

EXECUTIVE BRIEF

What Is an AI Vendor Assessment? A Practical Guide to Third-Party AI Risk

Buying an AI tool does not transfer accountability to the vendor. An AI vendor assessment helps an organization understand what it is buying, what can go wrong, what evidence the vendor can provide, which safeguards belong in the contract, and whether the remaining risk is acceptable for the intended use.

EXECUTIVE SUMMARY

Buying an AI tool does not transfer accountability to the vendor. An AI vendor assessment helps an organization understand what it is buying, what can go wrong, what evidence the vendor can provide, which safeguards belong in the contract, and whether the remaining risk is acceptable for the intended use.

KEY TAKEAWAYS

- An AI vendor assessment evaluates the product, the provider, the intended use, and the customer's ability to govern the system after purchase.
- Traditional security and privacy reviews remain necessary, but they do not answer questions about model performance, bias, explainability, human oversight, training-data rights, or AI-specific change risk.
- The depth of review should follow the use case and potential impact, not the size or reputation of the vendor.
- Vendor claims are not evidence. Higher-risk uses require documentation, testing results, contract protections, and independent validation where appropriate.
- The assessment does not end at purchase. Monitoring, change notification, incident response, renewal, and exit planning are part of the same lifecycle.

Read the full guide at ai-governance-jobs.com/insights/what-is-an-ai-vendor-assessment/

Executive Brief · AI Governance Essentials · Source: [GRC-Careers.org](https://www.grc-careers.org)