

VENDOR MANAGEMENT?




Vendor management, as it's commonly called, or more accurately, third party risk management in recent years, is the process of fully identifying all of the significant vendors that aid in the delivery of a product or service to your company or to your consumers on behalf of your company.

That's quite a mouthful – let's break it down a bit:



IDENTIFY VENDORS

It's important that you throw a wide net and look at every vendor involved in servicing your company. That sounds easy, but it's a multi-step process:

-  **What is written in the scope of your program?**
-  **Who does accounts payable say you've paid for a service?**
-  **Which ones need to be actively managed** (hint: you're probably not too concerned with pizza deliveries or Staples orders)?

CONFIRM THE LIST IS ACCURATE

Check with your risk committee and senior leadership to be sure you haven't missed any and to be sure that there aren't ones they're actively terminating. Once you've been through this process once or twice, it's a whole lot easier.

CHECK THE LIST AGAINST YOUR PRIOR LIST AND YOUR PROGRAM SCOPE

Adjust as needed and be absolutely certain to note the reason (e.g., spend threshold, one-time use, special limited designation by board, etc.)

ASSEMBLE THE FACTS

Your due diligence should have a formal process, a timing that dictates a beginning, an end and a schedule for updating based on risk (or contract renewal in some cases). Make sure to be thorough and not just go through the motions but analyze the documents.

GO THROUGH A THOROUGH RISK ASSESSMENT PROCESS

Every actively managed vendor requires some level of review – overlooking one may mean overlooking a real risk (believe me, I'll bet Target wishes they'd done a more thorough risk assessment of the HVAC contractor that allowed the breach). We have lots of resources on that for your assistance.

COMMIT IT TO WRITING

Be certain you have adequate tracking of your contracts (and renewal dates and key terms) and be certain you have adequate reporting for your board to review.

CONCENTRATE FIRST ON YOUR CRITICAL AND / OR HIGH RISK THIRD PARTIES

Prioritize according to the level of risk – that's what risk based is all about and make sure you have identified steps to help control those risks in an effort to lower the exposure for your company.

DON'T FORGET FOURTH PARTIES

As you mature your process, you're going to need to dig a level deeper and look as well at subservice providers or ones that represent different levels of risk to your subsidiaries. We also call these fourth parties.

Looking at these vendors will likely be a joint effort between your vendor management team and the appropriate people at your third party (since they have the direct contractual relationship with the subservice provider) and at your subsidiary. In those cases, it's important that if you cannot do your own direct review of that subservice provider, your contracted third party provides you their own policies for doing so and then adequate evidence that they are routinely completing those activities.

Anywhere your consumer's information may go, you need to be digging in – we've seen this in multiple industries – no one is prone to a breach.



Vendor management is both a **science** and an **art** – you need to have a process and be ready to be creative when needed to protect your company.

See how Venminder can help you reduce your vendor management workload.

[DOWNLOAD NOW](#)