INTRODUCTION

The financial sector is currently undergoing a digital transformation driven by artificial intelligence (AI). While AI brings immense promise, including increased operational efficiency, personalized financial services, optimizing supply chains, and advancements in healthcare, it also introduces new vulnerabilities, including algorithmic bias, lack of explainability, and portability of decisions. These risks can affect not only individual customers but also systemic market trust when unchecked.

One of the political priorities of the European Commission has been to create "*A Europe fit for the digital age*". This agenda has led to the creation of 10 significant digital regulations addressing topics such as cybersecurity, data governance and AI. In 2024, the European Union has introduced the Artificial Intelligence Act (AI Act), establishing a legal framework aimed at regulating the deployment and usage of AI systems across member states.

The AI Act introduces risk based approach by categorizing AI systems based on their use case, thereby establishing compliance requirements according to the level of risk they pose to users. This includes the introduction of bans on certain AI applications deemed unethical or harmful, along with detailed requirements for AI applications considered high-risk to manage potential threats effectively.

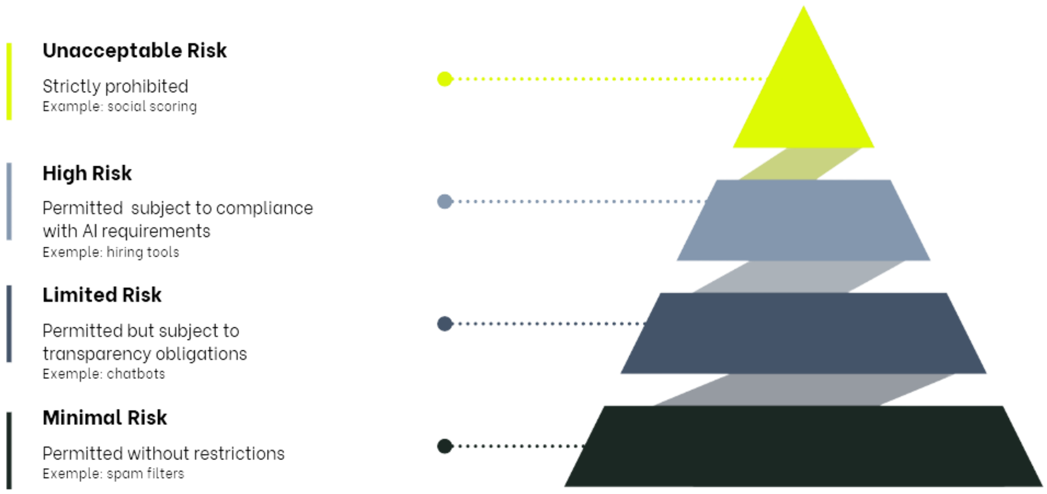
This regulation significantly impacts financial institutions as it classifies AI systems used for creditworthiness assessments, fraud detection and risk assessment tools as high-risk when they affect individuals. Customers rely on financial institutions to protect their assets and personal data, banks must implement AI responsibly. Financial entities are likely to face requirements around transparency, data governance, human oversight, and documentation. The AI Act not only affects how these systems are developed and deployed but also introduces new accountability expectations that legal, compliance, and risk teams must address proactively.

A New Chapter in Financial Regulation

The AI Act focuses on the use of AI rather than the technology itself, adopting a risk based approach where obligations increase with the level of risk. There are four categories within the framework, each with its corresponding set of requirements:

- Minimal Risk: Most AI applications currently available on the EU single market are unregulated and considered minimal risk (e.g. spam filters, AI enabled video games)
- Limited Risk AI Systems: AI systems with some potential risks but less severe than high-risk systems (e.g. AI chatbots or emotion recognition tools) are subject to lighter transparency obligations.
- High Risk AI Systems: AI systems that can significantly affect an individual's life are permitted subject to compliance with strict governance, transparency and documentation requirements (e.g. hiring tools, credit scoring tools)

- Unacceptable Risk AI Systems: AI systems that pose a clear threat to safety or fundamental rights, such as manipulative social scoring or real-time biometric surveillance in public spaces, are strictly prohibited.



