SUPPLY CHAIN

Procurify | Guide

How to Conduct a Vendor Risk Assessment in 8 Steps

Introduction

87 percent of organizations have had a disruptive incident with a third-party vendor within the past three years, according to a Deloitte report. What's more, 71 percent of supply chain leaders identify digital risk as the top priority when it comes to reducing third-party vulnerabilities.

Vendor risk management is a real concern in today's cloud-first, remote-friendly workplace. But for many, understanding and mitigating vendor risk is no easy feat. In fact, one-third (yes, one-third!) of organizations don't even know how many vendors have access to their systems.

Enter the vendor risk assessment.

In this guide, we'll talk you through the eight vital steps to conducting a vendor risk assessment so that you can help keep your organization safe and secure.

BEFORE WE BEGIN

What is a vendor risk assessment?

Understand what a vendor risk assessment is? Nice! Skip this section

A vendor risk assessment (also called a third-party risk assessment) is a process that helps you understand and identify the good vendors from the bad (and the ugly…). Quite simply, a risk assessment helps you evaluate the possible risks that come with working with a particular vendor.

When it comes to risk assessments, you need to approach them with the same mindset you do when going to the gym. It's important to conduct them regularly, for example, and every time you do, it's vital that you explore different areas and work a little harder so that you can guarantee results.

But, like the gym, there's a lot of techniques and equipment to consider, and in order to make some progress, you need to know a little about what you're doing.

Here are the eight steps you need to take to complete a successful vendor risk assessment.

Jump to a section

STEP 1

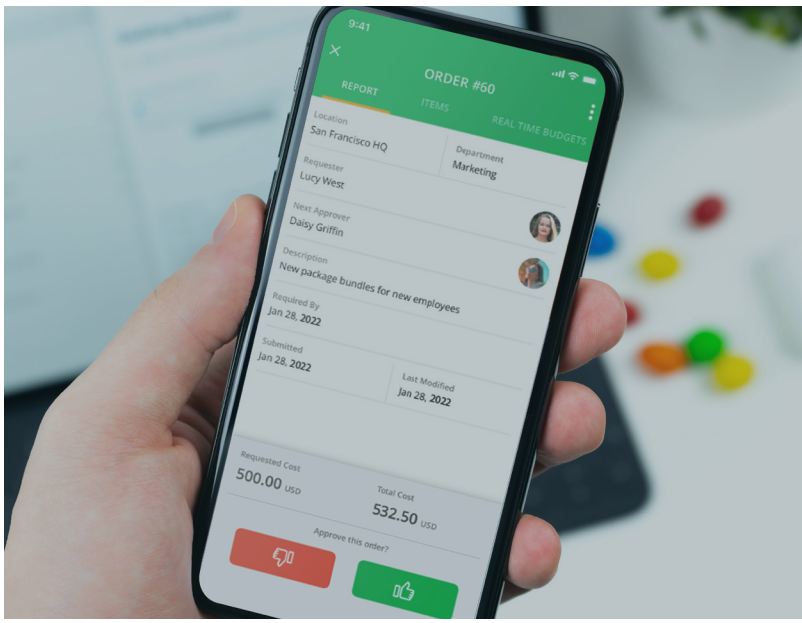
Understand the types of vendor risk

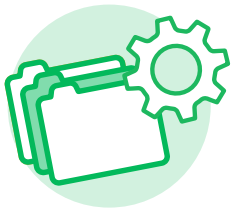
Risk comes in many forms. In some cases, organizations partner with third parties and risk losing financial control. In others, organizations risk facing penalties due to breaching compliance standards.

Here's a list of the most common types of vendor risk:

- **Strategic risk:** Your ideas are priceless, and some vendors will infiltrate your systems to steal them.
- **Financial risk:** Sometimes vendors will demand payment upfront and then conveniently 'go out of business'. Chances are you won't see that money again.
- **Compliance risk:** Industries like the biotechnology industry have to adhere to strict compliance standards. Do your third-parties meet these standards, too?
- **Geographic risk:** Working with vendors who are located in areas that are prone to natural disasters or political disruption is worth considering.
- **Technical risk:** If your potential vendor is still using Windows 98, it might be wise to keep them out of your systems for the sake of cybersecurity.
- **Subsequent risk:** Do your third parties use third parties, and will those third parties have access to your systems, too?
- **Replacement risk:** Are they a one-of-a-kind vendor that can't be replaced, or do you have a contingency plan in place should they go out of business?
- **Operational risk:** Is a potential vendor plagued by bureaucracy? Do they keep firing members of the leadership team?
- **Reputational risk:** How does it look to be partnering with a vendor? Are they a reputable organization?

Of course, the above depends on a variety of factors, like what industry you operate in and what exactly you offer to your community. But, understanding these types of risk will help you frame your risk assessment.





STEP 2

Build your risk assessment framework

Now that you have a handle on the different types of risk you face, it's time to build your assessment framework.

