

How to vet an AI agency

Check delivery evidence, data handling, staff and acceptance terms before you hire.

Updated October 29, 2026

Start with the business task. State who does it today, what fails and what evidence would justify a change. A strong supplier can explain when ordinary software is enough.

Ask for evidence you can inspect

Request a relevant project example. Ask what the team built, what the client supplied and what changed after launch. A logo wall does not answer these questions. Seek a reference who can discuss handover, missed assumptions and support. Respect client confidentiality; ask for a redacted test report where a live demonstration is not possible.

Meet the people who will do the work. Confirm the delivery lead, data lead and support owner. Ask which work goes to subcontractors and where data is processed. Put substitutions and approvals in the contract.

Test before you expand

Provide a controlled sample with permission to use it. Agree on a baseline and a test set that the supplier cannot tune against during delivery. Include difficult inputs, missing information and attempts to bypass permissions. Record errors by impact. A polished demo on selected inputs is weak evidence.

The NIST AI Risk Management Framework treats risk management as an ongoing activity. Use it to structure the review of context, measurement and response. It is not proof that a vendor is certified.

Contract for an exit

Ask for source access, deployment instructions, account ownership, data export and deletion records. Define who can approve production access. Tie payment to accepted deliverables. State the process for scope changes and failed acceptance tests. Keep infrastructure accounts under your control where practical.

Document unresolved risks before you choose. If a supplier refuses to explain dependencies or data flows, pause the purchase until you understand the consequence.

Sources

- [NIST, AI Risk Management Framework](#). Public page fetched 2026-10-29.
- [NCSC, Guidelines for secure AI system development](#). Public page fetched 2026-10-29.

Frequently asked questions

Is this a supplier recommendation?

No. Use this guide to prepare a brief and check the supplier evidence yourself.