Third-Party Risk Management **Checklist**

venminder

Vendor Management Governance Documentation

Below are examples of governance documentation to be created or updated:

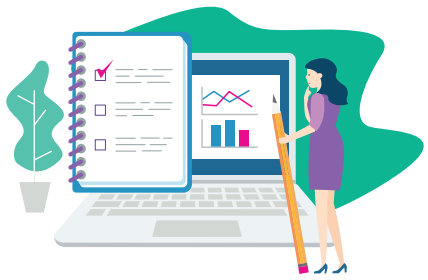
- [ ] Vendor management policy (requirements and responsibilities)
- [ ] Vendor management program (how policy is executed)
- [ ] Vendor management procedures (steps/directions to accomplish policy)

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/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 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 also be a foundational document request (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

- [ ] 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)

EXAMINATIONS AND REPORT

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

LICENSES AND CERITIFICATIONS

- [ ] 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
- [ ] Service roadmap
- [ ] Application architecture

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

- [ ] Anti-money laundering (AML) detection policies
- [ ] 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
- [ ] Privacy policy
- [ ] Service delivery policy

**The above is a list of common due diligence requirements we often see and should only be used as a reference. Specific due diligence requirements should be based on your organization's policy and the vendor relationship's criticality and risk level.*

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

- [ ] Person(s) involved in internal planning
- [ ] Person(s) responsible for negotiation/creating/drafting
- [ ] Person(s) authorized for approving/executing
- [ ] Storing (central repository with tracking of significant dates)
- [ ] Managing (e.g., service delivery, performance, ongoing relationship)

Reporting

It's recommended 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:

- [ ] Executive summary providing reporting highlights and any actions or decisions requested
- [ ] Overall inventory (e.g., actively managed vendors, percentages of critical and non-critical vendors) with trends showing increase/decrease over same period previous year
- [ ] 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

Here's the how-to from start to finish:

- [ ] Review the audit notification
- [ ] Look over talking points provided by the auditors
- [ ] Evaluate the plan (e.g., opening meeting, periodic updates, closing)
- [ ] Determine where the auditors will work
- [ ] Decide who will answer the auditors' 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
- [ ] Identify any potential concerns or clarify 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)