

Model Vendor Due Diligence Checklist

These items will vary by type of third party and 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

- Full legal name
- Address
- All physical locations
- Website
- 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)
- Picture or Google map view of facility (if required)
- Conduct check of CFPB Complaint Database and/or Better Business Bureau rating

FINANCIALS

- Annual report (if publicly traded)
- 3 years audited financials
- Accountant's statement

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 and testing
- SSAE 18 SOC 1, 2 or 3 and bridge letter, if needed

LICENSES OR PROFESSIONAL CERTIFICATIONS

- Any required licenses (e.g., state money transmitter license)
- PCI certification/QSA letter
- ISO certification
- Proof of admission to the bar for state practices

INSURANCE

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

EDUCATION

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

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

POLICIES AND PROCEDURES

- Compliance policies
- AML detection policies
- ID Theft Red Flags policy
- Scripting policy (call centers)
- Change management policy
- Data protection/information security policy
- Business continuity plan (including pandemic policy)
- Record retention/data destruction policy
- Hiring policy
- Drug testing policy
- Background check policy
- Media policy
- Vendor management policy
- Complaint management policy

Download free due diligence samples and see how Venminder is helping institutions reduce their workload.

