

Third-Party Risk Management Checklist



Vendor Management Governance Documentation

Below are examples of governance documentation.

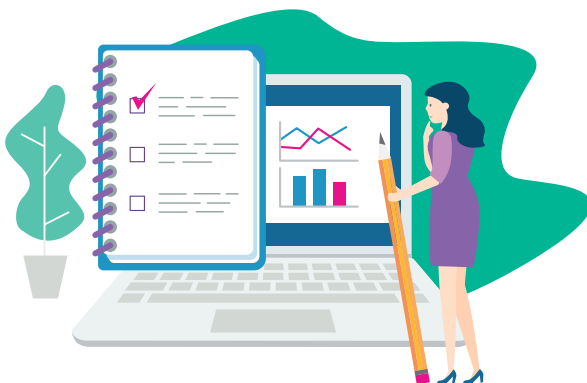
- Create or update a vendor management policy
- Create or update a vendor management program
- Create or update vendor management procedures

Foundational Documents/Baseline Due Diligence

These should be used from the vetting process through ongoing oversight and monitoring.

- Mutual Non-Disclosure Agreement (MNDA) or Confidentiality Agreement
- Basic Information (full legal name, address, all physical locations, website URL)
- Biographies of key managers and ownership (if needed)
- Ownership structure and affiliated companies
- Tax ID (can be found in the W9)
- State of Incorporation
- Certificate 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 critical or pertinent subcontractors / fourth parties
- Picture or 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).*



Due Diligence Often Required (in addition to foundational/baseline requirements)

These should be used from the vetting process through ongoing oversight and monitoring.

FINANCIALS

- Annual report aka 10-K (if publicly traded)
- 3 years audited financials
- Accountant's statement

EXAMINATIONS AND REPORTS

- External audit reports
- Regulatory regional office record of audit reports (FI's must request directly)
- Penetration testing
- Business continuity testing results
- Disaster recovery testing results
- SSAE 18, SOC 1, 2 or 3 and bridge letter

LICENSES OR CERTIFICATIONS

- Any required licenses (e.g., state money transmitter license)
- PCI Attestation of Compliance (AoC)
- ISO certification(s)
- NIST certification
- Professional certifications (CISSP, CISA, CRISC, CPA, etc.)

INSURANCE

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

INTERNAL EDUCATION

- 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
- Interactive Voice Response (IVR)/call routing flows

SLAs

- Provide record of outages and SLA violations (usually a contractual obligation)

SITE VISITS

The following may need to occur as part of your due diligence.

- Office walk through
- Data center walk through
- On-site documentation review

POLICIES AND PLANS

- Compliance policies
- Change management policy
- Information security policy
- Business continuity policy (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
- Access management policy

**The above is a list of the due diligence requirements we often see. However, due diligence requirements are based on the organization's policy and the vendor relationship's criticality and risk level to the organization.*

Risk Assessments

- Determine the vendor's criticality and inherent risk level
- Determine the residual risk level (after due diligence and inherent assessment are completed)

Contracts

Provisions to Include:

- Scope of service
- Rights/responsibilities of the parties
- Pricing methods
- Term/renewals/termination
- Performance standards
- Liability
- Indemnification
- Proprietary information
- Security and confidentiality
- Internal controls
- Reports
- Business Continuity
- Subcontracting
- Compliance with applicable laws and regulatory expectations
- Right to Audit

Contract Management

- Internal planning (know who is involved in the process)
- Negotiation/Creating/Drafting (know who is responsible)
- Approving/Executing (know who is authorized)
- Storing (central repository with tracking of significant dates)
- Managing (e.g., service delivery, performance, ongoing relationship)

Reporting

It's encouraged to provide reports on a regular, recurring basis to senior management, the board and your compliance and audit committees. A typical report contains the following with a page dedicated to each topic.

- Cover page with title and your organization's information
- Overall inventory (e.g., actively managed vendors, percentages of critical and on-critical vendors, etc.)
- New regulatory requirements (e.g., any that require changes to governance documents)
- Due diligence and vendor selection (e.g., status of current and ongoing vendor selection processes)
- Risk assessments (e.g., number of vendors with risk assessments completed, significant changes)
- Vendor risk issues (e.g., concerns with a contract, vendor isn't meeting SLA performance)
- Reporting timeline (e.g., timeline of the reports and meetings for the lines of business)
- Industry highlights (e.g., big news headlines like vendor announcements, vendor data breaches)
- Closing to wrap up by providing your contact information

Audit

How To – From Start to End

- Review the audit notification
- Review talking points provided by the auditors
- Review the plan (e.g., opening meeting, periodic updates, closing)
- Determine where the auditors will work
- Determine who the auditors may ask questions
- Establish a single point of contact
- Ensure your work product matches what is outlined in your program
- Create or update the vendor management governance documents
- Review your vendor list (be prepared to discuss the different vendor types)
- Review the document request lists
- Fully understand the scope of vendor monitoring practices
- Review your prior examination report for unaddressed items
- Address any prior examination items that have been missed
- Compare the prior examination to the new notice for changes in scope
- Communicate with your team regarding expectations
- Clarify any potential concerns or why you've done something a particular way, if needed
- Reciprocate auditor feedback
- Keep record of what you've provided
- Create an audit tracker (with findings, management's response, action items)

Download free sample assessments

of vendor controls and see how Venminder can help you reduce your third-party risk management workload.



SAVE CHECKLIST

PRINT CHECKLIST