Vendor Due Diligence **Checklist**

To both adequately prepare for regulatory examinations and maintain a healthy schedule of ongoing vendor management duties, it's critical your organization gathers all the necessary due diligence documents and specific data points from third-party vendors. The due diligence requirements will vary by type of third party, what sort of risk they represent and what you would reasonably expect a vendor to have, but here's a pretty good list of the items you should consider when performing your vendor due diligence. Remember, however, that vendor management is not just a checklist exercise – you should have an expert review each item for accuracy, timeliness and quality.

FOUNDATIONAL DOCUMENTS

- □ Mutual Non-Disclosure Agreement (MNDA) or Confidentiality Agreement
- □ Basic information (full legal name, address, all physical locations, website URL)
- □ Ownership structure and affiliated companies
- □ Tax ID
- □ State of Incorporation
- □ Articles of Incorporation
- □ Secretary of State Check
- □ Business license
- □ Certificate of Good Standing
- □ Credit report
- □ OFAC/PEP checks
- □ Any "doing business as" or "also/previously known as" (d/b/a, aka, pka)
- □ Dun & Bradstreet (D&B) report
- □ Vendor complaints research findings
- □ Vendor negative news search findings
- □ List of subcontractors/fourth parties
- □ Picture or Google map view of facility (if required)
- □ Conduct check of CFPB Complaint Database and/or Better Business Bureau rating

**Some of the other documents listed in this checklist may be a foundational document request, too (e.g., financials, SOC report, business continuity plan).*

FINANCIALS

- □ Audited financial statements/annual report (2-3 years; including income statement, balance sheet and cash flow statement)
- □ Audit letter/opinion
- □ Management discussion and analysis on financial performance
- □ Outstanding legal/litigation matters (as available)
- □ Ongoing mergers & acquisitions/corporate restructuring matters (as available)

INSURANCE

- □ General liability
- □ Cyber insurance
- □ Employee malfeasance
- □ Specific insurance standards required by business lines

DIAGRAMS

- □ Network diagram
- □ Data flow diagram, including any third party/fourth party
- □ Organization chart of affiliated companies and holding company
- □ Organization chart of staff
- □ IVR/call routing flows
- □ Service roadmap
- □ Application architecture

LICENSES OR PROFESSIONAL CERTIFICATIONS

- □ Any required licenses (e.g., state money transmitter license)
- □ Any required certifications (ISO, ITIL, NIST, HITRUST, FedRAMP, SIG, etc.)
- □ PCI certification/QSA letter
- □ Proof of admission to the bar for state practices

EDUCATION

- □ Biographies of key managers (if needed)
- □ Compliance education schedule
- □ Change management education schedule

EXAMINATIONS AND REPORTS

- □ Reports of internal and external audits
- □ Regulatory regional office record of audit reports (FI's must request directly)
- □ Information security penetration testing
- □ Vulnerability testing
- □ Business continuity plan (including disaster recovery and pandemic plans)
- □ Disaster recovery plan and testing
- □ SSAE 18, SOC 1, 2 or 3 and bridge letter, if needed

POLICIES AND PROCEDURES

- □ Compliance policies
- □ Anti-money laundering (AML) detection policies
- □ Change management policy
- □ Information security policy
- □ Business continuity plan (including disaster recovery and pandemic plans)
- □ Record retention/data destruction policy
- □ Hiring policies (drug testing, background check)
- □ Social media policy
- □ Vendor management policy
- □ Complaint management policy
- □ Service delivery policy

Download free sample assessments of vendor controls and see how Venminder can help reduce your third-party risk management workload.

SAVE CHECKLIST   PRINT CHECKLIST

venminder