IronRoot
Risk Consultants

AI Vendor Evaluation Guide

What to Ask Before You Buy Any AI Tool

AI vendors promise a lot. Before you sign a contract or roll out a new tool, these questions help you evaluate what you're actually buying -- and what risks you're taking on. Use this guide in conversations with vendors, in IT review meetings, or as part of your third-party risk assessment process.

---

01 Data Privacy & Security

AI tools process your data. You need to know where it goes and who controls it.

[ ] Does the vendor use our data to train or improve their models?

Note: Opt-out clauses vary widely — enterprise tiers typically offer stronger protections.

[ ] Where is our data stored, and is it encrypted at rest and in transit?

Note: Look for SOC 2 Type II certification and data residency options if you have compliance requirements.

[ ] What happens to our data if we cancel the subscription?

Note: Understand data deletion timelines and whether you can export before canceling.

[ ] Does the vendor have a published data processing agreement (DPA) or BAA (if applicable)?

Note: Required for HIPAA-regulated data; increasingly expected for regulated industries generally.

[ ] Has the vendor undergone a third-party security audit?

Note: Ask for SOC 2 reports, penetration test summaries, or equivalent documentation.

02 Accuracy, Reliability & Limitations

Understanding what the tool can't do is as important as what it can.

[ ] What is the expected error rate, and how is accuracy measured?

Note: Be skeptical of vague claims. Ask for benchmarks on tasks similar to your use case.

[ ] How does the system handle queries it cannot answer confidently?

Note: Well-designed tools acknowledge uncertainty rather than fabricating responses.

[ ] How frequently is the model updated, and how are updates communicated?

Note: Unannounced changes can break workflows or introduce new behaviors.

[ ] What is the vendor's uptime SLA, and what is their track record?

Note: Critical for any workflow that depends on AI availability.

03 Access Control & User Management

AI tools need the same access governance as any other system.

[ ] Does the tool support role-based access controls (RBAC)?

Note: Ensure not every user can access every capability or sensitive output.

[ ] Can we restrict which data sources or systems the AI can access?

Note: Principle of least privilege applies to AI agents too.

[ ] Does the tool integrate with our identity provider (SSO/SAML)?

Note: Reduces credential sprawl and makes offboarding cleaner.

[ ] Is there an audit log of user activity and AI outputs?

Note: Necessary for compliance, incident response, and accountability.

04 Compliance & Regulatory Fit

Regulated industries have specific requirements that AI vendors may not meet out of the box.

[ ] Which compliance frameworks does the vendor support or certify against?

Note: Look for relevant certifications: SOC 2, ISO 27001, FedRAMP, HIPAA BAA, etc.

[ ] If the AI is used in a regulated decision (lending, hiring, benefits), what explainability is available?

Note: Regulators are increasingly asking how AI-assisted decisions were made.

[ ] Does the vendor have experience with customers in your regulated industry?

Note: Reference customers in similar regulatory environments are a good sign.

[ ] Will the vendor sign a Business Associate Agreement (BAA) or Data Processing Agreement (DPA)?

Note: Non-negotiable for certain regulated data categories.

05 Cost, Lock-in & Exit Strategy

AI tools can become deeply embedded quickly. Know your options before you commit.

[ ] How is pricing structured -- per user, per query, or flat rate?

Note: Usage-based pricing can surprise you at scale. Model the cost at 2x and 5x current usage.

[ ] What integrations does the tool support, and are they proprietary?

Note: Open APIs and standard connectors reduce lock-in risk.

[ ] Can we export our data and configurations in a portable format?

Note: Critical if you need to migrate to a different vendor.

[ ] What does the offboarding process look like?

Note: Ask this question before you sign. A vendor's reluctance to answer is itself informative.

06 Vendor Stability & Support

The AI market is consolidating fast. Bet on vendors who will be there long-term.

[ ] How long has the company been operating, and what is their funding situation?

Note: Startups can disappear or pivot. Understand the risk of building a workflow on a fragile foundation.

[ ] What is the support model -- and what is the SLA for critical issues?

Note: Email-only support with 5-day response times is not acceptable for production workflows.

[ ] Is there a dedicated customer success or implementation resource?

Note: Complex deployments often need hands-on guidance beyond documentation.

[ ] What is the roadmap, and how is product direction communicated?

Note: Frequent surprise changes to features or pricing are a red flag.

Third-Party AI Tools Are Vendors -- Treat Them That Way.

IronRoot Risk Consultants helps organizations build vendor and third-party risk programs that include AI tools, SaaS platforms, and cloud services.

chris@ironrootrisk.com | ironrootrisk.com