INTAI

DOWNLOADABLE CHECKLIST

RISK & ASSURANCE

AI Vendor Due Diligence Checklist

Review the key questions organisations should ask before selecting an AI supplier, platform, model provider or technology partner.

INTAI LIMITED
AI Governance & Assurance Consultancy

www.intai.co.uk
2026 Edition

AI Vendor Due Diligence Checklist

This checklist helps you look beyond a polished vendor demo to the data handling, security, transparency and contractual factors that determine whether an AI vendor relationship is genuinely safe to proceed with.

1 Business & Commercial Fit

- ☐ **Does the vendor's solution genuinely address the business need, rather than a broader capability you don't require?**
  Over-specified solutions often carry unnecessary cost and unnecessary risk surface.
- ☐ **Is the commercial model transparent, including all costs beyond the headline licence fee?**
  Integration, support and usage-based costs are frequently unclear at the proposal stage.
- ☐ **Has the vendor's financial stability been considered, particularly for smaller or newer suppliers?**
  Vendor failure creates operational risk that is easy to overlook during procurement.

2 Data Handling & Privacy

- ☐ **Can the vendor provide a clear data processing agreement covering your organisation's data?**
  The absence of a clear agreement should be treated as a significant warning sign, not a minor gap to resolve later.
- ☐ **Is it clear where your data will be stored and processed, including whether it leaves the EU/EEA?**
  This has direct implications for GDPR compliance and should be established before contracting, not after.
- ☐ **Does the vendor disclose its sub-processors and any fourth parties with access to your data?**
  Undisclosed sub-processing is a common source of hidden risk in AI vendor relationships.
- ☐ **Is it clear whether your data will be used to train or improve the vendor's models?**
  This is a material distinction, and one that default settings do not always make clear.

3 Security

- ☐ **Can the vendor provide evidence of independent security testing or relevant certification?**
  Self-reported security posture, without independent verification, provides limited assurance.
- ☐ **Does the vendor have a documented incident and breach notification process?**
  This should specify clear timeframes for notifying your organisation, not vague or open-ended commitments.

- [ ] **Has the vendor disclosed any previous security incidents relevant to this product?**
  A vendor unwilling to discuss past incidents at all is generally a more significant concern than one with a disclosed, resolved history.

4 Model Transparency

- [ ] **Can the vendor explain, at a reasonable level, what data the model was trained on?**
  Complete transparency is not always possible for third-party foundation models, but a reasonable explanation should be available.

- [ ] **Can the vendor explain how the system arrives at its outputs, at least at a high level?**
  This matters particularly for higher-risk use cases where explainability may be a regulatory requirement, not just good practice.

- [ ] **Has the vendor disclosed known limitations or failure modes of the system?**
  A vendor who claims no known limitations warrants more scrutiny, not less.

5 Governance & Assurance Evidence

- [ ] **Can the vendor provide documentation such as a model card or equivalent technical summary?**
  This is increasingly considered standard practice among more mature AI vendors.

- [ ] **Does the vendor hold, or is it working toward, relevant certification such as ISO/IEC 42001?**
  This is not yet universal, but is a positive indicator of governance maturity where present.

- [ ] **Can the vendor demonstrate how it supports customers in meeting their own EU AI Act obligations?**
  As a deployer, your organisation retains obligations that a vendor's support can materially ease or complicate.

6 Contract & Exit Terms

- [ ] **Are data portability and exit terms clearly defined in the contract?**
  Establish this before signing; it becomes far harder to negotiate once you are dependent on the vendor.

- [ ] **Is there a clear process for terminating the contract and retrieving or deleting your data?**
  This should specify timeframes and confirm secure deletion, not simply cessation of access.

- [ ] **Does the contract avoid creating disproportionate lock-in relative to the value of the solution?**
  Some lock-in is often unavoidable, but it should be proportionate to the criticality of the use case.

7 Ongoing Supplier Management

- ☐ **Is there a named internal owner responsible for managing this vendor relationship on an ongoing basis?**
  Vendor risk does not end at contract signature; it should be actively managed for the life of the relationship.

- ☐ **Is there a process for reassessing the vendor periodically, not only at initial onboarding?**
  Vendor risk profiles change over time, including through ownership changes, incidents, or product changes.

HOW TO SCORE THIS CHECKLIST

Any unresolved 'No' answer in Data Handling & Privacy or Security should be treated as a blocker to proceeding, regardless of how strong the commercial proposal appears. These are the areas most likely to create material risk once the vendor relationship is live.

INTAI

Need help acting on this checklist?

INTAI works with SMEs, public sector bodies and larger organisations across Europe to turn checklist findings into a practical, proportionate AI governance programme — from strategy and policy through to risk management and regulatory readiness. If you would like support closing the gaps this checklist has identified, our team is glad to help.

www.intai.co.uk | hello@intai.co.uk

© 2026 INTAI Limited. This checklist is provided for general guidance purposes only and does not constitute legal, regulatory or professional advice. Organisations should adapt it to their own context and seek independent advice where appropriate.