Aavenir



Vendor Risk Management

Checklist

www.aavenir.com contact@aavenir.com

Please address each question from the sections & mention your answer in the box.

Vendor Management Program Documentation

- [x] Create or update a vendor management policy
- [x] Create or update a vendor management program
- [ ] Create or update vendor management procedures

Baseline Due Dilligence

- [ ] 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)
- [ ] Ownership structure and affiliated companies
- [ ] Tax ID
- [ ] State of Incorporation
- [ ] Articles of Incorporation
- [ ] Business license
- [ ] Picture or Google map view of facility (if required)
- [ ] List of subcontractors / fourth parties
- [ ] Credit report

Vendor Risk Assessment

- [x] Before you can begin evaluating vendors, you need to know all of the types of risk you could protect before entering into a business agreement.
- [ ] Strategy risk : Trade secrets, ideas or intellectual property
- [ ] Financial risk : Financial Stability
- [ ] Compliance risk : Follow relevant laws and regulations

- [ ] Geographic risk: Operate in a risky location (e.g. prone to natural disasters, politically unstable)
- [ ] Technical risk: IT and data management processes and infrastructure
- [ ] Subsequential risk: Use of third parties for any of their processes
- [ ] Resource risk: Availability for adequate resources
- [ ] Replacement risk: Ease of replacement if vendor ceased operations
- [ ] Operational risk: Following Day-to-day policies and procedures
- [ ] Reputational risk : Internally and externally

Financials

- [ ] Annual report & Auditor's Report
- [ ] 3 years audited financials
- [ ] Accountant's statement
- [ ] Financial Statements- Balance sheet, income statement and a statement of cash flows4
- [ ] Notes to the Financial Statement-v

Examination & Reports

- [ ] Reports of internal and external audits
- [ ] Information security penetration testing
- [ ] Vulnerability testing
- [ ] Business continuity plan and testing
- [ ] Disaster recovery plan and testing
- [ ] Can the system document results in a risk assessment report ?

Licenses or Professional Certifications

- [ ] Any required licenses (e.g., state money transmitter license)
- [ ] Proof of admission to the bar for state practices
- [ ] Operating system licenses

- [ ] Business continuity plan and testing
- [ ] On-premise licenses to public cloud

Insurance

- [ ] General liability
- [ ] Cyber insurance
- [ ] Employment Practices Liability
- [ ] Specific insurance standards required by business linesV
- [ ] Directors & Officers Liability
- [ ] Financial Institution Bond
- [ ] Fiduciary Liability
- [ ] Commercial Property

Education

- [ ] Biographies of key managers and ownership (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
- [ ] Call routing flows

SLAs

- [ ] Record of outages and SLA violations (usually a contractual obligation)

Site Visits

- [ ] Potential on-site visit, if needed

Policies & Procedures

- [ ] Compliance policies
- [ ] 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
- [ ] Logical account management policy
- [ ] Plans, protocols and results

Risk Assessments

- [ ] Determine business impact risk rating (critical or non-critical)
- [ ] Determine regulatory risk rating (typically low, medium or high risk based on categories of risk such as strategic, reputation, operational, etc.)

Contract

- [ ] Provisions to Include:
- [ ] Scope of service
- [ ] Rights/responsibilities of the parties
- [ ] Pricing methodsv

- [ ] Term/renewals/termination
- [ ] Performance standards
- [ ] Liability
- [ ] IndemnificationProprietary information
- [ ] Security and confidentiality
- [ ] Reports
- [ ] Internal controls
- [ ] 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 total inventory of actively managed third party vendors
- [ ] Overall inventory of third party vendors
- [ ] Overall status of assessing risk (e.g., perhaps a pie chart showing how many critical and non-critical or high, medium and low-risk third party vendors)
- [ ] 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 total inventory of actively managed third party vendors
- [ ] Overall inventory of third party vendors
- [ ] Overall status of assessing risk (e.g., perhaps a pie chart showing how many critical and non-critical or high, medium and low-risk third party vendors)
- [ ] Due diligence (e.g., how many documents, upcoming due diligence and any overdue or missing items)
- [ ] Ongoing monitoring activities (e.g., what your team is doing to meet this critical expectation)
- [ ] Contracts (e.g., upcoming renewals or terminations, any notable problems with critical or high-risk third party vendors)
- [ ] Any major changes with high-risk and/or critical third party vendors
- [ ] A calendar showing upcoming updates to various committees, helping to demonstrate management is adequately informed in an ongoing manner

Audit

- [ ] How To – From Start to End
- [ ] Notify senior management and the board
- [ ] Review the audit notification
- [ ] Prepare talking points
- [ ] Plan (e.g., opening meeting, periodic updates, closing)
- [ ] Determine who the auditors may ask questions
- [ ] Create or update the vendor management policy, program and procedures
- [ ] 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
- [ ] Ensure your work product matches what is outlined in your program

About Us

Aavenir

Aavenir revolutionizes age-old procurement processes with AI-enabled Source-to-Pay solutions including RFP-flow, Contractflow, Obligationflow, and Invoiceflow. Built on ServiceNow, Aavenir solutions streamline procurement, legal, and accounts payable work processes using the latest technologies such as AI, ML, and NLP to eliminate manual work, accelerate cycle time, and reduce dependency by offering smart suggestions based on historical data. For more information, please visit www.aavenir.com

