Arx Certa
Expert UK Cloud, Infrastructure & AI

AI READINESS · GOVERNANCE

AI Governance Checklist for UK Firms

15 governance items every UK firm should be able to evidence, mapped to UK GDPR, ICO guidance, and the main sector regulators.

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

Context

AI governance is becoming a discrete category from data governance and IT governance. UK regulators are starting to ask firms not just whether they use AI, but how it is governed: who owns it, what is logged, what is disclosed, and what would be produced on seven days' notice if an audit landed tomorrow.

WHAT THIS CHECKLIST MAPS TO

UK GDPR — Article 22 (automated decision-making), Articles 5/24/32 (accountability, security).

ICO — guidance on AI and data protection; explainability; DPIAs for AI.

NCSC — secure development and operation of AI systems.

Sector regulators — FCA (Consumer Duty, model risk), SRA (use of tech in legal services), NHS DSPT for health, MHRA for AI-enabled medical devices, OFCOM (Online Safety) where relevant.

> **How to read the rows below.** Each item has a one-line description, what it looks like in practice, and what regulator or guidance it maps to. Score 1–3 and aggregate. Score 1 on items 1, 3, 7, 12, or 14 means governance gaps that would surface immediately under audit.

The 15 items

Item	What it looks like in practice	Maps to
1. Written AI policy with leadership approval	A standalone, leadership-approved AI usage policy distinct from acceptable-use policy.	UK GDPR Art. 5/24 · ICO accountability.
2. AI tool inventory with sensitivity classification	Living list of every AI tool in use, by tier of data it touches, with a named owner.	ICO records of processing · NCSC asset inventory.
3. DPIA for every personal-data-touching AI use case	Completed DPIA before go-live; revisit on material change to data flow, vendor, or purpose.	UK GDPR Art. 35 · ICO DPIA guidance.
4. Vendor risk assessment for every AI vendor	DPA signed; sub-processor chain disclosed; data location and retention checked.	UK GDPR Art. 28 · sector procurement standards.
5. Staff training record covering AI use	Evidence that each staff member has been trained on the AI policy this year.	ICO accountability · ISO 27001 A.7.2.2.
6. Approval process for new AI tools	Written approval workflow with assessor, decision record, and tool inventory update.	ICO accountability · NCSC supply chain.
7. Incident response plan that covers AI	IR plan explicitly handles AI-specific scenarios (prompt leak, model jailbreak, output bias).	UK GDPR Art. 33/34 · NCSC IR guidance.
8. Audit logging of AI tool use	Logs retained ≥12 months; queryable by user, tool, and timestamp.	ICO accountability · ISO 27001 A.12.4.
9. Data retention policy that covers AI inputs and outputs	Inputs/outputs aged out on the same schedule as source data, or sooner.	UK GDPR Art. 5(1)(e) · ICO retention guidance.
10. Disclosure framework	Defined when, to whom, and how the firm discloses AI use (clients, regulators, partners).	Sector duty (e.g. FCA Consumer Duty) · contractual obligations.
11. Periodic review of AI use cases	At least annual review of each live AI use case: outcome, drift, retire/extend decision.	ICO ongoing accountability · sector model-risk rules.
12. Accountable owner at leadership level	Named board-level or leadership-team owner accountable for AI in the firm.	UK GDPR Art. 24 · sector senior-manager regimes.
13. Risk register that includes AI risks	Top AI risks listed with current controls, residual risk rating, and mitigations.	ISO 31000 · ICO accountability.

Item	What it looks like in practice	Maps to
14. Board reporting cadence	AI status reported to the board on a defined cadence (at least annually).	Sector senior-manager regimes · audit expectations.
15. External audit readiness — 7-day evidence pack	Could you produce policy, DPIAs, vendor DPAs, logs, training, and risk register inside 7 days?	Sector audit expectations · ICO investigatory powers.

How to score yourself

Score each of the 15 items 1–3 (1 = nothing; 2 = partial; 3 = mature, with evidence). Aggregate guides:

Score band	What it means
45 — Mature	Audit-ready today. Focus on continuous improvement.
35–44 — Operational	Most controls exist; harden evidence trails.
25–34 — Emerging	Controls are partial; close governance gaps before scaling AI.
15–24 — Early	Few controls in place; governance work has to lead AI work.
Below 15	Treat as a governance project, not an AI project, until you can lift this score.

Important caveat. This checklist is a maturity signal, not legal advice or a regulatory compliance attestation. Where regulated obligations apply (FCA, SRA, NHS, MHRA, etc.) take professional advice and read the applicable rulebook in full.

For a weighted, dimensioned version of this exercise

The 4-minute AI Readiness Scorecard scores you across five dimensions — Governance, Data, Infrastructure, Security, and Use case — and produces a personalised 30-day action plan.

Take the scorecard → arxcerta.com/ai-readiness-scorecard