As you do this, prioritize which areas of risk to focus on first. For example, if you're an education institution, you might consider data privacy as your top priority given that you're handling student data. If you're a unique technology startup, you might choose to secure your intellectual property from third parties as your top priority.

STEP 3

Involve key team members early on

Vendor risk involves more than just yourself, and chances are, you'll need to lean on multiple experts across your organization to ensure you factor in every possible circumstance. Most important is your IT team, who will have the knowledge to help you identify digital risks that come with third-party vendors.

Be sure to establish a cross-functional committee that includes the key team members across your organization, and get these people involved in any documents you create from day one to ensure open and collaborative communication.

STEP 4

Break your risk assessment into two key areas

There are two types of risk assessments you should conduct when bringing on a new vendor:

1. A risk assessment for the organization itself
2. A risk assessment for the product or service you're purchasing from them

Risk is a very specific beast, and it extends beyond just working with a new organization. You need to consider whether or not each product you purchase is compliant with industry standards, whether or not it was manufactured in an ethical way, and whether any app you purchase is secure to use.

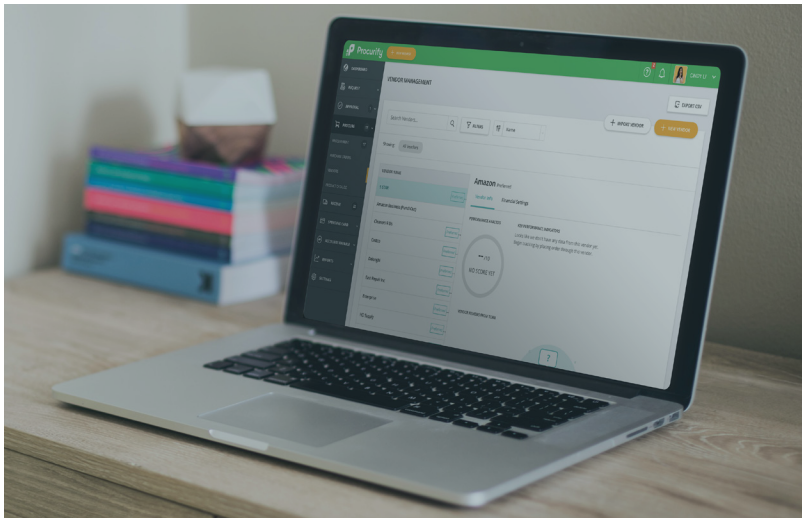
Diving deep into the specifics of what you're purchasing is as important as evaluating the risks of who you're purchasing from.

STEP 5

Risk assess every single vendor

If you use a specific vendor to purchase pencils so that your teams can write things down, that vendor must be risk assessed. If you place a coffee order every month so that there's a constant stream of caffeine at your workplace, that vendor also needs a risk assessment.

Risk assessments aren't reserved for high-priority vendors related to your product or service offering. Every single vendor that's in your systems must be scrutinized, no matter how small they are.



STEP 6

Categorize your vendors by risk level

After you've assessed every vendor, it's important to categorize them by risk. Are they a one-of-a-kind vendor who you can't afford to lose? Are they using up-to-date software that integrates with your internal systems? Are they at risk of going bankrupt or pivoting their product offering?

Of course, the list of questions to ask yourself is almost endless. Once you have a good understanding of each vendor's risk to your organization, give them a business impact score based on how vital they are to your own operations.

STEP 7

Put a risk assessment schedule in place

When you make the decision to work with a vendor, it's important to put together a regular plan of action that outlines how you're going to monitor risk moving forward. To do that, build a clear schedule that lets everyone know the frequency of your risk assessments, and more importantly, stick to it!

Consider things like:

- Regularly checking in on third-party process changes.
- An annual or bi-annual in-depth assessment to ensure you're up to date on third-party changes.
- Reviewing the smaller elements of your partnership with a third party, like external contractor access and data storage requirements.

To guarantee this, make sure to lean on your committee of cross-functional leaders!

STEP 8

Keep up to date with changes to laws and regulations

Depending on your industry, laws and regulations change often. As such, it's important to keep up to date with these changes to ensure you're working as safely as possible with your third parties.

This includes considering changes to privacy laws, tax concerns, employment and union laws, product standard requirements, and environmental considerations.

As this new information is published, it's important to adjust your risk assessment framework and factor this into every third-party risk assessment you run.

Let Procurify take care of your vendor management

The Procurify Platform has been named the best purchasing and vendor management software on the market in 2022 by Digital.com.

With our vendor management tool, you can:

- Conduct in-depth vendor performance scoring and measure vendors against metrics like speed, quality, accuracy, and price
- Quickly manage preferred catalog items and vendors
- Add and import purchasing items and details from vendor catalogs (including images)
- Manage vendor information and track fulfillment KPIs

Find out how you can work smarter with your vendors this year.

EXPLORE PROCURIFY


Procurify