



10 Red Flags When Onboarding New Vendors

A quick screening checklist to use before signing a contract, sending money, or sharing data.

1 Vague or overly broad scope of work
Deliverables, timelines, performance measures, or responsibilities are unclear.

2 Resistance to basic verification
The vendor will not provide registration, financial, insurance, or security information when appropriate.

3 No clear owner or escalation path
Communication relies on generic inboxes, with no accountable contact for issues or decisions.

4 No verifiable references or work samples
The vendor cannot demonstrate relevant experience or connect you with credible clients.

5 Pushback on confidentiality terms
The vendor resists reasonable NDA or confidentiality terms before receiving sensitive information.

6 Unusual or high-risk payment requests
Examples include 100% upfront payment, personal accounts, or refusal of standard invoicing terms.

7 Missing appropriate insurance
Coverage such as general liability, E&O, or cyber insurance is absent or does not match the work.

8 Undisclosed subcontractors or third parties
It is unclear who will perform the work, access data, or support critical operations.

9 No credible data protection or recovery plan
An IT or SaaS vendor cannot clearly explain security, backups, or outage and breach response.

10 Pressure to bypass normal review
Extreme urgency or artificial discounts are used to rush contracting or skip approval steps.

IF YOU CHECK A BOX

Pause and clarify the issue before approval. One red flag does not automatically disqualify a vendor, but it should prompt documentation, follow-up questions, and a decision appropriate to the risk.

READY FOR A REPEATABLE PROCESS?

Move from a quick check to documented vendor decisions.

STARTER KIT | Pre-screen prospective vendors with a guided questionnaire and risk classification.

FULL TOOLKIT | Organize assessments, evidence, approvals, monitoring, and offboarding.

[VIEW THE \\$15 STARTER KIT](#)

[VIEW THE \\$39 VENDOR RISK TOOLKIT](#)