Due Diligence Checklist

For Low, Moderate, and High-Risk Vendors

A Member Firm of Andersen Global

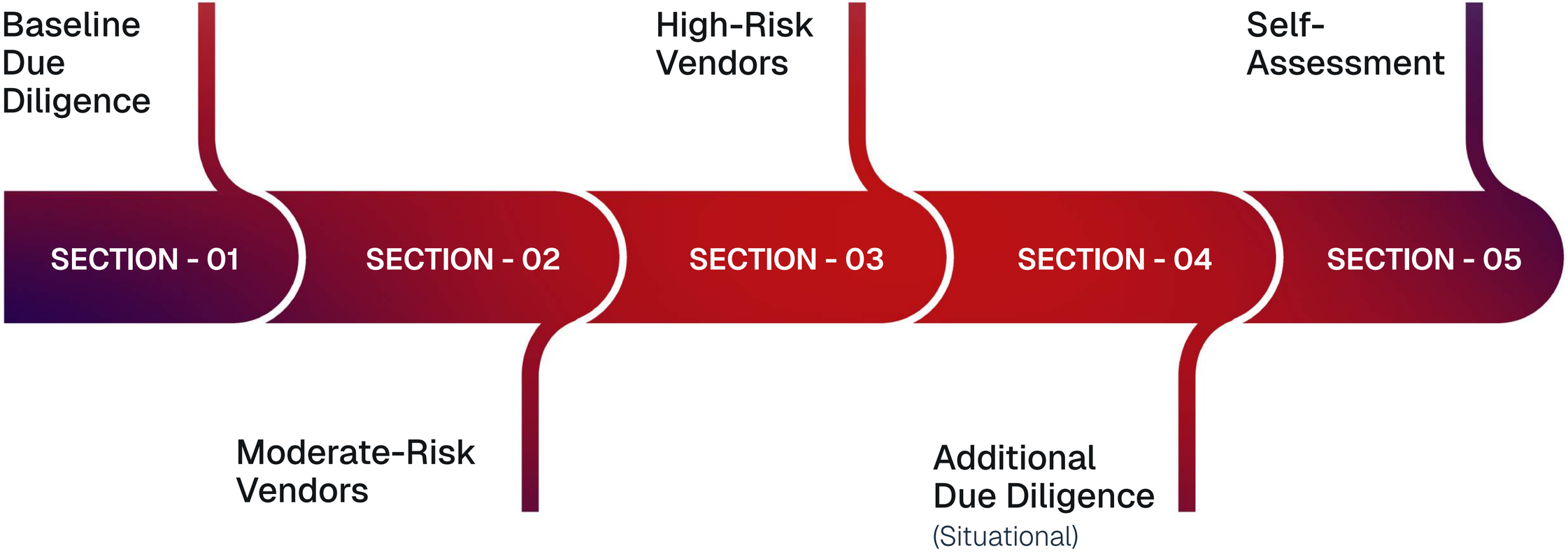
Introduction

Due diligence is not a one-time task. It should be reviewed periodically and adapted to reflect the nature of the vendor relationship and the level of risk involved.

The purpose of this checklist is to provide a clear, tiered approach to vendor due diligence, starting from basic requirements applicable to all vendors and extending to deeper checks for higher-risk engagements.

Note

This checklist should not be used in a mechanical, checklist-only manner. Every document must be carefully reviewed for relevance, accuracy, and completeness. Some findings may warrant deeper inquiries or changes to contractual terms.


