Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

European Union Law Working Papers

No. 121

AI Meets Financial Regulation:
How the EU Is Advancing the Algorithmic Shift

Maria Lucia Passador & Giovanni Bravi

2025

European Union Law Working Papers

Editors: Siegfried Fina and Roland Vogl

About the European Union Law Working Papers

The European Union Law Working Paper Series presents research on the law and policy of the European Union. The objective of the European Union Law Working Paper Series is to share "works in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The working papers can be found at http://ttlf.stanford.edu.

The European Union Law Working Paper Series is a joint initiative of Stanford Law School and the University of Vienna School of Law's LLM Program in European and International Business Law.

If you should have any questions regarding the European Union Law Working Paper Series, please contact Professor Dr. Siegfried Fina, Jean Monnet Professor of European Union Law, or Dr. Roland Vogl, Executive Director of the Stanford Program in Law, Science and Technology, at:

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Authors

Maria Lucia Passador is an Assistant Professor of Corporate Law and Financial Markets Regulation, Bocconi University, Milan; Associated Researcher, European Banking Institute; Research Fellow, Baffi Centre on Economics, Finance and Regulation; Affiliate, Transatlantic Technology Law Forum (TTLF), Stanford Law School.

Giovanni Bravi is an Academic Fellow and PhD Student in Comparative Corporate Law, Bocconi University, Milan.

General Note about the Content

The opinions expressed in this paper are those of the authors and not necessarily those of the Transatlantic Technology Law Forum, or any of TTLF's partner institutions, or the other sponsors of this research project.

Although the paper stems from a joint collaboration, authorship of paragraphs 2, 3.1, and 3.2 is attributable to Giovanni Bravi, while paragraphs 4, 5, 6, and 7 were authored by Maria Lucia Passador. Paragraph 1 was conceived and written jointly.

Suggested Citation

This European Union Law Working Paper should be cited as:
Maria Lucia Passador & Giovanni Bravi, AI Meets Financial Regulation: How the EU is Advancing the Algorithmic Shift, Stanford-Vienna European Union Law Working Paper No. 121, http://ttlf.stanford.edu.

Copyright

Abstract

After considering the evolution of European Union (EU) regulation in tech-related fields and its implications for transatlantic financial markets, this paper specifically examines the EU AI Act and its implications for AI governance and oversight within the financial sector, including its impact on US financial institutions operating in Europe.

More specifically, we will explore the intersection between the AI Act and the ECB's prudential supervisory tasks, assessing the obligations imposed on providers and users of high-risk AI systems within finance. The analysis focuses on the challenges and opportunities presented by the AI Act's governance mechanisms, including the role of the AI Office and the AI Board in ensuring compliance and mitigating risks. Furthermore, the Paper delves into the operational synergy between the AI Office and the ECB, proposing pathways for collaborative regulation that ensures AI innovation aligns with financial stability and ethical standards. The research highlights the critical need for a cohesive supervisory approach that balances the innovative potential of AI with the prudential demands of financial supervision, offering strategic policy recommendations to enhance oversight capabilities while safeguarding the integrity of the financial system. This Paper contributes to the academic discourse by providing insights into the evolving regulatory landscape, with particular attention to navigating the challenges of AI integration in finance from both European and US perspectives.

Table of Contents

1. INTRODUCTION

In the words of the renowned financier John Maynard Keynes, "The difficulty lies not so much in developing new ideas as in escaping from old ones." This paper ventures into the heart of that challenge within the financial markets, where the European Union's Artificial Intelligence Act (the "AI Act" or the "Act") seeks to reshape[1] the landscape by balancing the drive for technological advancement with the weighty responsibility of regulatory oversight. As AI transforms the way we understand risk, governance, and stability of companies and institutions, the AI Act emerges as both a compass and a cautionary tale—steering the financial sector towards a future where innovation and prudence must coexist in harmony. The EU has devised a regulation aimed not at impeding risk, but at managing the varying levels of risk that have arisen so far and may develop in the future.

