NEXUS SECURITY ADVISORS

AI Governance Readiness Self-Check

Organizations adopting or building AI, including generative AI and agents

Baseline AI governance mapped to the NIST AI RMF (Govern, Map, Measure, Manage), ISO/IEC 42001, the EU AI Act, and the OWASP Top 10 for LLM Applications.

Organization: _____ Completed by: _____ Date: _____

☐	ID	Section	Requirement	Reference	Priority	Evidence
☐	AIGOV-01	Govern	Publish an AI acceptable-use policy covering approved tools, data handling, and human review	NIST AI RMF GOVERN; ISO/IEC 42001 cl. 5	High	Approved AI policy
☐	AIGOV-02	Govern	Assign accountable owners for AI risk and an AI governance committee	NIST AI RMF GOVERN; ISO/IEC 42001 cl. 5	High	RACI; committee charter
☐	AIGOV-03	Govern	Provide AI literacy training for staff who use or oversee AI	EU AI Act Art. 4	Medium	Training records
☐	AIGOV-04	Map	Inventory AI systems, models, agents, and AI features in third-party software (including shadow AI)	NIST AI RMF MAP; ISO/IEC 42001 cl. 4	High	AI inventory
☐	AIGOV-05	Map	Classify each use case by EU AI Act risk tier (prohibited, high-risk, limited, minimal)	EU AI Act Art. 5–6, 50	High	Risk classification register
☐	AIGOV-06	Map	Run AI impact and risk assessments before deployment	ISO/IEC 42001 cl. 6; NIST AI RMF MAP	High	Impact assessments
☐	AIGOV-07	Measure	Test for prompt injection, data leakage, insecure output handling, and excessive agency	OWASP Top 10 for LLM Applications	High	Red-team / test results
☐	AIGOV-08	Measure	Evaluate accuracy, bias, robustness, and drift with defined metrics	NIST AI RMF MEASURE	Medium	Evaluation reports
☐	AIGOV-09	Manage	Give AI agents their own identities and least-privilege permissions; log their actions	OWASP AI Exchange; NIST AI RMF MANAGE	High	Agent identity and permission inventory
☐	AIGOV-10	Manage	Keep a human-in-the-loop for high-impact decisions and outbound actions	NIST AI RMF MANAGE; EU AI Act Art. 14	High	Approval workflow evidence
☐	AIGOV-11	Manage	Vet AI vendors for data use, retention, and training on your data	ISO/IEC 42001 Annex A	Medium	Vendor AI questionnaires; contract terms
☐	AIGOV-12	Manage	Include AI incidents in your incident response plan	NIST AI RMF MANAGE	Medium	Updated IR plan

Readiness self-check for general guidance only. Not legal advice and not a formal assessment or certification. Confirm requirements against official sources.