

12 questions your AI vendor can't answer

A model-risk evaluation checklist

Use this on any vendor. None of these are trick questions: a serious supplier answers them quickly and specifically, and a demo-stage one gets vague.

Watch for the shape of the answer as much as the content. Specifics, numbers and a willingness to say 'we don't do that' are good signs. Deflection to a case study is not.

Data and boundaries

- ☐ 1. Where does our data physically go, and who can see it?
Good: a clear diagram, named sub-processors, regions. Bad: 'it's secure'.
- ☐ 2. Is our data used to train your models, or anyone else's?
Get the answer in the contract, not the sales call.
- ☐ 3. What happens to our data when we leave?
Ask for the deletion process and how deletion is evidenced.

The model itself

- ☐ 4. Which model is behind this, and what happens when it changes?
Providers deprecate and silently update models. Ask how you are notified and re-validated.
- ☐ 5. How do you measure quality, and can we see the evaluation set?
If quality is only demonstrated by demo, there is no quality process.
- ☐ 6. What is your error rate on cases like ours, broken down by segment?
An aggregate number with no breakdown is close to meaningless for risk.
- ☐ 7. Show me a case where it fails.
A vendor who cannot show you a failure has not looked for one.

Accountability

- ☐ 8. Can you explain an individual decision to a customer or a regulator?
Not global feature importance. This specific case, in plain language.
- ☐ 9. What audit trail do we get by default, and how long is it retained?
- ☐ 10. Who is liable when the model is wrong?
Read the limitation of liability against the size of the decision you are automating.

Running it for years

- ☐ 11. How do we detect drift, and whose job is it to act on it?

Deployment is the start of the cost, not the end of it.

- ☐ 12. What does it cost at ten times our current volume?

Per-token and per-seat pricing scale very differently. Model both.

A vendor who answers all twelve well is not necessarily the right choice, but a vendor who cannot answer them is not a choice at all.