It is worth remembering that, more broadly, the AI Act aims to harmonize AI governance across the EU, helping to prevent regulatory fragmentation in response to phenomena that are, by nature, cross-border. By establishing a clear legal framework that balances innovation with ethical considerations, the AI Act seeks to create an environment where AI technologies can thrive and be further developed, but not at the expense of public trust or fundamental rights.[2] The Act also introduces mechanisms for AI regulatory sandboxes,

---

[1] The European Union recognizes the AI Act as means to *Shaping Europe's digital future*: see European Commission, AI Act Shaping Europe's Digital Future, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (last visited Apr. 13, 2025). Furthermore, in its AI Continent Action Plan initiative, the European Union stresses its commitment to becoming a global leader in AI, through sustained investment in infrastructure, including computing power and networks, focusing on further development of AI algorithms, leveraging their adoption in the EU's strategic sectors, ensuring access to high-quality data, facilitating compliance with the AI Act and most notably "*maintaining its own distinctive approach to AI*": see Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. AI Continent Action Plan, COM (2025) 165 final (Apr. 9, 2025), https://digital-strategy.ec.europa.eu/en/library/ai-continent-action-plan.

[2] *See* Article 1 of the AI Act, as well as Recitals 3, 5, 68. *See also* Paul Voigt & Nils Hullen, *The EU AI Act, Answers to Frequently Asked Questions* 2 (Springer 2024); Ceyhun Necati Pehlivan, Nikolaus Forgó & Peggy Valck (eds.), *The EU Artificial Intelligence (AI) Act: A Commentary* (Kluwer Law International 2024).

controlled environments where developers can test and refine AI systems before they are deployed outside of the sandbox's scope. These sandboxes offer a flexible regulatory approach, enabling innovation to move forward while ensuring that AI systems are rigorously tested for safety, fairness, and compliance.[3] Like several provisions in the AI Act, they play a key role in shaping best practices throughout the EU.

The global implications of the AI Act are far-reaching. As one of the first comprehensive AI regulatory frameworks in the world, the AI Act sets a high bar for ethical AI governance that other jurisdictions may seek to emulate. The Act's approach to regulating high-risk AI applications through mandatory risk assessments, [4] transparency requirements, [5] and enforcement mechanisms[6] serves as a potential blueprint for international AI governance. By promoting transparency and accountability in AI systems, the EU is positioning itself as a leader in global AI regulation, fostering trust in AI technologies and encouraging others to follow its lead.[7] This regulatory leadership is particularly significant given the ongoing dialogue between EU and US regulators, with American financial institutions naturally looking to the AI Act as a benchmark for their own AI governance frameworks. For US readers, this is more than a distant regulatory experiment in Brussels. If an institution touches European markets—even indirectly through cross-border transactions or subsidiaries—the AI Act sets the standard that may define your compliance obligations tomorrow. In that sense, Europe is not just writing rules for Europe; it is sketching the outlines of a playbook US banks and asset managers may soon be forced to adopt, whether by law or by competitive necessity.

---

[3] *See* Articles 57 to 61 of the AI Act.

[4] *See* Articles 9 and 16 of the AI Act, as well as Recital 65.

[5] *See* Articles 13 and 50 of the AI Act, as well as Recitals 66, 72, 101 and 132.

[6] *See* Articles 88 to 93 of the AI Act.

[7] *See* Recital 5 of the Commission Decision C(2024) 390 final of 24 January 2024 establishing the European Artificial Intelligence Office, 2024 O.J. (C 1459) 1, where the Commission maintains the global vocation of the governance structure for AI in the EU.

In fact, the same rationale that is driving EU-wide harmonization suggests the need for larger-scale collaboration and cooperation mechanisms, as AI development will unlikely see differentiated regional developments. Regulatory differences will inevitably place limits on their use; nonetheless, technological development will progress at its own pace, whether within the European Union or elsewhere. The differences will be appreciated in the regional *applications* and practical uses of such technology. From a global perspective, regulation truly comes in at the nexus between such technology and practical applications, and only limitedly in terms of regional development.[8] This harmonization of AI governance could reduce regulatory fragmentation, facilitate smoother cross-border trade, and ensure that AI systems meet universal safety and ethical standards. This is particularly relevant in the context of AI applications in financial markets. On the one hand, global interconnectedness, the need for uniform compliance, and the cross-border nature of financial transactions necessitate consistent governance frameworks. On the other hand, at EU-level, the integration of financial supervision mandates alignment between AI regulation and sector-specific provisions and supervisors.

