4 Keys to Creating a Vendor Risk Management Program

ProcessUnity

ProcessUnity

4 Keys to Creating a Vendor Risk Management Program

What Is Vendor Risk Management?

It wasn't long ago—perhaps just five or ten years—that your company viewed third-party vendors as merely providers of goods and services to your business. The conventional wisdom back then characterized vendors (including consultants and contractors) as suppliers, not business partners; so their problems weren't your problems.

But that was then and this is now. Several influences have forced a change in how you look at vendors and the risks they might pose to your business.

Globalization has created a dependence on critical activities outsourced to an increasing number of partners and vendors; this in turn has fueled a dramatic rise in the third-party ecosystem. It's highly likely that your company now outsources significant aspects of its business to outside providers. Whether it's accepting orders over the Web, manufacturing various products or components, or delivering services across town or to far-flung markets, your company relies on other companies to fill important needs of one sort or another. In effect, this makes them extensions of your own company. What's more, in this age of globalization, your critical suppliers can be anywhere in the world, including "in the cloud."

Having a dependency on outsiders increases your company's vendor-related risk. Oftentimes, your vendors are provided access to your intellectual property or to sensitive customer information. With significant security compromises making headlines, it's no surprise that most organizations are now requiring vendors to abide by not only their internal standards, but also by industry and governmental regulations surrounding privacy and security.

This heightened regulatory environment is a major influence, designed to force companies like yours to assess and address internal and external risks. It is an effort to maintain stability and to protect customers and investors alike. Regulations such as Basel II, SarbanesOxley Act (SOX), the Payment Card Industry Data Security Standard (PCI DSS), the Health Information Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), Federal Financial Institutions Examination Council (FFIEC) guidelines and German Supply Chain Act (LkSG), among others , mandate that risk-management policies extend to third-party vendors, outsourcers, contractors and consultants. Third (and fourth) parties have the potential to insert risk into your environment because they are outside your direct sphere of control.

Good corporate governance—which can't be legislated—means you have an obligation to understand vendor risk and to actively take steps to mitigate the risk and its impact on your business. Simply put, you need a single, collective view of your vendor risk in order to manage it well and have a more stable and productive business ecosystem.

Why Assess Vendor Risk Management?

For most companies, regulatory requirements are the leading reason to conduct vendor risk management (VRM) assessments. External regulators as well as internal auditors are expecting that you thoroughly understand the range of risks inherent in doing business with outside organizations, and that you have taken measures to lessen the impact of those risks on your own business. Regulatory compliance is well and good, but there are additional motivations to assess third-party risk. One reason is to protect your company's brand and reputation from being damaged by another company's actions. Consider how Apple's reputation has been tainted by its ongoing relationship with Foxconn. The reputational damage began in 2010, when 18 assembly-line workers attempted suicide at the company's iPhone production plant, but the impact has continued in the face of questionable labor practices and increased media scrutiny. As recently as November 2022, the facility received global attention due to worker protests: in response to China's zero-Covid policy, workers were isolated inside dorms, where they faced limited access to food and medicine. For years, then, Apple's relationship with Foxconn has produced negative media attention and earned them a reputation for producing smartphones at a great cost to the people who assemble their products.

Looking Further Up The Supply Line

When we talk about third-party risk, we mean the companies that you do business with directly. But those companies also have vendors that become fourth parties to you, and they, too, can pose a potential risk. For example, you may have a partner whose IT systems are hosted in the cloud with a fourth party. This is becoming increasingly common. You need to understand how well-protected that cloud environment is. There could be yet another business hosted on that same cloud that is a major target for cyber attacks. A sustained attack could knock your vendor's business offline for a period of time.

How would your company be impacted if your partner's IT systems are down?

What measures can you take to mitigate that risk?

The more deeply you understand your partners' ways of business, the easier it will be for you to maintain quality of service (QoS). This includes both the level of service to you from your vendors, and to your customers from your company—especially when your vendors touch your customers directly; for example, contract personnel who provide delivery and installation on your behalf. Could their behavior reflect poorly on your company? You bet, because customers often don't see the distinction between your company and your contracted service providers.

