AI Governance UK
By CyPro

THE WORKING FRAMEWORK

The AI Governance Framework

An AI governance framework you can actually implement: six pillars, one standards map and five implementation steps, built for UK businesses by the CyPro team. Use it as it stands or as the skeleton of your own.

How to use this document: work the six pillars in order; each states what good looks like and the first artefact to produce. The standards map on the final page shows how ISO 42001, NIST AI RMF and the EU AI Act relate, so evidence gathered once serves every audience that asks.

1 AI inventory and ownership

You cannot govern what you have not listed. Record every AI system and use case: the tool, the owner, the data it touches, the decisions it influences and whether it is built, bought or simply used by staff. Include the unofficial uses; they carry most of the early risk. First artefact: a use-case register with a named owner per row.

2 Policy and acceptable use

One short policy that says what may be used, for what purposes, with what data, and what is prohibited outright. Write it for the staff member with a deadline, not the auditor. First artefact: an AI policy signed off by leadership and acknowledged by staff.

3 Risk assessment

Assess each use case for the harms it can produce: wrong outputs acted on, data leaving your control, bias, security failures and regulatory exposure. Score consistently, so effort follows the biggest risks rather than the loudest voices. First artefact: a scored risk register reviewed at a set rhythm.

4 Controls through the lifecycle

Controls belong at every stage: what checks happen before a new AI use is approved, what rules apply while it runs, and how it is retired without leaving data or access behind. Buying decisions deserve the same gate as building decisions.

5 Monitoring and incidents

Decide what you watch and who reacts: output quality, complaint and error reports, provider changes, security events involving AI systems. Extend your incident process to cover AI failures, and rehearse the questions the board will ask afterwards.

6 Review and reporting

Governance that is not reviewed decays. Set an annual formal review, event-driven reassessment when systems or regulation change, and a standing board report that says what AI the business runs, what risks it carries and what changed since last time.

How the standards fit together

INSTRUMENT	WHAT IT IS	BINDING?	WHEN IT LEADS
ISO 42001	Certifiable management-system standard for AI (an AIMS)	Voluntary; certifiable	Customers or tenders ask for certified evidence of responsible AI management
NIST AI RMF	US risk-management framework: Govern, Map, Measure, Manage	Voluntary	You need a shared risk vocabulary, especially with US-facing customers
EU AI Act	Binding EU product regulation, tiered by risk category	Binding where it applies	You place AI on the EU market or your systems' outputs are used in the EU
UK Code of Practice	Voluntary UK government code for the cyber security of AI	Voluntary	You want a UK-native security baseline across the AI lifecycle

Implementing the framework: five steps

- [ ] **1** **Give it an owner and a mandate**

  Name the person accountable for AI governance and have leadership say so. Without a mandate, every later step becomes a suggestion.

- [ ] **2** **Build the inventory**

  Survey the business for AI in use, official and otherwise. The register from pillar one is the foundation every other pillar stands on.

- [ ] **3** **Adopt the framework and write the policy**

  Tailor the six pillars to your business and publish the policy. Short and enforced beats long and ignored.

- [ ] **4** **Risk-assess the use cases that matter**

  Start with the systems touching customer data, money or automated decisions. Score them, pick the top treatments, assign owners.

- [ ] **5** **Set the rhythm and keep evidence**

  Diary the reviews, capture evidence as a by-product of normal operation, and report to the board on a fixed cadence.

Each step produces evidence that maps to ISO 42001 clauses, NIST AI RMF functions and, where it applies, EU AI Act obligations. That single-evidence, many-audiences pattern is the difference between governance as a system and governance as paperwork.

Want the framework installed rather than described?

Our governance engagements deliver the register, policy, risk assessment and roadmap as a fixed-fee programme, with prices published in full. If you work through this framework yourself, the free scoping call is still a useful sense check.

aigovernanceuk.co.uk/pricing/