AI RISK REGISTER

ISO 42001 AI Management System Deliverable

Client:	**[SAMPLE COMPANY]**
Assessment Date:	**December 2024**
Assessor:	**Careful Security**
Framework:	**ISO/IEC 42001:2023**
Classification:	**Confidential**

31	3	7	4
Total AI Risks	Critical	High	Categories

RISK CATEGORIES

Category	Description	Risks
Bias & Fairness	Discrimination, demographic disparities, unfair outcomes	8
Data Privacy	PII exposure, training data issues, consent, retention	6
Security & Adversarial	Model attacks, prompt injection, data poisoning	7
Transparency & Governance	Explainability, oversight, documentation, compliance	10

DETAILED RISK REGISTER

Each risk is scored using likelihood × impact methodology and mapped to ISO 42001 Annex A controls. This sample shows 12 of 31 identified risks.

ID	Risk Description	Category	Score	ISO Control
AI-001	Demographic bias in credit scoring model	Bias	9.8	A.6.2.4

AI-002	Model inversion attack vulnerability	Security	**9.5**	A.7.3.2
AI-003	No human oversight for high-stakes decisions	Governance	**9.2**	A.8.2.1
AI-004	Training data contains unredacted PII	Privacy	**8.7**	A.6.1.3
AI-005	Prompt injection in customer chatbot	Security	**8.4**	A.7.2.4
AI-006	Black-box model with no explainability	Transparency	**8.1**	A.9.3.1
AI-007	No model versioning or rollback capability	Governance	**7.8**	A.5.4.2
AI-008	Age discrimination in hiring recommendation	Bias	**7.6**	A.6.2.4
AI-009	Third-party API data retention unknown	Privacy	**7.3**	A.6.1.5
AI-010	Data poisoning vulnerability in feedback loop	Security	**7.1**	A.7.1.3
AI-011	No AI disclosure to end users	Transparency	**6.5**	A.9.2.1
AI-012	No documented AI impact assessment	Governance	**6.2**	A.5.2.3

RISK SCORING METHODOLOGY

Score Range	Priority	Required Action	Timeline
9.0 - 10.0	CRITICAL	Immediate remediation required	Within 7-14 days
7.0 - 8.9	HIGH	Prioritize for remediation	Within 30 days
4.0 - 6.9	MEDIUM	Plan for remediation	Within 90 days
0.1 - 3.9	LOW	Address as resources allow	Within 6 months

ISO 42001 CONTROL REFERENCE

This risk register maps to ISO/IEC 42001:2023 Annex A controls for AI management systems:

Control	Domain	Description
A.5.x	AI System Lifecycle	Planning, design, development, deployment, monitoring
A.6.x	Data Management	Data quality, privacy, bias in training data
A.7.x	Security	AI-specific threats, adversarial attacks, model protection
A.8.x	Human Oversight	Human-in-the-loop, accountability, intervention
A.9.x	Transparency	Explainability, documentation, user disclosure

NEXT STEPS

1. Review the AI Risk Register with your AI/ML and security leadership teams
2. Prioritize critical risks (AI-001, AI-002, AI-003) for immediate remediation
3. Establish AI governance committee with executive sponsorship
4. Begin AI impact assessments for all production AI systems
5. Schedule follow-up assessment in 90 days to validate progress toward ISO 42001

QUESTIONS?

Contact Careful Security:

Email: icare@carefulsecurity.com

Phone: +1-818-533-1402

Web: carefulsec.com