

# UK AI READINESS 2026

From national ambition  
to organisational action

---

A practical briefing for UK boards and leadership teams seeking  
valuable, responsible and secure AI adoption.

# The UK is accelerating. Organisational capability now matters.

The UK's AI Opportunities Action Plan established a national programme to strengthen foundations, increase adoption and build homegrown capability. The January 2026 progress report said 38 of 50 actions had been met.

50

ACTION PLAN ACTIONS

38

REPORTED AS MET

3

NATIONAL PRIORITIES

## THE MANAGEMENT REALITY

### Technology access does not equal readiness

Organisations still need clear outcomes, accountable governance, trustworthy data, secure systems, capable people and disciplined delivery. These are management capabilities - not features that arrive with an AI licence.

# Three priorities shaping the national AI agenda

01

## Lay the foundations

Infrastructure, data, compute, skills and the enabling conditions for AI development and use.

02

## Adopt and change lives

Support adoption across public services, organisations and the wider economy.

03

## Secure homegrown AI

Strengthen UK capability, investment, innovation and strategic advantage.

### WHAT THIS MEANS FOR ORGANISATIONS

National momentum increases both the opportunity and the expectation to act. Leaders need to connect AI ambition with ownership, controls, cyber security, workforce capability and measurable outcomes.

# National infrastructure is not organisational readiness

## National direction

Compute and infrastructure Skills and talent Public-sector adoption Innovation and investment AI Growth Zones and domestic capability

## Organisational responsibility

Clear purpose and outcomes Executive accountability Data and cyber controls Human oversight and workforce capability Measurement and improvement

## The readiness question

Can your organisation turn access to AI into controlled, measurable and repeatable value - while protecting people, information, services and reputation?

# Eight dimensions of organisational AI readiness



## Leadership & Strategy

Assessed through evidence-led questions



## Governance & Risk

Assessed through evidence-led questions



## Data Readiness

Assessed through evidence-led questions



## Technology & Infrastructure

Assessed through evidence-led questions



## People & Skills

Assessed through evidence-led questions



## Security & Compliance

Assessed through evidence-led questions



## Adoption & Business Value

Assessed through evidence-led questions



## Continuous Improvement

Assessed through evidence-led questions

ARI combines these dimensions to help leaders see dependencies, strengths and priority gaps rather than treating AI as a standalone technology purchase.

# Secure AI adoption is a leadership responsibility

The Cyber Governance Code places cyber risk within board and director responsibilities. The AI Cyber Security Code and NCSC secure-development guidance extend that discipline across the AI lifecycle.

**OWN** Named accountability for AI cyber risk

**KNOW** Critical systems, data and dependencies

**CONTROL** Access, suppliers and secure deployment

**EXERCISE** Incident response and recovery

**MONITOR** Logging, vulnerability and remediation

# Six actions that turn ambition into controlled progress

01

## Set accountable leadership

Name an executive owner and define decision rights.

02

## Create an AI inventory

Record use cases, suppliers, data, owners and dependencies.

03

## Prioritise measurable value

Use baselines, success measures and benefit owners.

04

## Build proportionate governance

Apply risk tiers, oversight and retained evidence.

05

## Secure the AI lifecycle

Address access, suppliers, monitoring and recovery.

06

## Develop people and capability

Enable staff to use, challenge and supervise AI.

# A practical route from uncertainty to action

DAYS 1-30

## DISCOVER

Establish ownership, inventory AI use, identify obligations and agree the evidence baseline.

DAYS 31-60

## DESIGN

Prioritise value, define risk tiers, approval routes, minimum controls and success measures.

DAYS 61-90

## DELIVER

Launch controlled use cases, train people, retain evidence, monitor outcomes and schedule review.

The goal is not maximum paperwork. It is enough structure to make good decisions, show accountability and learn safely as adoption grows.

# Experience built before the AI hype began

unoui's approach is grounded in more than 25 years across compliance, strategy, automation, systems and data governance, with the past five years increasingly focused on artificial intelligence across public and private sectors.

25+

YEARS ACROSS OPERATIONAL DISCIPLINES

5

YEARS FOCUSED INCREASINGLY ON AI

2

PUBLIC AND PRIVATE-SECTOR PERSPECTIVES

ARI views AI as an organisational capability: leadership, controls, information, technology, people and measurable outcomes working together.

# Official sources, methodology and limitations

## PRIMARY SOURCES

- 1 UK Government - AI Opportunities Action Plan: One Year On (January 2026)
- 2 Department for Science, Innovation and Technology - AI Cyber Security Code of Practice
- 3 Department for Science, Innovation and Technology - Cyber Governance Code of Practice
- 4 National Cyber Security Centre - Guidelines for Secure AI System Development

## IMPORTANT LIMITATIONS

This is an independent unoui briefing based on publicly available government and NCSC material. It is not endorsed by the UK Government. It provides general organisational-readiness information and is not legal advice, regulatory assurance, cyber-security certification or a formal conformity assessment.

Policy, guidance and regulatory expectations change. Organisations should verify current requirements and obtain specialist advice where appropriate.

**UNOUI.CO.UK**

Assess readiness. Prioritise action. Build confidence.