

12 technology red flags to check before you invest

A one-page checklist from Evgeny Goncharov, Alarifa (Madrid). Free to forward to clients.

For investors, M&A advisers and deal lawyers looking at a company whose value depends on its technology. One red flag is not a reason to walk away. It is a question to answer before signing, and often something to price in or cover in the contract.

#	RED FLAG	WHAT TO ASK
01	Key-person dependency. One engineer, founder or outside agency holds the knowledge, the code or the admin access.	Who could keep the system running if that person left tomorrow? Is any of it documented?
02	Unclear ownership of the code. Software built by freelancers or agencies without a written transfer of IP; open-source licences never reviewed.	Are there signed IP assignments for everyone who wrote code? Has anyone checked open-source licence obligations?
03	No map of personal data. Nobody can say where customer data sits, who processes it, or on what legal basis.	Is there a record of processing under the GDPR, and data processing agreements with each supplier?
04	AI claims the product cannot support. “AI” that is really rules or manual work behind the screen, or models trained on data the company may not have the right to use.	What exactly is the model, how is it measured, and where did the training data come from? Does any use fall under the EU AI Act's stricter categories?
05	Uncontrolled use of AI tools. Staff paste customer or company data into tools nobody approved.	Is there a written AI policy, and which tools have company data gone into?
06	Technology costs growing faster than revenue. Cloud, licences and contractors rise with every new customer.	What does technology cost per customer or per transaction, and how has it moved over time?
07	Technical debt with no plan. Old frameworks, unsupported versions, and every change feels risky.	What would the team rebuild first, and what would it cost in time and money?
08	Backups never tested. Backups exist, but nobody has restored from one.	When was the last full restore test, and how long did it take?
09	Weak access control. Shared passwords, no multi-factor authentication, former staff still with access.	Who has admin rights today, and when was access last reviewed?
10	Lock-in to one supplier. A critical platform with no exit terms, or data that cannot be exported.	If the main supplier raised prices or closed, how would the company leave, and with its data?
11	No security history. No penetration test, no logging, no record of past incidents.	Has there been an independent security test, and what incidents have occurred and been reported?
12	Delivery that depends on heroics. No release process, no automated tests, no monitoring. Roadmap promises far ahead of what actually ships.	How often does the team release, how do they roll back, and how do last year's plans compare with what shipped?

How to use it. Send the “What to ask” column to the target’s management before the data room opens. Vague answers are a signal in themselves. For a fixed-price technical due diligence on one company (red flags, AI and data risk, and a 100-day technology plan), contact eg@alarifa.com.