venminder

THE DIFFERENCES BETWEEN A HIGH RISK AND CRITICAL VENDOR

There's a different definition and, therefore, real differences between a **high risk vendor** and a **critical vendor**. This isn't something we've made up — this is something we've seen in best practices, heard at conferences, codified into programs at different organizations and executed pretty effectively.

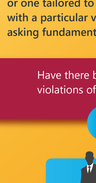
2 DIVISIONS OF RISKS

The differences between "HIGH RISK" and "CRITICAL" come down to two fundamental risks.

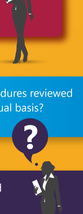
BUSINESS IMPACT RISK 01

The risk associated with whether you are so reliant on a third party, that if that third party were to suddenly disappear, it would cause a material disruption to your business. If you believe that is the case, then that is a Critical third party.

You may have a vendor who is CRITICAL BUT LOW RISK. Think of the phone company.



You could have a vendor who is NON CRITICAL BUT HIGH RISK. Think of the shred company.



Both can be replaced easily, but THEY ARE LITERALLY WALKING OUT THE DOOR WITH **YOUR** DATA!

REGULATORY RISK 02

Working your way through the various categories of risk laid out in the guidance. For example, OCC Bulletin 2013-29 and Bulletin 2017-7 identify numerous categories of risk you should consider.

Whether you use a standardized questionnaire or one tailored to the types of risks associated with a particular vendor, you should always be asking fundamental questions such as:

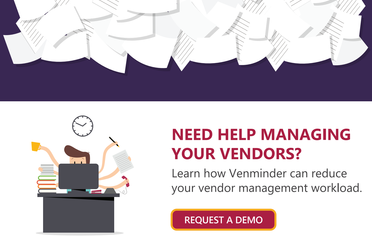
Have there been any reported/disclosed violations of law or regulatory guidance?

Are all policies and procedures reviewed and approved on an annual basis?

Are all materials, terms and conditions required to have your organization review and approve prior to distribution by the vendor?

Obviously, these will vary depending on whether it's your marketing company or your shred vendor, but you should develop a set of questions that help you fully discern the risk.

There are many categories of risk that may come into play, depending on the type of product or service. The OCC guidance, Bulletin 2013-29, lists a few, but you should consider if there are others in play as well.



The OCC Bulletin specifically identifies various risks:

- ⚠ Operational Risk
- ⚠ Compliance Risk
- ⚠ Reputation Risk
- ⚠ Strategic Risk
- ⚠ Credit Risk

However, you may very well find you need to think about:

- ⚠ Geographic Risk
- ⚠ Concentration Risk
- ⚠ Country Risk
- ⚠ Information Security Risk...

...just to name a few.

JUST TO RECAP
HERE ARE EXAMPLES OF HOW THIS WORKS

You could easily have a Critical third party who is Low risk.

Think of the phone company, if they fall within your scope.

You are absolutely reliant on them to be up and available and their disruption would disrupt your activities and impact your customers, but there is very low risk associated with them from a regulatory risk perspective.

Conversely, you could have a Non-Critical third party who is High risk.

Think of your shred vendor or your backup server provider.

You could likely do without them for a day or replace them in relatively short order, but they have unfettered access to all of your confidential information and your customer's data.

NEED HELP MANAGING YOUR VENDORS?

Learn how Venminder can reduce your vendor management workload.

REQUEST A DEMO

venminder
400 Ring Road, Suite 131, Elizabethtown, KY 42701 | (270) 506-5140
www.venminder.com

PRINTABLE VERSION