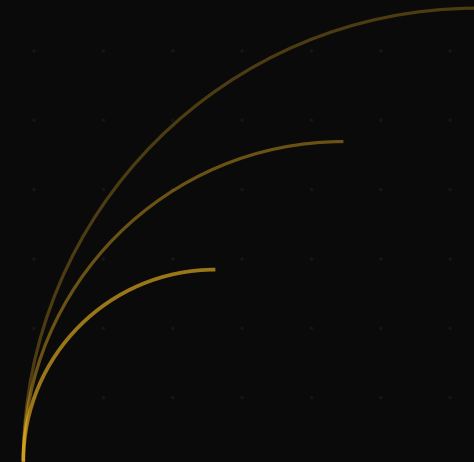


PROCUREMENT, SECURITY, AND RISK

Vendor due diligence checklist

A buyer's due-diligence checklist across security, compliance, financial stability, data handling, references, and concentration risk - before you sign.



WHAT'S INSIDE

4 steps in this guide

- 01 Security & data
- 02 Compliance & legal
- 03 Financial & operational stability
- 04 Concentration & exit risk

Vendor due diligence is the practice of verifying - before you commit - that a vendor won't introduce risk you can't manage.

01

Security & data

Verify controls against your obligations, not just certificates.

- Where is data hosted and processed; is it encrypted at rest and in transit?
- Can the vendor map controls to your specific obligations (SOC 2, ISO 27001, HIPAA, GDPR)?
- What is the data-return format, cost, and timeline on exit?

02

Compliance & legal

Confirm the paper matches the pitch.

- Are sub-processors disclosed, and is there advance notice of changes?
- What do the liability cap, carve-outs, and indemnities actually cover?

03

Financial & operational stability

A cheaper vendor that fails is the most expensive option.

- Is the vendor financially stable; what's the funding/ownership picture?
- What is the support model, and who delivers - named staff or a pool?

04

Concentration & exit risk

The most overlooked dimension.

- How hard and expensive would it be to replace this vendor if they failed, hiked prices, or were acquired?
- What's the realistic switching cost at years 3, 5, and 7?

PUT THIS TO WORK

Walk into every evaluation with the vendor's own playbook.

- A vendor-proof scope, issued before any proposal
- Gap analysis scoring every proposal against your scope
- A risk-weighted interrogation kit for the vendor meeting
- Scope-drift detection across proposal versions

Start free at benchsideai.com

Your first project is free. No card required.