What Is A Vendor Risk Management Program?

A vendor risk management program is a formal way to evaluate, track and measure third-party risk; to assess its impact on all aspects of your business; and to develop compensating controls or other forms of mitigation to lessen the impact on your business if something should happen. A program of this nature gives you consistency for managing your vendors and a way to share information about them within your organization. Whether your VRM program is manual or automated, homegrown or offtheshelf, the important thing is that it reflects and enforces your internal controls framework, ensures your compliance with governmentor industry regulations, and achieves consistency withall of your vendors.

Want A VRM Program That Works? Follow These Four Principles

Managing vendor risk is an ongoing process. As your company embarks on or continues with this process, you want to get the most benefit from the program and ensure that the information you learn is used organization-wide to make better decisions. Here are four basic principles that will help you develop a VRM program that works well for your organization:

1. Identify potential vendor risk
2. Develop effective strategies for addressing higher risk vendors
3. Align vendor control environments with your internal framework
4. Implement ongoing oversight utilizing metrics and external alerts

01. Identify potential vendor risks

Many companies that implement a VRM program wrongly assume they have to deeply assess every business partner. In fact, doing so can be a waste of time and money. Of the hundreds or even thousands of vendors you work with, only a small percentage may present a serious risk to your business, and these are the ones to evaluate thoroughly.

Some of your vendors deserve far more scrutiny than others because of the strategic role they play in your company's ability to generate revenue from your goods and services. Others may provide a minor service but have the potential to expose confidential information. Therefore, you want to categorize and prioritize your vendors and then focus your assessments on the risks that are germane to specific vendors and the services they provide. Consider which aspects of your business a vendor touches. IT systems? Critical or sensitive data? Business processes? Facilities? Manufacturing? What are your concerns in this area? What is your regulatory exposure? Is this a strategic vendor or a bit player?

For example, suppose you contract a company to accept electronic payments over the Web. This is a high-value partner as it collects revenue for your company and presents your brand to the world. This company touches your customers' highly sensitive credit card data. A breach of this data could be a financial and public relations nightmare for your company—even if you aren't directly responsible for the breach. Your risk assessment must include what measures the company has in place to secure this data. Furthermore, this company's Web applications might be hosted on yet another service provider's computer systems, dictating the need to expand your risk assessment to this fourth-party company.

Identifying when to assess a vendor is also key. When you start the assessment process early in the relationship, it will help to dismiss any company that has "issues" before you engage in a contractual relationship. For vendors with whom you currently do business, a suggested time to assess them would be prior to renewing the contracts. This will ensure you have time to engage with the vendor and ascertain that control and reliability are adequate for the services they are providing.

02. Develop effective strategies for addressing higher risk vendors

When you have a vendor that your VRM process has identified as presenting substantial risk and you are willing to accept this vendor as a business partner, you need strategies to work with the company in order to keep the vendor's issues from causing you harm. In order to effectively do so, you must consider the following:

- Know what aspect of your business you are trying to protect and focus on minimizing the risk in that area. Make risk mitigation part of the negotiation and contract service-level agreement (SLA).
- Work closely with the vendor to identify and resolve issues to lessen your risk.
- Assess the vendor prior to contract renewal or more frequently; conduct ad hoc reviews when concerns arise.
- Gather outside information about the vendor, such as from Dun & Bradstreet, to assess financial health. These services might advise you of issues that are affecting your partner's performance.
- Use metrics to measure the vendor's performance over the time of your relationship. This can show if the partner's service level is improving, holding steady or declining.
- Have a plan of what to do if a vendor exceeds your threshold for risk. You also should have plans for all vendors in the event they are put out of business for any reason, such as an act of nature or financial collapse.

03. Align vendor control environments with your internal framework

Your company already has a control environment to mitigate your internal risks—likely based on ISO, NIST, or PCI control sets or reflecting the COSO or COBIT risk/process frameworks. Now you must work with your vendor to assess the effectiveness of controls it has in place for the risks you've identified with that company. Realize that you can't get the same level of detail from a vendor as you do from your internal groups.