Unacceptable Risk

Strictly prohibited
Example: social scoring

High Risk

Permitted subject to compliance with AI requirements
Exemple: hiring tools

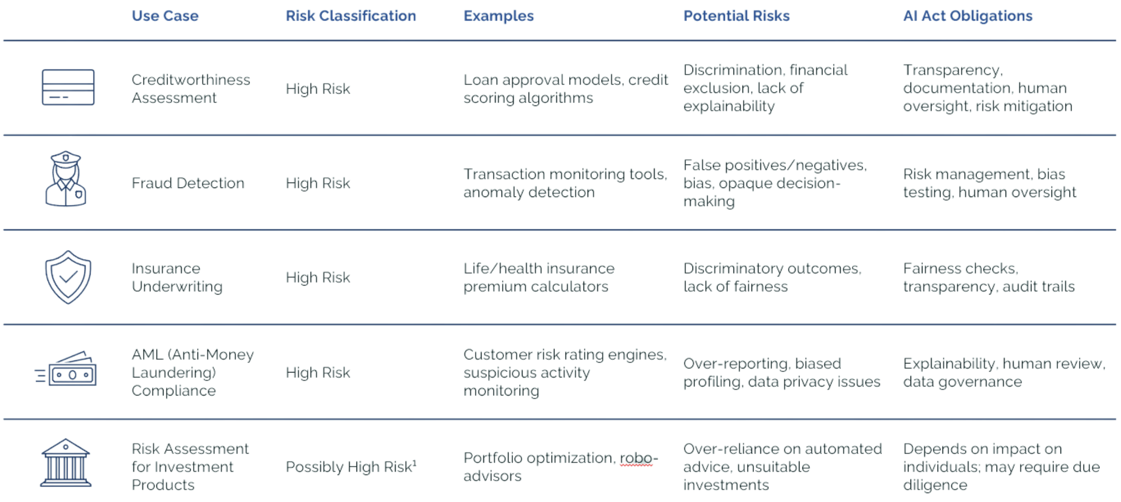
Limited Risk

Permitted but subject to transparency obligations
Exemple: chatbots

Minimal Risk

Permitted without restrictions
Exemple: spam filters

The high-risk category is of particular relevance to financial institutions. Annex III of the AI Act explicitly identifies high-risk AI systems used for creditworthiness assessments, fraud detection, insurance underwriting, and AML compliance as high-risk. These systems influence fundamental economic rights and can have significant impact on individuals' access to financial resources like loans and credits. The same designation applies to AI systems used for risk assessment in the case of life and health insurance which, if not properly designed, can lead to serious consequences for people's lives and health, including financial exclusion and discrimination.



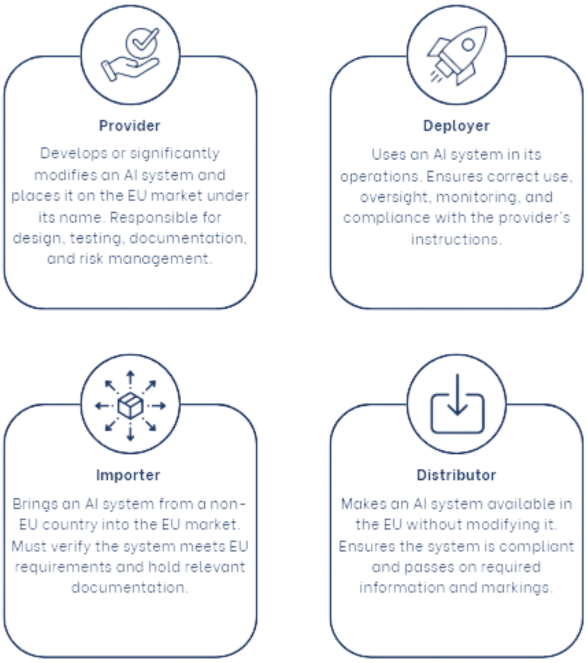
	Use Case	Risk Classification	Examples	Potential Risks	AI Act Obligations
	Creditworthiness Assessment	High Risk	Loan approval models, credit scoring algorithms	Discrimination, financial exclusion, lack of explainability	Transparency, documentation, human oversight, risk mitigation
	Fraud Detection	High Risk	Transaction monitoring tools, anomaly detection	False positives/negatives, bias, opaque decision-making	Risk management, bias testing, human oversight
	Insurance Underwriting	High Risk	Life/health insurance premium calculators	Discriminatory outcomes, lack of fairness	Fairness checks, transparency, audit trails
	AML (Anti-Money Laundering) Compliance	High Risk	Customer risk rating engines, suspicious activity monitoring	Over-reporting, biased profiling, data privacy issues	Explainability, human review, data governance
	Risk Assessment for Investment Products	Possibly High Risk[1]	Portfolio optimization, robo-advisors	Over-reliance on automated advice, unsuitable investments	Depends on impact on individuals; may require due diligence

The potential of these high-risk AI systems to produce opaque, automated outcome leads to financial entities to comply with a set of requirements ranging from risk mitigation and human oversight to strict documentation and transparency measures. These go far beyond industry best practices and require the involvement of legal and compliance professionals at every stage of the AI lifecycle.

