnaire.

The screenshot below shows an example of vendor details from the KnowBe4 Compliance Manager GRC program.



Vendor Details - NightKing Inc.

Organization Details

Name: NightKing Inc.

Contact Name: Arya Stark

Contact Email: AryaS@nightking.com

Telephone: +1 813 425 5567

Website:

Vendor Type: External

Vendor Status: Active

Industry: Telecommunications

Mailing Address: 42 S. Miller Rd

Mailing Address 2:

Country: US

City: TAMPA

State: FL

Postal Code: 33607

Data Types: CPI

Vendor Owner: duranth@knowbe4.com

Communicate the Program to Vendors

Once you believe you have collected as many active vendors as you can and are ready to start your program, it's time to send out an introduction letter, document, or email. You want to introduce the program, its objectives, and basic workflow. Many times, the initial scoping questionnaire (or even better, scoping URL) is included. Be sure to clearly document all requirements, timelines, and the "rhythm" of the program. Let vendors know that a failure to respond in a timely manner will automatically result in their future suspension as an allowed vendor. With that said, active vendors who do not respond are usually contacted by their normal person they interface with to make sure they received the announcement and to clear up any remaining questions and requirements.

Note: Make sure the initial communications include an ethics statement, requesting all vendors to act and respond in ethical ways. Include text that essentially says that the organization expects all vendors to comply with the program's overall objectives and intent, and anything not covered that could cause critical risk to the organization should be proactively reported to the organization when noticed. Vendors should strive to help the organization meet the intent and objectives of the program as a partnership in which both sides bring out one another's strengths and thrive together.

Send Compliance Surveys

If not yet sent, send the compliance surveys to each vendor's contact. Again, hopefully this is an online document so that information is easy to request, answer, and evaluate. Give vendors a set time period in which they need to complete the survey, along with additional warnings if they fail to complete the survey on time. Brand new vendors should be sent the scoping questionnaire, as they are considered for addition to the organization. They should also be sent and required to answer the compliance survey before being fully admitted for any business transactions. Have ad hoc, one-off policies and procedures for vendors needed during emergency or last-minute circumstances. It will happen.

Assess and Validate

Collect, assess, and validate the vendor compliance questionnaire answers. Identify the most critical gaps and assign, or have the system automatically assign, risk scores. Be aware that not all risks are alike. For example, the risks from social engineering and unpatched software account for more malicious cybersecurity incidents than any other risk factors. Make sure risk scores truly match the risk to the vendor or organization.

Determine ahead of time and communicate to vendors how often they can be expected to repeat the questionnaires. Define how long you can wait for a vendor to meet critical compliance requirements before their vendor status is in jeopardy. Your key objective is to remedy the top, most critical risks first and best.

Remediate

Help vendors remediate, whatever that means. It could mean that you simply tell them the top critical issues they need to resolve, it could involve education, or it could even involve you telling them how to resolve a particular issue. It is essential that your program defines what happens to vendors that do not or are not able to remediate critical risks in a timely manner.

Update Your Vendor Risk Management Process

Update your risk management process and system information as needed in order to make your VRM program a success. VRM is a moving target, constantly being updated to focus on different, emerging critical risks. Make sure your VRM program has built-in agility.

The key is you want to try to be seen as a partner, interested in them successfully remediating critical issues and not just a roadblock (i.e., “Fix this or you are gone!”). That’s not going to make vendors or those within the organization relying on them happy. Your objective is to reduce unnecessary risk to the organization, not to become a roadblock to operations and profitability.

KCM
Audits Done. Half The Time.

KnowBe4’s KCM GRC Platform

Most old-school, on-premise compliance applications require months of implementation and outside consulting help to deploy, as well as a commitment to yearly maintenance and support fees. Small, mid-sized organizations, and many divisions of multi-nationals can’t afford this high cost, nor do they need an enterprise compliance platform. There are affordable, cloud-based alternatives, however. KnowBe4’s KCM GRC, a pure SaaS platform, provides you with Compliance, Risk, Policy and Vendor Risk management modules to help you save tons of time getting through audit requirements. KCM GRC has a simple, intuitive user interface, easy to understand workflows, a short learning curve, and deployment that takes days, not weeks or months. It’s also affordable for any size organization. KCM GRC makes it easy to get rid of spreadsheets and manual processes and efficiently manage risk and compliance both internally and for third-party providers.

Finish your audits in half the time and half the cost. Finally, affordable GRC for the rest of us.

Click here for more information »

Contact us at: Sales@KnowBe4.com, 855-KNOWBE4 (566-9234)

Additional Resources

- Osterman Research and Knowbe4, *The Critical Need to Improve Compliance Practices*
- *Costs of Non-Compliance with Privacy Laws*, September 2019
- CIOReview, *Enhancing Compliance Automation Efforts Step-by-Step*, Amy Matsuo, Principal, global leader for compliance transformation solutions, KPMG and Todd Semanco, partner, banking and consumer compliance risk, KPMG
- Shared Assessments and Protiviti, *2019 Vendor Risk Management Benchmark Study: Running Hard to Stay in Place*
- KnowBe4, *Improving Legal Compliance Through Security Awareness Training*
- KnowBe4’s *KCM GRC Platform*