However, some service providers, including cloud service providers, will have an SSAE 16 SOC report, which provides a control benchmark to use when comparing outsourced service providers. Should your vendor not have an SOC report, your organization can stipulate the need for audits in your vendor agreement.

Regardless of how you gain insight into a vendor's internal control systems, you should perform a gap analysis of your controls versus the vendor's controls, and work together to close the gap and align the vendor's controls to your specific needs. These needs should be aligned with industry control standards and guidelines.

When determining vendor internal control requirements, you should recognize that no single standard or guideline is appropriate for every organization. A best practice is to identify services and capabilities of the vendor and map them to the relevant industry regulations and control standards. This effort can be helpful in meeting compliance goals.

04. Implement ongoing oversight utilizing metrics and external alerts

Once you've identified your key vendor risks, metrics are a way to measure actual performance against those risks. Set up metric exception levels and what risks are tied to it. For example, suppose you have a business process that relies heavily on contract workers. You expect some level of worker turnover, but lately the turnover rate has become excessively high. The exodus of workers not only affects your productivity, but it also exposes you to higher training costs for replacement workers and leads to a potential for data breaches by ex-workers who still have system access.

External alert services also can clue you in to potential problems, such as when a key vendor has an issue that may impact your business. Say your vendor is being acquired, or a major lawsuit has been filed against the company. An early alert gives you the opportunity to meet with your partner sooner rather than later to discuss the issue and develop a plan to minimize your risk.

When developing measurements, it's important to identify the business value that is intended to be gained with the function or capability being measured, and then define objective criteria that can be used to assess this value. This is important because subjective measures can be open to interpretation by the audience evaluating the metric. Some measures to consider include:

- Performance and SLA expectations
- Disruption in workflow based on vendor performance
- Expectation or vendor-issued warning that workflow may be disrupted for any reason
- Breach of the vendor network, systems or facilities
- Information/results on tests of internal security (physical or systems) controls
- Vendor (non) compliance with laws, rules, regulations, policies and procedures

Your Next Steps

Vendors provide value in the expertise and services they offer; however, it is imperative that companies maintain active oversight. As a manager of business risk, you must recognize that when a vendor performs a service or function on your behalf, your company bears the ultimate responsibility for minimizing business exposure and ensuring compliance.

Because varying levels of risk remain with the company that offers the product or service, a strong and comprehensive automated VRM program is necessary to truly understand and track the risks your vendors pose to your business interests. Once you thoroughly understand, measure and track your risks, you can develop strategies to mitigate them to protect your company from harm. With effective vendor risk management, your company can minimize the risk of less direct oversight or control and maximize the benefits gained through a well-managed vendor relationship.

Processunity & Vendor Risk Management

ProcessUnity is a leading provider of cloud-based applications for risk management and service delivery management. The company's software-as-a-service (SaaS) platform gives organizations the control to assess, measure, and mitigate risk and to ensure the optimal performance of key business processes. ProcessUnity for Vendor Risk Management helps companies effectively identify and mitigate risks posed by third-party service providers in critical risk areas such as information security, service delivery, supply chain processing, financial processing, reputation, and regulatory compliance. ProcessUnity provides organizations with clear visibility into the business impact of third-party risk via direct links from vendors and their services to specific business elements such as processes and lines of business. Powerful assessment tools enable evaluation of vendor performance based on customer defined criteria through automated, questionnaire-based self-assessments as well as through detailed audits of vendor controls. Flexible reports and dashboards enable ongoing monitoring of vendor ratings, assessment progress, and status of remediation activity. Learn more at http://www.processunity.com.

ProcessUnity

www.processunity.com

info@processunity.com

978.451.7655

Twitter: @processunity
LinkedIn: ProcessUnity

ProcessUnity
33 Bradford Street
Concord, MA 01742
United States

ProcessUnity

www.processunity.com

info@processunity.com

978.451.7655

Twitter: @processunity
LinkedIn: ProcessUnity

ProcessUnity
33 Bradford Street
Concord, MA 01742
United States

230606