The AI Act thus marks a new era in financial regulation, one where the legal risk landscape expands to include not just the outcomes of AI decisions, but the integrity, fairness, and traceability of the systems that generate them.

Meeting the Obligations as an Operator of High-Risk AI Systems

Under the AI Act, operators of AI systems are categorized in four roles: providers, deployers, importers, and distributors. While all four carry distinct regulatory responsibilities, financial institutions most commonly act as providers or deployers, either by developing their own AI systems or by integrating third-party solutions into their operations. Roles such as importer or distributor may occasionally apply, particularly when institutions source AI tools from outside the EU or redistribute them internally or to clients, but these are less frequent in traditional banking and insurance settings.



Provider

Develops or significantly modifies an AI system and places it on the EU market under its name. Responsible for design, testing, documentation, and risk management.

Deployer

Uses an AI system in its operations. Ensures correct use, oversight, monitoring, and compliance with the provider's instructions.

Importer

Brings an AI system from a non-EU country into the EU market. Must verify the system meets EU requirements and hold relevant documentation.

Distributor

Makes an AI system available in the EU without modifying it. Ensures the system is compliant and passes on required information and markings.

Providers, those who develop, significantly modify, or place AI systems on the market, must implement a comprehensive risk management system to identify, monitor, and mitigate potential harms throughout the system's lifecycle. This includes ensuring that training, validation, and testing data are relevant, representative, and free from bias, preventing discriminatory outcomes or financial exclusion.

The Act also requires providers to maintain a detailed technical documentation and record-keeping that explain how the AI system works, the logic behind its outputs, and any changes made post-deployment. To protect fundamental rights, human oversight mechanisms must be established to allow human intervention, meaning financial institutions must ensure that humans, not just algorithms, can intervene in, audit, and ultimately override automated decisions when necessary.

Financial institutions acting as deployers or users, those who implement the AI systems developed by third parties, must ensure that these systems are used in compliance with the AI Act. This includes monitoring system performance, maintaining logs, ensuring human oversight, and cooperating with regulators. Deployers must also verify that AI systems are used according to the provider's instructions and conduct impact assessments when required.

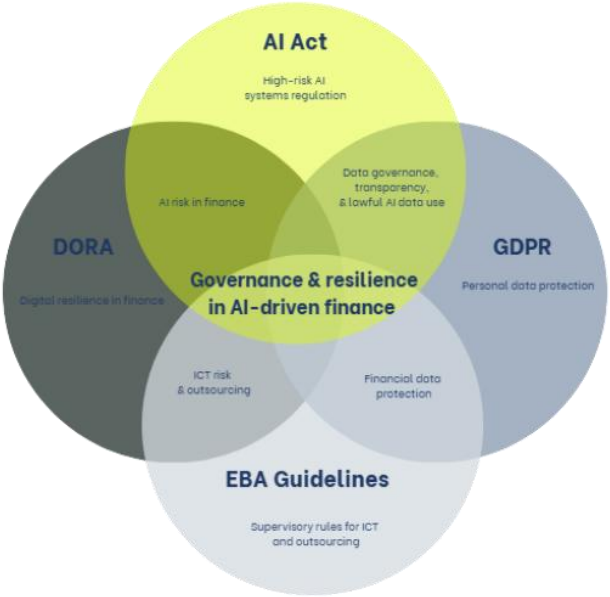
Transparency and information disclosure must be also guaranteed by both providers and deployers, so that affected individuals are adequately informed when interacting with high-risk AI.

These obligations not only introduce operational and legal challenges but also push financial institutions to integrate responsible AI principles into their technology and compliance strategies. This introduces a new dimension of due diligence: institutions can no longer treat third-party tools as black boxes, they must audit, understand, and take legal responsibility for the AI systems they use. AI procurement and deployment are therefore transformed into a regulated supply chain exercise, necessitating closer collaboration between legal, compliance, data science, and procurement teams.

Navigating Interactions with Other Regulations

The AI act being part of Europe's "Digital Decade" completes and interacts with a set of EU regulations that financial institutions must already navigate.