For businesses, the AI Act presents both challenges and opportunities. The compliance costs associated with the Act—particularly for high-risk AI applications—are significant. Companies must invest in compliance infrastructure, including hiring specialists to oversee adherence to the Act's requirements, conducting regular audits, and maintaining transparency in AI operations. Larger firms may be well-equipped to meet these demands; by contrast, smaller enterprises could struggle with significant financial and administrative burdens, potentially resulting in market consolidation. However, the Act also incentivizes innovation: it

[8] Development in the region may be directed (e.g., via regulated sandboxes), supervised and reviewed, especially in high-risk areas, but core AI processes and algorithms are likely to cross borders and be implemented elsewhere, within and subject to the limits and constraints of local regulatory frameworks.

provides for regulatory sandboxes, encourages innovation in ethical AI, and promotes the adoption of harmonized technical standards, lowering the compliance costs for innovators. Furthermore, by providing defined regulatory structures it offers a certain level of legal certainty, supporting long-term research investments planning. Overall, companies that develop AI technologies aligned with regulatory standards may gain a competitive advantage in the market. This is particularly relevant for U.S.-based multinational corporations operating in Europe, which must now navigate both American market-driven approaches and European regulatory requirements.

For consumers, the AI Act is a robust safeguard against the misuse of AI. By ensuring that AI systems are transparent, accountable, and ethically governed, the Act protects consumers from the risks of biased decision-making, privacy violations, and unsafe AI applications.[9] Consumers will benefit from greater transparency, particularly in sectors like finance, where AI-driven credit scoring and risk assessments can have a direct impact on individuals' financial opportunities. The Act mandates that consumers be informed when they interact with AI systems,[10] empowering them to challenge decisions and seek redress in cases of harm or unfair treatment.

---

[9] AI depends significantly on vast datasets for training. As it becomes increasingly integrated in businesses and public institutions worldwide, it raises significant concerns around privacy on a massive scale. The OECD AI Principle 1.2 emphasizes the importance of fairness and privacy, among other considerations. The OECD'S "ARTIFICIAL INTELLIGENCE PAPERS NO. 22: AI, DATA GOVERNANCE AND PRIVACY, SYNERGIES, AND AREAS OF INTERNATIONAL COOPERATION" (June 2024), https://doi.org/10.1787/2476b1a4-en, stresses that the OECD AI Principles call for respect for the rule of law, human rights, and democratic values, throughout the entire lifecycle of AI systems (Principle 1.2). They also highlight the importance robustness, security, and safety (Principle 1.4), as well as continued investment in AI research and development (Principle 2.1). AI—when developed and regulated responsibly—may in fact strengthen privacy and data protection. The OECD maintains that advances in AI technologies (and the related governance frameworks) could contribute to strengthening these protections, particularly through privacy-enhancing training methods. This perspective aligns with legislative efforts such as the implementation of the AI Act and the governance framework established therein.

[10] *See* Article 50 of the AI Act.

For policymakers, the AI Act represents a critical opportunity to shape the future of AI governance and AI practical applications, both within the EU and globally. It offers a framework that balances the need for innovation with the imperative to protect public welfare and fundamental rights. Policymakers will need to remain vigilant in updating the Act as AI technologies evolve, ensuring that the regulatory framework keeps pace with the rapid underlying advancements in AI technology. Additionally, the AI Act's emphasis on international cooperation highlights the need for cross-border regulatory alignment, particularly as AI systems increasingly operate in a global context and, as mentioned, are characterized by their ease of cross-border transferability.

This article begins by dissecting the AI Act's foundational elements, including its risk-based framework for categorising AI systems and its governance architecture, which introduces critical entities such as the European Artificial Intelligence Office (AI Office) and the European Artificial Intelligence Board (AI Board).[11]

From there, the narrative weaves into the intricate interplay between these mechanisms and the European Central Bank's (ECB) supervisory mandate, focusing on high-risk AI systems employed in finance—tools integral to credit scoring, fraud detection, and algorithmic trading. The paper highlights the synergies between the AI Office and the ECB, drawing attention to the potential for collaborative governance that harmonises the pursuit of AI-driven innovation with the ethical imperatives of financial stability. Expanding its scope, the piece positions the AI Act within the global regulatory landscape, illustrating how its provisions extend the EU's influence and offer a blueprint for jurisdictions navigating the complexities of AI in financial markets. In doing so, the AI Act may potentially serve as a benchmark for other jurisdictions, therefore fostering global regulatory harmonization and potentially

[11] *See* Section V; *see also* Paul Voigt & Nils Hullen, *The EU AI Act, Answers to Frequently Asked Questions* 162 ff. (Springer 2024).

generating spillover effects to states that traditionally maintain lighter, more permissive regulations. Finally, it reflects on the challenges and opportunities presented by the AI Act, from managing systemic risks to fostering compliance, ensuring alignment with fundamental rights,[12] and safeguarding the resilience of financial systems. Through this layered analysis, the article contributes a picture of the AI governance, financial regulation, and technological innovation in light of the AI Act.

