BeyondFS

August 2025

The EU AI Act:

What it means for UK Financial Services

A briefing note for banks, insurers and Lloyd's syndicates on new compliance obligations and their impact on financial crime, risk and customer operations.

The AI Compliance Challenge UK Financial Firms Can't Ignore

The EU's Artificial Intelligence Act became law in **August 2024** - the first comprehensive regulation of its kind worldwide.

For UK banks, insurers and Lloyd's syndicates, this is not just another European rule that can be left aside post-Brexit. It marks a significant shift in how firms must use AI - especially in high-stakes areas like financial crime controls, customer onboarding, fraud detection and sanctions compliance.

Brexit Isn't a Shield

A common misconception is that Brexit insulates UK firms from EU regulation. In practice, the AI Act has **extraterritorial reach**. If your AI systems impact anyone in the EU - whether through onboarding an EU client, running sanctions or fraud screening, or evaluating staff who serve EU customers - you're caught.

The Act applies whether you are the **provider** (building or selling an AI system) or the **deployer** (using one in operations).

Typical touchpoints for FinCrime teams include:

- London-based platforms screening EU payments.
- Shared service centres processing EU transactions.
- Branches onboarding EU customers.

For many UK firms, European markets are material. Non-compliance isn't just a regulatory risk; it threatens access to critical markets.

Why Financial Services AI May Fall Into the "High-Risk" Category

The Act categorises AI systems by risk. **Certain specific use cases in financial services are automatically high-risk under Annex III**:

- Creditworthiness / credit scoring.
- Life and health insurance risk assessment and pricing.

Other FS applications - including many FinCrime systems such as AML/KYC monitoring, sanctions screening, fraud detection and customer risk scoring - are **not automatically high-risk**. They may, however, fall into scope if they overlap with another Annex III category (e.g., biometric verification) or if their impact on fundamental rights is material.

Edge cases matter:

- A chatbot explaining why a transaction was flagged → may not be high-risk.
- A chatbot that blocks or releases funds → not high-risk by default, depends on Annex III and Article 6 tests.

For systems that are high-risk, firms must demonstrate:

- Risk management.
- Data governance.
- Documentation & logging.
- Post-market monitoring.
- Transparency.
- Meaningful human oversight.

In practice, this means model owners must be able to explain why a transaction was blocked, why a customer was risk-rated, or why a claim was declined - not simply rely on "the model says so."

The Clock Is Ticking

With some deadlines already in effect and most obligations applying by **August 2026**, any new monitoring or onboarding platforms must now be designed with compliance front of mind.

Key dates:

- **February 2025:** Prohibited practices banned; AI literacy duties apply
- **August 2025:** Obligations for general-purpose AI providers take effect.
- **August 2026:** Most obligations, including those for high-risk systems, apply..
- **August 2027:** Certain Annex I high-risk safety systems and some legacy/GPAI cases must comply.

Building an AI governance framework across trading, underwriting, fraud and FinCrime systems typically takes **12–18 months**. Delay further, and compliance will become a rushed, more costly exercise.

Beyond Compliance: An Opportunity

The EU AI Act is more than a compliance exercise - it is a chance to strengthen the risk and control environment around AI. By implementing its governance, oversight, and transparency requirements, businesses can reduce operational and reputational risks while increasing confidence in AI-driven decisions. This enhanced control framework not only satisfies regulators but also builds trust with clients, partners, and investors, positioning firms to scale AI responsibly and sustainably.

What Implementation Means in Practice

For all businesses using AI, firms will need to:

- Establish and maintain an **inventory of all AI systems**, including vendor-supplied and embedded tools. This could include transaction monitoring, screening, onboarding/KYC models, fraud detection, and other areas, such as claims scoring and HR tools.
- **Classify each system** according to the risk categories defined in the Act (prohibited, high-risk, limited-risk, minimal), with documented justification.
- **Implement transparency measures** for limited-risk systems, including clear disclosure when individuals interact with AI systems and labelling of artificially generated or manipulated content.
- **Maintain technical documentation** and records demonstrating compliance decisions.
- Provide appropriate training to staff on AI Act requirements, governance, and compliance responsibilities.

For High-Risk AI systems:

- **Implement a risk management system** covering the design, testing, monitoring, and oversight of the AI system.
- **Ensure data governance practices** are in place, including data quality, representativeness, and bias mitigation.
- **Define and document measures for human oversight** to ensure accountability and the ability to intervene.
- **Prepare detailed technical documentation** and instructions for use in line with the requirements of Annex IV.
- **Ensure logging and record-keeping capabilities** to allow traceability and audit.
- **Carry out the required conformity assessment** (internal or involving a notified body, depending on the system).
- **Register high-risk AI systems in the EU database** maintained by the European Commission.
- **Establish post-market monitoring procedures** and ensure mechanisms for reporting serious incidents.
- **Conduct a Fundamental Rights Impact Assessment (FRIA)** where required, particularly for high-risk systems in Annex III (such as those used for creditworthiness or life/health risk assessment and pricing).