The Digital Operational Resilience Act (DORA), for example, imposes requirements on the resilience of critical ICT systems, including those powered by AI, creating overlaps in areas like risk management, incident reporting, and third-party oversight. Meanwhile, the General Data Protection Regulation (GDPR) adds further complexity, especially where AI systems process personal data. Tensions may arise, for example, between the AI Act's push for transparency and explainability, and GDPR's principle of data minimization. Similarly, the EBA Guidelines on ICT and Security Risk Management already expect banks to assess model risk and system resilience, which will need to be synchronized with the AI Act's requirements for high-risk systems.


AI Act
High-risk AI systems regulation
AI risk in finance
Data governance, transparency, & lawful AI data use
DORA
Digital resilience in finance
GDPR
Personal data protection
Governance & resilience in AI-driven finance
ICT risk & outsourcing
Financial data protection
EBA Guidelines
Supervisory rules for ICT and outsourcing

Rather than treating these frameworks separately, financial entities should pursue an integrated compliance model, mapping controls across regulations, streamlining documentation, and identifying synergies that reduce duplication while enhancing governance.

Turning Compliance into a Strategic Advantage

The AI Act transforms how financial institutions approach their digital transformation and regulatory compliance. Where AI adoption was once primarily seen as a matter of technological innovation or IT governance, it now falls under legal and compliance oversight. It demands an integrated oversight from legal, compliance, data science, IT, and business teams throughout the AI lifecycle. requiring an integrated, multidisciplinary approach. This operational shift requires institutions to build or scale internal governance frameworks that incorporate regulatory scrutiny into AI processes, creating new roles, workflows, and accountability mechanisms.

However, this disruption also presents a unique strategic opportunity to build trust, enhance transparency, and differentiate themselves in a competitive market. By following responsible AI principles, including fairness, explainability, and human oversight, institutions can meet regulations while boosting customer confidence and resilience.

Achieving this strategic advantage requires more than intention—it demands concrete action. Financial institutions must translate these principles into practical governance structures that ensure responsible AI use across all stages.

Next Steps: Building a Robust AI Governance Framework

To effectively navigate the AI Act and transform compliance into a strategic advantage, financial institutions must take deliberate, structured actions. Important upcoming actions include:

- Comprehensive AI Inventory and Classification: Conduct a detailed audit of all AI systems currently in use, categorizing them according to the AI Act's risk levels and, consequently, enabling focused compliance efforts and resource allocation.
- Gap Analysis and Risk Assessment: Evaluate existing AI governance practices against the AI Act's requirements, as well as identify shortcomings in risk management, documentation, transparency, and human oversight to prioritize remediation efforts.
- Policy and Governance Enhancement: Update or establish policies that integrate AI risk management and ethical principles into business processes. This includes revising procurement policies to mandate supplier compliance and contractual obligations related to AI systems.
- Cross-Functional Collaboration: Strengthen partnerships between legal, compliance, data science, IT, and procurement teams. Integrating legal expertise into the AI lifecycle from design to deployment ensures regulatory alignment and reduces risk.
- Training and Awareness: Develop tailored training programs to raise awareness about AI risks and regulatory obligations among all stakeholders, especially decision-makers and technical teams.
- Prepare for Regulatory Engagement: Establish documentation protocols and audit trails demonstrating compliance efforts, enabling smoother regulatory inspections and reinforcing trust with regulators and customers alike.

By integrating these steps into their operational DNA, financial institutions will not only comply with the AI Act but also foster greater innovation, resilience, and customer confidence.

Conclusion: Embracing a New Era of AI-Driven Financial Services

The AI Act marks a pivotal shift for financial institutions, requiring them to view AI not just as technology but as a source of legal and ethical responsibility. Compliance calls for a coordinated effort across legal, risk, and technical teams to ensure AI systems are transparent, fair, and accountable.

While this creates operational challenges, it also offers a promising window to improve confidence, governance and differentiate in a competitive market. Institutions that proactively embrace these changes will be better equipped to innovate safely and lead in responsible AI adoption, securing long-term success in the digital era.

FirmC guides organizations within financial services in their journey towards AI Act compliance. Interested to know more?

References

European Commission. (n.d.). *A Europe fit for the digital age*. Retrieved July 23, 2025, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en

European Union, *Artificial Intelligence Act*, Regulation (EU) 2024/1689. Regulation - EU - 2024/1689 - EN - EUR-Lex