



AI VENDOR VETTING CHECKLIST

WHAT TO ASK BEFORE YOU BUY

3rd Element Consulting

Before You Buy

AI vendors are easy to find right now and hard to tell apart. This checklist is the same due-diligence framework used to vet AI vendors from the buyer's side: not marketing claims, but the specific questions that tell you whether there's a real, stable product and team behind what's being sold.

Work through each section before signing a contract. If a vendor can't answer a question plainly, or gets defensive, that reaction is itself useful information.

VENDOR STABILITY & SUPPORT

- ☐ How long has the vendor been in business, and how long specifically with this AI product?
- ☐ Can they provide references from businesses your size, not just enterprise logos?
- ☐ What's their support structure: real hours, a real escalation path, or a ticket into a queue?
- ☐ Is the company funded to keep operating, or is a sale or shutdown a real near-term risk? What happens to your data if it is?

WHO'S ACTUALLY BUILDING THIS

- ☐ Does the vendor have real engineers on staff who built this, or is it a small team that bolted together a few existing AI tools and put a new interface on top?
- ☐ Is development onshore, offshore, or outsourced to contractors? Not automatically a problem either way, but they should tell you plainly, not dodge the question.
- ☐ How many people actually work there, and how many touch the product versus sell it? A five-person company that's mostly sales and one contractor building the product is a different risk than a real engineering team.
- ☐ Was this built the way software used to be built, or assembled quickly with AI coding tools and shipped without real testing, security review, or a second engineer checking the work? Ask directly. A vendor that can't answer, or gets defensive, is telling you something.
- ☐ How many other businesses like yours have they actually implemented this for? Not "customers," implementations. Plenty of vendors claiming AI capability have done this zero times for a real client.
- ☐ Ask them to walk through their own architecture, even roughly. If they can't sketch how their own product works, that's the answer.

HOW THE AI ACTUALLY WORKS

- ☐ Is the model proprietary, open-source, or a wrapper around a third-party model (like OpenAI or Anthropic)?
- ☐ If it calls an outside AI model behind the scenes, what data gets sent there, and is it anonymized first?
- ☐ Is there a human reviewing or approving outputs before they reach you or your customers, or is it fully automated?

DATA SECURITY & PRIVACY

- ☐ Is data encrypted at rest and in transit?
- ☐ Is your data used to train their model, or kept separate? Get this in writing, not a verbal assurance.
- ☐ Where is your data stored, and does that matter for your compliance requirements (HIPAA, GDPR, CCPA)?
- ☐ What's their data retention and deletion policy once you stop using the tool?
- ☐ Will they sign a Data Processing Agreement?

COMPLIANCE

- ☐ Do they carry the certifications relevant to your industry (HIPAA, SOC 2, GDPR, CCPA)?
- ☐ Who's liable if the AI makes a mistake that costs your business money or damages a client relationship?
- ☐ Do they disclose subcontractors or other vendors who touch your data?

INCIDENT RESPONSE

- ☐ Is there a documented incident response plan, and will they share it?
- ☐ What are the actual notification timelines if something goes wrong?
- ☐ Do they have a track record of past incidents, and how they handled them?

CONTRACT & EXIT TERMS

- ☐ What does it actually cost, all-in: licensing, setup, support, not just the sticker price?
- ☐ Can you get your data out if you leave, in a usable format?
- ☐ What's the real length of the contract, and what does renewal look like?



NEXT STEP

If you'd like a second set of eyes on a specific vendor's answers, or help building AI use into your business safely from the start, 3rd Element Consulting [can walk through this with you](#).