CONSULT · FREE CHECKLIST

AI due diligence checklist for investors.

40 questions to put to an AI company before you invest, in nine areas. Use it on your own, send it to the founders, or hand it to us.

Free to use, copy and print. vocabotics, VOCABOTICS LTD (no. 17412438).

1. Claims and evidence

Every number in the deck should trace back to something you can re-run or read.

- [ ] List every claim the company makes about its AI (accuracy, speed, savings, “proprietary model”). Which have evidence behind them?
- [ ] For each headline figure: what test set, how many cases, measured when, by whom?
- [ ] Can the team re-run the headline figure in front of you, today, on the current version?
- [ ] Is any figure from a vendor benchmark rather than the company's own data?
- [ ] What does the product get wrong, with examples? Has anyone read the failures?

2. Data

The data is usually the real asset, and the real risk.

- [ ] Where does the training, tuning or retrieval data come from, and on what terms?
- [ ] Do they have the rights to use customer data the way they do? Show the contract clause.
- [ ] Is personal data involved? Where is it stored and processed, and under which lawful basis?
- [ ] How is test data kept apart from data the system learns from?
- [ ] What happens to the product if one data source is withdrawn?

3. Models and vendor dependence

Many “AI companies” are a well-made layer on someone else's model. That can be fine, if it is known.

- [ ] Which models does the product use (own, open-weight, or a provider's API), and for which steps?
- [ ] What breaks, and how fast, if the provider changes price, terms or model version?
- [ ] Has the product been moved between models before? How long did it take?
- [ ] If they claim their own model: what was trained, on what, at what cost, and is it better than an off-the-shelf model on their own tests?

4. Testing and quality

Without a test set, nobody knows whether the last change made it better or worse.

- [ ] Is there a written test set of real cases with known right answers?
- [ ] Do the tests run automatically on every change to prompts, models or code?
- [ ] Who decides the pass mark, and was it set before or after the results came in?
- [ ] Is there monitoring in production that would show quality falling?
- [ ] How are customer complaints about wrong answers recorded and fed back into the tests?

5. Human oversight and safety

Where the AI acts on its own, the cost of a mistake is the cost of the worst action it can take.

- [ ] Which actions can the AI take without a person approving them?
- [ ] Is there a record of what the AI did, when, and who approved it?
- [ ] Are there caps on spend, volume or sends, and do they stop the system when hit?
- [ ] Can an answer be traced to its source passage, record or rule?
- [ ] What is the plan when it gives a harmful or embarrassing answer in public?

6. Security and privacy

AI adds new ways in: prompts, uploaded files and tool access.

- [ ] Who holds the API keys and secrets, and how are they stored and rotated?
- [ ] Has anyone tried to make the system leak data or ignore its instructions (prompt injection)?
- [ ] What certifications or assessments exist (for example Cyber Essentials, ISO 27001, SOC 2), and what do they cover?
- [ ] Is there a data processing agreement and a list of sub-processors, including AI providers?

7. Costs and unit economics

Model costs scale with use. A product that loses money per customer gets worse with growth.

- [ ] What does one customer, query or document cost in model and infrastructure fees today?
- [ ] How does that compare with the price the customer pays?
- [ ] What assumptions about future model prices are built into the plan?
- [ ] Is there a usage pattern (a heavy customer, a long document) that would blow the budget?

8. Team, code and IP

Small AI teams often rest on one or two people.

- [ ] Who built the core system, and are they staying? What happens if they leave?
- [ ] Is the code in the company's own repositories, with history, reviews and tests?
- [ ] Who owns the IP: assignments from founders, contractors and agencies all in place?
- [ ] Which open-source components and model licences are used, and do the licences allow commercial use?

9. Regulation and contracts

The rules depend on where the product is sold and what it decides.

- [ ] Does the product make or support decisions about people (hiring, credit, health, access to services)?
- [ ] If it is sold into the EU: which EU AI Act risk category does the company believe applies, and why?
- [ ] What do customer contracts promise about accuracy, liability and data use?
- [ ] Is there professional indemnity or product liability insurance that covers the AI's output?

WANT IT DONE FOR YOU?

A written report in 5 to 10 working days.

We work through this list on the company's code, data and claims, re-run what can be re-run, and write up what we found and what we could not check. From £4,500 (light) to £9,500 (full), fixed per deal.

hello@vocabotics.com · vocabotics.com/consult/tech-due-diligence. A checklist, not advice on any particular investment.