Baseline Due Diligence
High-Risk Vendors
Self-Assessment
SECTION - 01
SECTION - 02
SECTION - 03
SECTION - 04
SECTION - 05
Moderate-Risk Vendors
Additional Due Diligence
(Situational)

Section 01

Baseline Due Diligence

Applicable to all vendors under active management

- [ ] Mutual Non-Disclosure Agreement (MNDA) or Confidentiality Agreement
- [ ] Basic Vendor Information:
  - [ ] Full Legal Name
  - [ ] Registered Address
  - [ ] Physical Locations
  - [ ] Website URL
- [ ] Any aliases: doing business as (d/b/a), also known as (aka), previously known as (pka)
- [ ] State of Incorporation
- [ ] Articles of Incorporation
- [ ] Business License
- [ ] Secretary of State verification
- [ ] OFAC / PEP screening
- [ ] Certificate of Good Standing
- [ ] Relevant certifications or licenses (e.g., ISO, PCI DSS, Bar Admission)
- [ ] Tax Identification Number
- [ ] Credit Report
- [ ] Dun & Bradstreet (D&B) Report
- [ ] Ownership structure and associated entities
- [ ] Vendor complaint history
- [ ] Negative media or regulatory search results
- [ ] Subcontractor and fourth-party disclosures Facility location (photos or map view, if needed)
- [ ] Reputational checks (e.g., BBB, CFPB complaint databases)

Section 02

Moderate-Risk Vendors

Includes all Baseline requirements plus the following

- [ ] Audited financial statements for the past 3 years (If unavailable, a credit report or published annual report may suffice)
- [ ] Insurance certificates
- [ ] Compliance-related policies (as applicable)
- [ ] Overview of the vendor's third-party/ vendor management practices
- [ ] SOC 1 / SOC 2 report (with bridge letter, if applicable)
- [ ] Internal and external audit reports
- [ ] Anti-Money Laundering (AML) policy (where applicable)
- [ ] Information security policy
- [ ] Data retention and destruction policy
- [ ] Background check policy
- [ ] Hiring and onboarding practices

Section 03

High-Risk Vendors

Includes all Baseline and Moderate requirements plus the following

- [ ] Complete documentation of internal policies and procedures
- [ ] Executive bios and ownership details
- [ ] Logical access controls and authorization protocols
- [ ] Data classification and handling policy
- [ ] Incident management and response procedures
- [ ] Business continuity and disaster recovery plans, including test results or reports
- [ ] Penetration testing results
- [ ] Vulnerability assessment reports
- [ ] Network architecture diagram
- [ ] Data flow diagram (including third- and fourth-party involvement)
- [ ] Records of service outages and SLA violations
- [ ] On-site assessment or visit (if appropriate and feasible)

Section 04

Additional Due Diligence (Situational)

Depending on the service or industry, further checks may be necessary

- [ ] If handling credit card data: confirm PCI DSS compliance.
- [ ] If regulated by local or international authorities: confirm valid licensing in relevant jurisdictions.
- [ ] If due diligence raises additional concerns: request clarifications or direct interaction with senior management.
- [ ] For high-impact or business-critical vendors: consider conducting a site audit or in-person review.

Section 05

Self-Assessment

Use this as a quick reference to evaluate the thoroughness of your review process.

Total number of checklist items	Number of checks completed
48	_____

Completion Rate

$$\frac{\text{Number of checks completed}}{48} \times 100$$

90% – 100%
Safe

The vendor has met nearly all requirements. Risks are minimal and documentation appears thorough. Suitable for onboarding or renewal without further escalation.

75% – 89%
Acceptable
(Needs Review)

Most checks are in place, but there are a few gaps. Further review or limited follow-up is recommended, especially for medium or high-risk vendors.

60% – 74%
Caution

Significant parts of the due diligence are incomplete. Proceeding without additional review could expose the company to operational, regulatory, or reputational risk.

40% – 59%
At Risk

Less than half of the critical checks are completed. Vendor approval should be put on hold. Immediate attention is required before moving forward.

Below 40%
Critical

Due diligence is insufficient. High likelihood of risk exposure. Vendors should not be onboarded or renewed until major gaps are resolved.

This checklist is a guide — not a one-size-fits-all document. Due diligence should always align with the risk, context, and services provided. Ensure your vendor assessments are part of a broader risk management process and that all findings are documented in your third-party governance framework.

We help businesses set up clear vendor risk frameworks based on the nature of services.

Our Expert team assists in reviewing documents, checking compliance, and identifying potential gaps, Supports detailed assessments for high-risk vendors and ongoing third-party reviews.

A Member Firm of Andersen Global

www.intuitconsultancy.com