Vendor Risk Assessment Best Practices

The vendor risk assessment is a very critical step in vetting and ongoing monitoring.

The assessment gives you a better understanding of the risk posed by each one of your vendor relationships.

Any third-party risk is also your risk. Common risks associated with third-party vendors range from everything to operational risk, to financial and reputational loss and compliance risk.

For instance, data shows third-party data breaches cost more than in-house breaches at $13 per compromised record.

Data breaches arising from vendor errors are common with 59% of those

surveyed reporting a third-party related data breach.

That said, you cannot completely eliminate all vendor risk.

However, vendor risk assessment allows you to manage the risk to minimize impact on your organization.

Take a look at these best practices for conducting your regular vendor risk assessment.

Best Practices for Vendor Risk Assessment

Compare Accounts Payment Department Lists to Your Vendor List

Pull a list from the accounts payable department and compare it to your vendor list.

This will ensure you have not overlooked any vendors when you are completing your risk assessments.

Segment Actively Managed Vendors into Groups

With your list from accounts payable in hand, sort the vendors into different groups based on their type.

For instance, marketing agencies, cloud storage providers, processors, etc. as you classify your 3rd party vendors, ask:

- Which suppliers are tied to your organization’s most critical business operations?

- Which suppliers have access to protected information? Do those vendors need access to that information?
- What does each vendor do?
- Who owns the vendor relationship?

To determine your critical vendors, ask yourself:

- Would any sudden or unexpected loss of this supplier cause a material disruption to the organization?
- Would that loss impact our customers?
- Would the time to recover be greater than a business day or 24 hours?

If you answer yes to any of these questions, you're dealing with a critical, or high-risk vendor.

Examine Business Impact and Regulatory Risks

A vendor's impact on the business determines if they are critical or non-critical to your organization.

Regulatory risk determines if the vendor is of low, moderate, or high risk. You need to understand both to provide vendors with both designations.

This can be tricky because in some cases, vendors may have experienced information security issues in the past but unless the vendor is regulated and has to report the data breach or other issue, you won't know this occurred.

A vendor may have experienced the data incident that doesn't rise to the level of a data breach and therefore won't need to report it so it's possible you lack the information to appropriately analyze the risk.

> *This step is important because not all of the vendors pose the same risk to your organization. Vendors that handle mission critical processes will be a bigger*

threat then smaller contractors who only work with a single department.

Keep a Standardized and Disciplined Approach

Your risk assessment process needs to be repeatable. It must be consistent both in content and in form. Deviation from the standard process could skew your assessment results.

Assess Supplier Relationships at the Product or Service Level

To thoroughly understand all risk posed, you must complete a risk assessment on each product or service the vendor offers instead of a single vendor risk assessment on an entire vendor relationship.

This can be particularly complex and time-consuming for vendors who supply the majority of your products or services. The more you rely on the vendor, the more time you need to spend with their risk assessment.

Determine Due Diligence Requirements for Mission Critical or High Risk Vendors

Vendor due-diligence refers to gaining assurance that a potential vendor or current vendor is ethical and financially stable.

It’s corporate structure is sound and you can rely on them to help your business as agreed upon in your contract terms.

You should use vendor due-diligence reports to assess potential vendors before hiring them to reduce risk to business operations and financial stability, but to

also reduce compliance risk and reputation risk.

This includes a security assessment to look at their IT security and determine their security risk, especially if they will have access to sensitive company or customer data.

Organizations who fail to carry out vendor due-diligence may suffer penalties or lawsuits if the vendor acts inappropriately or fails to keep up their end of the contract.

Due diligence is an important part of vendor management and when done right, can go a long way toward better third-party risk management. Taking time to research the company and learn more about their cybersecurity,

If a vendor is high risk for example, you may want to add additional contract considerations, more frequent monitoring, and more in-depth due diligence annually.

Evaluate Risk in the Vendor Selection Phase

Beyond being a continuous part of your ongoing monitoring, it is best to conduct a vendor risk assessment during the vendor vetting phase too, so you know you are selecting the best possible vendor at the time.

When you know their level of risk going into the relationship, you can watch for changes.

If you notice the vendor's risk rating is increasing over time, then you are better equipped to replace the vendor should you decide that it is necessary for risk management.

Remain Well-Versed in Regulatory Requirements

It’s important to stay on top of regulatory regulations so you can Implement new guidance into your vendor risk assessment as it is necessary.

Regulatory compliance is crucial for business continuity and to minimize risk.

Keep Stakeholders Informed

Always keep your senior management and board of directors informed. If you must make significant changes to the risk assessment, notify them.

Risk Rate All Vendors

Every supplier relationship should be risk rated. But, a full risk assessment template may not be required for all of them. This is dependent on the parameters of your vendor risk management program.

Your vendor risk assessment needs to go to all vendors in your supply It should address reputation, financials, governance and organizational structure as well as security controls and Technology.

Questions to include on your questionnaire may be:

- Do you have your own vendor risk management program in place?
- What is the chain of command within your organization and who is the main contact for the vendor risk management program?
- Are there any areas of compliance that you need to meet?
- Do you have a chief information security officer?
- How do you prioritize your organization’s most critical assets?

- Do you outsource any IT or IT security functions to third-party service providers? if so, who are they, what do they do, and what type of access do they have?
- How do you specifically protect your customer information?
- How do you manage remote access to your corporate Network?
- How do you monitor for an authorized personnel, connections, software, and devices?
- Describe the process you have in place to communicate to us any security incidents that may affect our data.
- Do you use automated tools that continuously monitor your system to ensure malicious software is not deployed?

Once you've determined the assessment form you'll use, provide it to all of your vendors to get the information you need to complete each vendor assessment.

Then, develop your plan and timeline for continuous monitoring.

What's your goal today?

1. Use PLANERGY to manage purchasing and accounts payable

We've helped save billions of dollars for our clients through better spend management, process automation in purchasing and finance, and reducing financial risks. To discover how we can help grow your business:

- Read our case studies, client success stories, and testimonials.
- Visit our "Solutions" page to see the areas of your business we can help improve to see if we're a good fit for each other.
- Learn about us, and our long history of helping companies just like yours.

Book a Live Demo

2. Download our guide “Preparing Your AP Department For The Future”

Download a free copy of our guide to future proofing your accounts payable department. You’ll also be subscribed to our email newsletter and notified about new articles or if have something interesting to share.

download a free copy of our guide

3. Learn best practices for purchasing, finance, and more

Browse hundreds of articles, containing an amazing number of useful tools, techniques, and best practices. Many readers tell us they would have paid consultants for the advice in these articles.

Related Posts