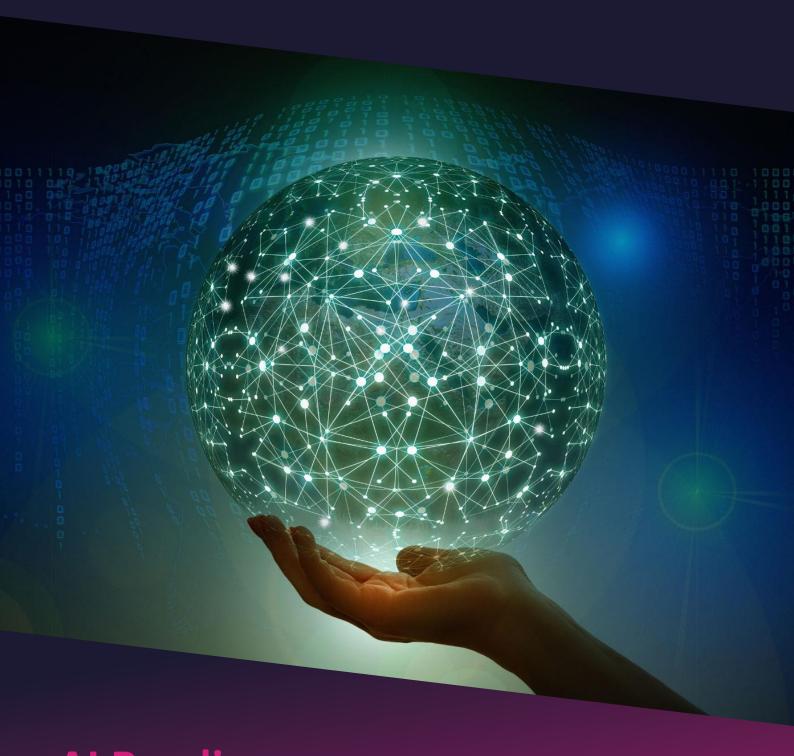# Delta Capita

AI Readiness

Introducing our AI Risk Assessment Toolkit

AI Readiness:
Overview

Financial Institutions need to keep their Risk and Governance policies, processes, and controls updated to manage new risks as they test and deploy Artificial Intelligence (AI) tools.

Regulatory Uncertainty: firms are reluctant to adopt AI tools due to an unclear regulatory & legal landscape.

Emerging Standards: 65% of UK high street banks have taken action to upgrade AI risk management* to account for AI.

Stakeholder Collaboration: 65% consider conflicting regulatory rules between different AI stakeholders to be among the top three concerns*.

2027 **Competing Priorities**: competing investment priorities, such as inflation, customer service, and regulatory compliance.

65% of UK financial institutions *consider uncertainty regarding the direction of regulation as a top concern for AI adoption**

* The Impact of AI in Financial Services, UK Finance

1. Unestablished AI Governance

- Unclear accountability for data & AI including lack of roles and responsibilities
- Inconsistent AI policies including privacy, security storage, and usage.

2. Regulatory Uncertainty

- Firms are reluctant to adopt AI tools due to an unclear regulatory & legal landscape
- AI models require a well-architected, and compliant infrastructure often using cloud-based AI services

3. Competitive Disadvantage

- Inability to respond quickly to evolving market demands including competitive AI landscape
- Lost opportunities due to slow AI integration, system agility and inability to scale AI models

Delta Capita Offering: AI Risk Assessment Toolkit

- *Despite the potential of AI, most Financial Institutions rely on existing control functions like Model Risk, Compliance, Infosec, and Internal Audit*
- *Our Risk Assessment Toolkit offers a four-stage process for assessing AI risks, including assessments, and controls from our AI Controls Library.*

Stage 1: Initial Risk Assessment

AI Use Case Proposed

Initial Questionnaire

Example Output

- ➤ Is the AI system at the proof-of-concept stage, production-ready, or live in trading?

- ➤ Who will interact with the AI system? Internal teams, external clients, or end-users?

- ➤ Will the solution be on-premises, in the cloud, or hybrid?

- ➤ Are synthetic data or third-party models being used? Does it involve novel or high-risk processes?

- ➤ **Initial risk rating** (low, medium, high) to prioritise next steps

- ➤ A heatmap summary to visualise areas of concern

Stage 2: Detailed Risk Assessment

- *With the initial risk rating established, a bottom-up detailed assessment is carried out against 70 AI specific questions across 6 categories*

1. Data	2. Model	3. Cybersecurity
4. Operational & Systemic	5. Social Behaviours and Human Values	6. Legal & Compliance

Stage 3: Mapping Risk to the AI Controls

- *With the detailed risk register established, the risks are then mapped against a library of 60+ risk mitigating controls specific to AI*

Stage 4: Risk Approval Decision

- *With the risk to control mapping established, risk teams can now make informed decisions on go-live for AI and GenAI implementations*