

WHY WE DO

Vendor Due Diligence

Due diligence is one of the most critical activities in third party risk management.

The information collected can truly make or break how you feel about a vendor and failing to do appropriate due diligence exposes your institution to incredible risk. The things you learn along the way should help you craft better ongoing monitoring, structure more accurate contracts and may even lead you to need to inform senior management and the board of major changes in the relationship.

3 Reasons **WHY** Due Diligence Is Completed on Vendors

1 LET'S START WITH THAT IT'S A REGULATORY EXPECTATION.
Articulated clearly by each of the major regulators and the FFIEC, due diligence must be conducted on all third parties to determine the level of risk associated with doing business with the vendor. Even if your institution isn't regulated by the Office of the Comptroller of the Currency (OCC), [Bulletins 2013-29](#) and [2017-7](#) are must-reads.

2 IT MAKES GOOD BUSINESS SENSE.
Due diligence findings can lead to walking away from a potential vendor relationship in some cases and, in other cases, lead to discovering some additional contractual issues that need to be addressed. It's important to document and address any gaps in the third party relationship not only to protect your institution, but also to protect your customers and their data.

3 YOU MAY FIND RISKY AREAS OF THE VENDOR RELATIONSHIP AND HAVE THE OPPORTUNITY TO FIX THEM.
It's important that we resist the temptation to make due diligence simply a checklist activity. Due diligence reviews of financials and SOC reports, for example, need to be thorough and not just a "check the box" exercise as each effort requires analysis and thorough documentation to truly protect your institution.

HOW Vendor Due Diligence Makes a Difference

The goal is to mitigate risk and protect the institution but exactly how does one do this? Let's take a look.

GATHER ALL NECESSARY INFORMATION
This must be timely and comprehensive and should closely match the nature of the product or service being outsourced.

REVIEW YOUR VENDOR'S FINANCIAL REPORT
This protects your institution by giving a clear understanding of the vendor's financial posture and ensures you have ample time to replace the vendor, if needed, prior to a decline in service levels or a sudden close of business.

REVIEW YOUR VENDOR'S SOC REPORT
This protects your institution by making you aware of the controls in place and ensures you understand next steps that must be taken to request that the vendor strengthen those controls to protect your institution from any risk presented.

REVIEW YOUR VENDOR'S BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN (BCP/DR)
This helps protect your institution from unexpected events the vendor may experience that may impact your business operations. It ensures the vendor's preparedness meets or exceeds your own plan before a disaster strikes.

REVIEW YOUR VENDOR'S CYBERSECURITY REPORT
This protects your institution from potential weaknesses in the vendor's cybersecurity posture and ensures you can effectively communicate with the vendor to request controls are strengthened if needed.

REVIEWING AND MAINTAINING ALL OTHER VENDOR DUE DILIGENCE
This protects your institution from increased risk and ensures you "know your vendor" and are prepared for the next examination.

Best Practices to Make the Task **LESS** Daunting

There are ways to save time and effort. Here are a few very important ones:

Re-evaluate your third party risk management program. Does your team take a **centralized, decentralized or hybrid approach** to managing the vendors? We recommend hybrid.

Outsource vendor due diligence to companies with the discipline and expertise, if needed.

Implement **software** solutions that make scheduling, organization and reminders more efficient as this can be a huge help.

Bonus: Not only do some companies tend to have the software, but they also tend to have experts on staff who are certified professionals and readily available to complete your due diligence reviews in order to produce a highly qualified work product.

When you understand why due diligence reviews are necessary and how they make a difference at your institution, it's much easier to see the increased benefits and make due diligence a priority.