Axiom Sovereign

TECHNOLOGY SOVEREIGNTY ADVISORY

AI GOVERNANCE SERVICE — EVALUATION TOOL

AI Vendor Risk Scorecard

Standardized Evaluation Framework for AI Tool Approval

v1.0 — 2026

Axiom Sovereign LLC · Severna Park, MD · info@axiomsovereign.com · axiomsovereign.com

AI Vendor Risk Scorecard

How to Evaluate Any AI Tool Before Approving It for Work Use

This scorecard provides a standardized evaluation framework for assessing any AI tool before it is approved for use with client or organizational data. It is designed to be completed by the AI governance owner or vCISO for each tool under evaluation, and to produce a consistent, documented approval or rejection decision.

Use this scorecard whenever: a staff member requests approval for a new AI tool, you are evaluating existing tools in your environment, a vendor proposes a new AI-enabled product, or you are conducting your quarterly AI tool inventory review.

PART 1: VENDOR PROFILE

Field	Response
Tool Name	
Vendor / Parent Company	
Country of Headquarters	
Ultimate Beneficial Owner / Parent Entity	
Date of Evaluation	
Evaluated By	
Business Justification (what staff want to use it for)	
Data Types Likely to Be Entered	

PART 2: DATA GOVERNANCE EVALUATION (SCORE 0–2 EACH)

Score: 0 = Unacceptable / Not addressed | 1 = Acceptable with conditions | 2 = Fully satisfactory

#	Evaluation Criterion	Finding (summarize what terms say)	Score (0–2)
DG 1	Training opt-out available: Vendor confirms your inputs are NOT used to train AI models, OR a clear opt-out mechanism exists and is confirmed active.		

#	Evaluation Criterion	Finding (summarize what terms say)	Score (0–2)
DG 2	Data retention policy: Vendor specifies exactly how long your inputs are retained and confirms deletion process. Enterprise/API plans typically have shorter retention than free plans.		
DG 3	Data residency: Data is processed and stored within an acceptable jurisdiction (U.S., EU, or jurisdiction required by your client contracts).		
DG 4	Third-party sharing: Terms confirm your data is not shared with third parties for any purpose other than service delivery.		
DG 5	Data Processing Agreement available: Vendor will execute a DPA (for GDPR-covered data) or BAA (for PHI). Vendor willing to sign if requested.		
DG 6	Breach notification commitment: Terms include obligation to notify customers of data breaches within a defined timeframe.		
	DATA GOVERNANCE SUBTOTAL (max 12)		

PART 3: SECURITY EVALUATION (SCORE 0–2 EACH)

#	Evaluation Criterion	Finding	Score (0–2)
S1	SOC 2 Type II report: Vendor has current SOC 2 Type II report available (within past 12 months). Report available upon request.		
S2	Encryption standards: Data encrypted in transit (TLS 1.2+) and at rest (AES-256 or equivalent). Vendor can confirm.		
S3	Access controls: Vendor implements role-based access controls limiting which vendor employees can access customer data.		
S4	MFA: Vendor requires MFA for customer accounts (admin portal and user access).		
S5	Penetration testing: Vendor conducts regular third-party penetration testing and can provide summary findings or attestation.		
	SECURITY SUBTOTAL (max 10)		

PART 4: REGULATORY AND ETHICS EVALUATION (SCORE 0–2 EACH)

#	Evaluation Criterion	Finding	Score (0–2)
RE 1	GDPR compliance documentation available (if EU data subjects): Vendor has published GDPR compliance documentation, DPA template, and sub-processor list.		
RE 2	HIPAA BAA availability (if PHI will be processed): Vendor will execute a HIPAA-compliant BAA. (If NO and PHI will be entered — automatic disqualification.)		
RE 3	Geopolitical sovereignty: No ownership, control, or significant government data access obligations from adversarial foreign jurisdictions.		
RE 4	AI Act / NIST AI RMF alignment: Vendor has published documentation on responsible AI practices, bias mitigation, and model transparency.		
RE 5	Enterprise vs. consumer data handling: Tool has an enterprise/professional plan with materially different (better) data protections than the free/consumer version.		
	REGULATORY & ETHICS SUBTOTAL (max 10)		

PART 5: SCORING SUMMARY AND DECISION

Section	Max Score	Score Achieved	Notes
Data Governance (DG1–DG6)	12		
Security (S1–S5)	10		
Regulatory & Ethics (RE1–RE5)	10		
TOTAL	32		

Total Score	Recommendation	Conditions
27–32	APPROVED — No conditions	Proceed. Add to approved tool list. Annual re-evaluation.
20–26	APPROVED WITH CONDITIONS	Specify conditions below (e.g., no PHI, no privileged matter data, enterprise plan only). Document in approved list.

Total Score	Recommendation	Conditions
13–19	CONDITIONAL / DEFER	Do not approve until vendor addresses gaps. Document gaps and request vendor remediation. Re-evaluate in 90 days.
0–12	NOT APPROVED	Tool does not meet minimum data protection standards. Document reasons. Communicate to requesting staff.
Any DG5=0 (no BAA) AND PHI will be entered	AUTOMATIC DISQUALIFICATION	Using this tool with PHI would be a per se HIPAA violation. Reject regardless of total score.

DECISION AND APPROVAL

Field	Response
Decision (circle one)	APPROVED / APPROVED WITH CONDITIONS / CONDITIONAL / NOT APPROVED
Conditions (if applicable)	
Date	
Approved by	
Next re-evaluation date	(12 months from approval date)
Added to approved tool list?	YES / NO / N/A (not approved)