Governance and Integration Activities:

- **Align AI Act compliance** with existing regulatory frameworks such as GDPR, Solvency II, and outsourcing requirements.
- **Update third-party and vendor management processes** to include AI Act compliance obligations.
- **Report on AI governance, risk, and compliance** to senior management and the board, ensuring clear accountability.

How BeyondFS Can Help

1. Control Framework (enterprise-level compliance)

- **Obligations mapping:** Translate the Act into a set of obligations and identify the evidence required.
- **Scope definition:** Define what qualifies as "Regulated AI" within the organisation.
- **Target framework design:** Design an "ideal-state" control framework aligned to the Act, covering governance, policies, risk management, supplier oversight, IT and HR processes.
- **Gap analysis:** Compare current controls against the target framework, highlighting deficiencies and missing evidence.
- **Uplift plan and delivery:** Develop and implement a roll-out plan, assigning responsibilities and timelines to close identified gaps.

2. Current AI Use Review (system-level compliance)

- **Inventory creation:** Identify AI usage across the organisation, including monitoring, sanctions screening, onboarding/KYC, fraud detection, HR tools, and third-party systems.
- **Risk classification:** Assess and classify each system according to the Act's categories (e.g. high-risk, limited-risk), with rationale documented.
- **Gap analysis and remediation:** Perform detailed assessments against the Act's requirements and define remediation actions.
- **Implementation support:** Execute remediation activities such as retrofitting explainability, updating supplier contracts, documenting testing processes, or embedding new monitoring and oversight procedures.

Approach and governance

On a project of this nature we typically bring together a team spanning Compliance, Operations, Technology, Risk and Procurement. The sponsor might be the Head of Compliance, Technology or the COO, but delivery is a shared effort across functions. We keep things on track with regular check-ins every two weeks and monthly updates for senior executives – giving both transparency and momentum.

The result is a clear, evidence-based compliance framework and a full system inventory with any gaps closed. This not only meets regulatory expectations but also makes controls stronger, audits easier, and day-to-day operations more resilient.

Your Strategic Options

Financial institutions have a choice in how they respond to the EU AI Act:

- **Option 1: Reactive compliance.** Wait until 2026 and approach the Act as a box-ticking exercise. This is likely to lead to rushed remediation, higher costs, weaker assurance, and greater exposure to regulatory action if deadlines are missed.
- **Option 2: Proactive compliance.** Begin now by embedding AI obligations into existing frameworks such as model risk governance and third-party risk management. Build inventories, design control frameworks, and address gaps ahead of time. This spreads the workload and ensures readiness for both EU and emerging UK/US requirements.

Leading firms are already pursuing the proactive route. They are putting senior oversight in place, investing in explainability and transparency, and requiring suppliers to provide robust documentation and evidence. By integrating AI compliance into their broader risk and control frameworks, they avoid duplication and achieve consistent governance across financial crime, customer onboarding, fraud and HR.

About BeyondFS

BeyondFS was founded in 2018 by three former Big 4 consultants who saw a persistent challenge: senior leaders in Financial Crime functions were under immense pressure, but too often lacked the clarity, capacity and capability to push initiatives forward against a tide of regulatory, business and market change.

We exist to help financial institutions build high-performing Financial Crime programmes that reduce risk, satisfy regulators, and run efficiently day-to-day.

We don't just advise - we deliver. Our role is to close the execution gap, apply proven FinCrime expertise, and turn strategy into reality. With methods refined over many years in complex regulatory and operational settings, we introduce improvements that last.

We work with clients facing regulatory scrutiny, limited resources, and rising expectations, who turn to us when:

- Large programmes lose focus, stall, or fail to deliver results.
- Regulatory gaps appear and urgent remediation is required.
- Costs and complexity rise while performance doesn't improve.

Our trusted senior experts cut through complexity, bring clarity, and restore momentum. Drawing on broad expertise across regulation, operations, data, technology, and change, we deliver practical solutions that build confidence and capability.

In the end, our work enables FinCrime leaders to take control, drive meaningful progress, and focus on what matters most.

Contact Us

Matt Neill, Partner
matt.neill@beyondfs.co.uk

Matt Beattie, Partner
matt.beattie@beyondfs.co.uk

Al Catto, Partner
alistair.catto@beyondfs.co.uk

BeyondFS

Contact

BeyondFS
Dawson House, 5 Jewry St, London
EC3N 2EX, United Kingdom

+44 (0)203 637 4117
info@beyondfs.co.uk
beyondfs.co.uk