How to Do Vendor Due Diligence

COLLECTION > REVIEW > DECISION

Due diligence should be risk-based and tailored to match the product or service provided by a third party.

It's important to do initial due diligence prior to signing a contract and then ongoing due diligence during the course of the relationship. Continue to stay abreast of regulatory expectations as this will help guide you through the process as well.

Medium Risk

All standard due diligence requirements plus...

- 3 Years Audited Financials *(if can't get, then credit report or annual report can help)*
- Insurance Certificates
- Applicable Compliance Policies
- Vendor's Third Party Management Practices
- SOC Report (with bridge letter, if needed)
- Reports of Internal and External Audits
- AML Policies (if applicable)
- Information Security Policy
- Record Retention/Data Destruction Policy
- Background Check Policy
- Hiring Practices

Low Risk

All standard due diligence requirements

High Risk

All standard due diligence requirements and the medium risk requirements plus...

- Policies and Procedures
- Biographies of Key Managers
- Logical Account Management Policy
- Data Classification and Handling Policy
- Incident Management Policy
- Business Continuity/Disaster Recovery Plans, Protocols and Results
- Penetration Testing Results
- Vulnerability Testing
- Network Diagram
- Data Flow Diagram *(including third and fourth party)*
- Record of Outages and SLA Violations *(usually a contractual obligation)*
- Complaint Escalation Procedure
- Potential Onsite Visit

Are they low, medium or high risk?
Here are lists to use as guidelines of what to collect based on regulatory risk impact. Keep in mind there can be some overlap of requirements from your previous step of criticality best practices as a vendor must have a business impact level AND regulatory risk level.

Here's the overall process of how to do due diligence.

1 Gather your vendor list

2 Do standard due diligence on all vendors

Standard due diligence includes, but is not limited to, these items as it's dependent on your organization's policy:

- ✓ Articles of Incorporation
- ✓ All physical locations *(but depends on if required by policy/program)*
- ✓ The address
- ✓ Any "doing business as" or all "also/previously known as" *(d/b/a, aka, pka)*
- ✓ Business license
- ✓ TAX ID
- ✓ Business type
- ✓ Website
- ✓ Ownership information
- ✓ State of Incorporation
- ✓ Reputational risk check *(Better Business Bureau and CFPB consumer complaint database)*
- ✓ OFAC/PEP Check
- ✓ Secretary of State Check
- ✓ Any specialized certification or licenses *(e.g. PCI certification, ISO certification, proof of admission to the bar for state practices)*
- ✓ Insurance information
- ✓ Certificate of Good Standing *(if required by policy/program)*
- ✓ Onsite tour or at minimum a picture of the facility *(especially for critical vendors)*

3 Additional due diligence is required based on the vendor type, criticality and risk level

Criticality level is determined by understanding the vendor's business impact to the organization.

Therefore, look to see which of your vendors are considered critical and non-critical.

If your vendor is **critical**, you should ensure that the vendor has all the relevant controls in place in order to limit any risks to your organization.

Critical vendors may impact your day to day operations and place you in operational, financial and reputational risk should they fail to perform.

If your vendor is **non-critical**, you should differentiate between non-critical vendors which are high risk and non-critical that are low risk. If the vendor is high risk and has access to non-public personal information (NPPI) but can be easily replaced, the level of oversight is similar to a critical vendor since the fall out for nonperformance is the same. The key difference is that the non-critical vendor can easily be replaced with another complementary vendor.

4 It's important to understand your vendor's regulatory risk impact

5 Keep in mind the frequency of due diligence

- You're likely to collect SOC reports, business continuity plans and disaster recovery plans on an annual basis. SSAE 18 reports are annual attestations, so you will also collect these yearly.
- Internal policies are typically a living, breathing document so these documents can change based on changes to regulations or internal best practices the firm is implementing. Request periodically on an as needed basis. It's unlikely you will need to ask for these more than annually unless something triggers a risk event.
- Publicly traded firms issue quarterly financials, so you could request these documents to be shared and reviewed as they occur. These are available online so it's important to set reminders to gather the information as released. If the firm is private, it's more likely that you'll request the financials on an annual basis.

6 Always document your attempts to collect the documentation from each vendor

You may not always be able to obtain the requested documentation, but you should note when you reached out, the request type and the number of attempts. Perhaps you can contractually commit the vendor to supply the document to avoid this.

7 After you have all documentation in hand, don't just file it all away!

Review everything and ensure there are no issues, questions and you truly have all you need.

8 Repeat this process for ongoing due diligence, especially when considering a renewal of a contract

The more critical the vendor is to your operation, the higher the frequency of doing ongoing due diligence. **Due diligence should be updated no less than annually to confirm the vendor still meets expectations.**

Why You Need to Do Due Diligence

- Performing due diligence **protects your organization** from unnecessary risk.
- It's a **regulatory expectation** and overall sound business practice.
- It provides a **baseline or standard of minimum requirements** needed in order to onboard a new vendor.

Remember, due diligence mitigates risk.

By reviewing your vendors, you catch errors, potential breaches and other major business impacting issues and can act upon those findings to prevent actual damage to you and your consumers.

Download free due diligence samples and see how Venminder can help reduce your workload.

DOWNLOAD NOW

What to Collect Based on Vendor Business Impact Risk

All standard due diligence, plus the following considerations:

Non-Critical

Attorneys and Title Agencies
Information Security information (if they do not have a policy, that is a huge exposure to risk)

Credit Reporting Agency Information Security, SSAE 18 reviews, Complaint Management Policy, training on Federal Consumer Protection Laws and Compliance Management System

Landscaper and Cleaning Services
General Liability Insurance and Hiring Policies

Landlord or Financial Facility
Financials, Hiring Policies and General Liability Insurance

Offsite Document Storage
Financials, Information Security, SSAE 18 and Disaster Recovery reviews

Shred Provider
Financials, Information Security, SSAE 18 and Policies and Procedures

Critical

Core Processor
Disaster Recovery Plan, Financials and Information Security reviews

Lending Platform
Disaster Recovery Plan, SSAE 18, Financials, Information Security reviews and Compliance Management System

Cloud Providers
Financials, Information Security, SSAE 18 and Disaster Recovery Reviews

Phone Company
Simply the Standard Due Diligence

* Note: For offshore vendors, consider their training, hiring practices, masking of offshore data and any GDPR requirements.

PRINTABLE VERSION

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