Arx Certa
Expert UK Cloud, Infrastructure & AI

AI READINESS · RISK

AI Risk Assessment Template

A pre-populated AI risk register UK businesses can adopt, adapt, and present to the board.

Free download · May 2026 · v2026-05
Scorecard companion: **arxcerta.com/ai-readiness-scorecard**

How to use this template

Twelve common AI risks with descriptions, likelihood / impact scoring, and mitigation patterns drawn from Arx Certa's real-world engagements. Add your own risks. Score honestly. Bring the result to your next leadership or risk-committee meeting.

SCORING METHOD

Likelihood (1-5). 1 = unlikely in next 12 months, 5 = expected in next quarter.

Impact (1-5). 1 = recoverable in a day, 5 = material to the business.

Residual risk = L × I after mitigations. ≥ 12 needs board awareness; ≥ 16 needs board action.

> **This is not a regulated risk assessment.** Where formal AI risk documentation is required (FCA SS1/23, sector-specific), use this as the working draft, not the final artefact.

Risk register

Risk	Description	L × I	Mitigation pattern
Data leakage to public AI tools	Staff paste confidential or personal data into ChatGPT, Claude, Copilot. Data enters vendor logs under vendor terms.	L=4 I=4 → 16	AI usage policy + enterprise tier + DLP + training + audit.
UK GDPR non-compliance	AI processing of personal data without DPIA, transparency notice, or lawful basis. ICO action; Article 33/34 reporting.	L=3 I=5 → 15	DPIA framework + privacy notices updated + lawful basis per use case.
Sector-regulatory exposure	AI used in regulated activity without governance fit (FCA, SRA, ICAEW, NHS). Supervisor finding; remediation cost.	L=3 I=5 → 15	Sector mapping (SS1/23, SRA Code etc.) + named senior owner.
Output quality drift / hallucination	AI outputs degrade silently. Decisions made on faulty outputs reach customers.	L=4 I=3 → 12	Sampling + eval set + human-in-the-loop + retire/rebuild triggers.
Vendor lock-in / portability	Critical workflows depend on one AI vendor; migration cost grows over time.	L=3 I=3 → 9	Abstraction layer + portable formats + multi-vendor on commodity tasks.
Bias / disparate impact	AI-augmented decisions affect protected groups disproportionately.	L=2 I=5 → 10	Pre-deployment fairness assessment + ongoing monitoring + appeal mechanism.

Risk register (continued)

Risk	Description	L × I	Mitigation pattern
Prompt injection / jailbreak	Malicious inputs trick AI into ignoring policy or revealing data.	L=3 I=3 → 9	Input sanitisation + restricted system prompts + monitoring + IR plan.
Third-party AI exposure	Embedded AI in existing SaaS processes company data without notice.	L=4 I=3 → 12	Third-party register refresh + DPA review for AI features + opt-out.
Skill gap / change resistance	Team unable to operate or trust AI outputs; adoption stalls.	L=4 I=2 → 8	Skills plan + training before go-live + partner support window.
Cost overrun / unmanaged consumption	AI usage costs scale unexpectedly (generative + agent workflows).	L=3 I=2 → 6	Cost monitoring + budgets per use case + alerts on anomalies.
Inaction / competitive disadvantage	Competitors capture AI productivity gains the business does not.	L=4 I=3 → 12	Quarterly horizon scan + Q1 foundations plan even without pilots.
Audit failure / inability to evidence	Cannot produce policy, DPIAs, vendor DPAs, logs, training on 7 days' notice.	L=3 I=4 → 12	Audit-ready evidence pack + quarterly internal review.

Methodology and next steps

For every risk, decide: accept, reduce, transfer, or avoid. For anything to reduce, name the control owner and the review date. Cadence: full review every 6 months; light-touch refresh every 90 days; trigger-based review on vendor change, regulatory change, or material incident.