Due Diligence Checklist for Low, Moderate, and High-Risk Vendors

Due diligence should be risk-based and tailored to match the product or service provided by a third party **along with the level of risk**. With that as a backdrop, let's examine some common due diligence items you may want to gather based on the level of risk.

Due diligence is not a static, one-time event – it should be refreshed periodically or as key documents, such as financial statements, are updated.

Although we often refer to these items as a checklist, please be sure not to simply take a "checklist mentality" to them – **all documents should be reviewed for accuracy and adequacy**. In some cases, the results of that analysis may change your view of the risk represented or even require some additional contract provisions or additional monitoring.

venminder

BASELINE DUE DILIGENCE

First, there should be some baseline due diligence for all third parties. Yep, all of them that you're including in your third-party program.

> **Note**
> *We all have certain ones we deliberately exclude, perhaps based on a spend threshold, or because they represent no real risk at all – the office supply company is a good example.*

For all third parties that you're actively managing and new ones coming in the door, you should gather:

- [ ] Mutual Non-Disclosure Agreement (MNDA) or Confidentiality Agreement
- [ ] Basic Information (Full Legal Name, Address, All Physical Locations, Website URL)
- [ ] Any "doing business as" or "also/previously known as" (d/b/a, aka, pka)
- [ ] State of Incorporation
- [ ] Articles of Incorporation
- [ ] Business License
- [ ] Secretary of State Check
- [ ] OFAC/PEP checks
- [ ] Certificate of Good Standing
- [ ] Any specialized certifications or licenses (e.g. PCI certification, ISO certification, proof of admission to the bar for state practices)
- [ ] Tax ID
- [ ] Credit Report
- [ ] Dun & Bradstreet (D&B) Report
- [ ] Ownership structure and affiliated companies
- [ ] Vendor complaints research findings
- [ ] Vendor negative news search findings
- [ ] List of Subcontractors/Fourth Parties
- [ ] Picture or Google Map view of facility (if required)
- [ ] Reputational risk check (Better Business Bureau and CFPB consumer complaint database)

These are all important items so you know with whom you're doing business and can be certain you're not doing business with someone who could harm your reputation.

LOW RISK

All items of **BASELINE DUE DILIGENCE**

MODERATE RISK

All items for **LOW**
PLUS

- [ ] 3 years audited financials (if can't obtain, then a credit report or annual report can help)
- [ ] Insurance certificates
- [ ] Any 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

HIGH RISK

All items for **LOW** and **MODERATE** **PLUS**

- [ ] Policies and procedures
- [ ] Biographies of key senior management and owners of the organization
- [ ] Logical access 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 party/fourth party
- [ ] Record of outages and SLA violations (usually a contractual obligation)
- [ ] Potential on-site visit

ADDITIONAL DUE DILIGENCE

Depending on the type of product or service provided, you may need to do some additional due diligence. For example:

- [ ] If they'll be storing or processing credit card information, you need to be sure they're PCI compliant.
- [ ] If they require particular licensing, you should verify that they have the appropriate certifications in the right locations as well.

Any time that a certain piece of due diligence raises additional questions, be certain to ask for additional information as needed. If they can't readily provide it, carefully consider alternatives – perhaps a discussion with key management officials or even an on-site visit is in order.

Remember, due diligence is both a science and an art – you must follow a well-prescribed approach but be ready to get creative when needed.

Disclaimer: This is not a one-size-fits-all, and absolutely must work in conjunction with the product or service provided. Please make sure it's well-documented in your third-party risk management program. In addition, a document found in a different section could be a foundational document depending on the vendor relationship (e.g., SOC report). This is by no means an exhaustive list but rather a review of the most commonly obtained types of documents.

SAVE CHECKLIST **PRINT** CHECKLIST