HILLSIDE AI · AI TRANSFORMATION TOOLKIT — POLICY TEMPLATE

AI Vendor Assessment Protocol

The standard process for evaluating AI vendor risk across four critical dimensions

Chapter Reference: Chapter 9 — Building Your AI Policy Stack

HOW TO USE

This template provides the structure and key questions your policy must answer. Customise each section for your organisation's specific context, legal jurisdiction, and AI programme. Have your Legal team review before finalising. Review and update at minimum annually.

Document Title:	[Organisation Name] AI Vendor Assessment Protocol
Version:	1.0
Effective Date:	
Review Date:	
Document Owner:	
Approved By:	

Instructions

Complete this protocol for every new AI vendor relationship before contracting. Review annually for existing vendors. Conduct as a cross-functional team: Legal, IT Security, and the relevant business function. A vendor who cannot answer these questions clearly is not protecting proprietary information — they are avoiding inconvenient details.

Vendor Details

Vendor Name: _____ Solution/Product: _____

Assessment Date: _____ Assessed By: _____

Use Case: _____ Contract Value: _____

Dimension 1: Ethics and Governance

- **Does the vendor have a published AI ethics policy? [Yes / No / Partial]**
- **Do they have a formal AI governance framework with named accountability? [Yes / No]**

- [ ] **Have they experienced significant AI-related incidents or regulatory actions in the last 3 years? [Yes / No — If yes, details:]**
- [ ] **How do they conduct bias testing? What are their fairness standards?**
- [ ] **Who is responsible for model ethics and fairness within their organisation?**

Assessment Score (1–5): ___ Notes: _____

Dimension 2: Data Security and Privacy

- [ ] **Where is your data stored? What jurisdiction governs its protection?**
- [ ] **What certifications does the vendor hold? (ISO 27001, SOC 2, GDPR compliance)**
- [ ] **Is your data used to train or improve their models? Have you consented to this?**
- [ ] **What is their breach notification process and timeline?**
- [ ] **What are the data deletion procedures at contract end?**

Assessment Score (1–5): ___ Notes: _____

Dimension 3: Model Transparency

- [ ] **Can the vendor explain how their model works at a conceptual level?**
- [ ] **What data was the model trained on? How recent is it? How often is it retrained?**
- [ ] **What are the model's known failure modes and edge cases?**
- [ ] **Are accuracy statistics from real deployments (not just controlled test environments)?**
- [ ] **Can the vendor provide reference clients in a similar context to yours?**

Assessment Score (1–5): ___ Notes: _____

Dimension 4: Commercial Stability and Continuity

- [ ] **What is the vendor's ownership structure and funding status?**
- [ ] **What is the exit path if the vendor is acquired, pivots, or ceases operation?**
- [ ] **Who owns the model if the vendor is acquired? What happens to your data?**
- [ ] **What SLAs govern system uptime, performance, and support response?**
- [ ] **What is the contract notice period and transition support available?**

Assessment Score (1–5): ___ Notes: _____

Assessment Summary

Dimension 1 (Ethics & Governance): ___/5

Dimension 2 (Data Security & Privacy): ___/5

Dimension 3 (Model Transparency): ___/5

Dimension 4 (Commercial Stability): ___/5

Total Score: ___/20

Recommendation: [ ] APPROVED [ ] CONDITIONAL APPROVAL [ ] NOT APPROVED

Conditions / Required Actions: _____

Approved By: _____ Date: _____

Ready to go further? Book your free AI Discovery Call.
hillsideai.dev/book