The paper's main contribution to the literature therefore lies in its thorough examination of the AI Act within the context of financial regulation, with particular emphasis on its implications for the supervisory responsibilities of the ECB. Specifically, it offers a distinctive perspective by linking the governance mechanisms introduced by the AI Act with the prudential framework that underpins financial stability. Among the key takeaways are an incisive analysis of the AI Act's risk-based regulatory structure and practical policy proposals aimed at enhancing compliance, mitigating systemic vulnerabilities, and maintaining the integrity of the financial system. By addressing the opportunities and challenges inherent in the integration of AI into finance, this study provides policymakers, financial institutions, and academics with insights into the complex interplay between innovation, regulation, and financial stability, offering a roadmap for navigating these interconnected domains.

[12] On the role of fundamental rights in the design of the AI Act, *see* Marco Almada & Nicolas Petit, The EU AI Act: A Medley of Product Safety and Fundamental Rights, Robert Schuman Centre for Advanced Studies RSC 2023/59, https://ssrn.com/abstract=4308072, according to which the AI Act is fundamentally structured as a product safety regulation, and on how this may determine an inadequate approach to safeguarding fundamental rights within the AI domain, due to a misalignment between the Act's methods and its objectives. On the AI Act being comparable to safety product legislation, *see also* Claudio Novelli, Federico Casolari, Antonino Rotolo, Mariarosaria Taddeo & Luciano Floridi, *AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act*, 3 Digit. Soc'y (2023), n° 13.

2. GENERAL FRAMEWORK AND SCOPE OF THE AI ACT

The European Union's Artificial Intelligence Act (AI Act) represents one of the most comprehensive and ambitious regulatory frameworks for governing the development, deployment, and use of AI technologies. It aims to ensure the safety, transparency, and ethical deployment of AI systems across the EU, particularly in high-risk sectors such as finance,[13] healthcare,[14] law enforcement,[15] administration of justice,[16] and critical infrastructure.[17] With the rapid expansion of AI technologies, which have transformative implications across various industries, the AI Act provides a structured legal response to address both the opportunities and risks posed by AI.

In the financial sector, the AI Act is particularly transformative. Financial institutions increasingly rely on AI for critical processes such as credit scoring, fraud detection, risk assessment, and algorithmic trading.[18] Given the high stakes and potential risks, such as bias in creditworthiness assessments or systemic risks from AI-driven trading systems, the AI Act

---

[13] Fausto Parente, *The AI Act and its impacts on the European financial sector*. The EUROFI Magazine (2024), https://www.eiopa.europa.eu/document/download/5dc730b7-29b6-44dd-819b-3a04476416ed_en?filename=ai-act-fausto-eurofi-magazine_ghent_february-2024%20128.pdf.

[14] *See* Annex III, paragraph 5 of the AI Act. *See also* Recitals 58 and 96.

[15] *See* Annex III, paragraph 6 of the AI Act. *See also* Articles 5, 26, 43, 49 and 74 as well as in Recitals 33, 59, 93, 131 and 159. For flexibility to authorities and to Member States in relation to law enforcement *see* Articles 2, 14, 46, 59 72 and 78 as well as Recitals 22, 130, 132, 141 and 155.

[16] *See* Annex III, paragraph 8 of the AI Act. *See also* Recital 96.

[17] *See* Annex III, paragraph 2 of the AI Act. *See also* Recitals 33, 55, 110 and 155.

[18] For a brief overview of the challenges posed by AI in the context of public administration, *see* Bernd W. Wirtz, Jan C. Weyerer & Benjamin J. Sturm, *The Dark Sides of Artificial Intelligence: An Integrated AI Governance Framework for Public Administration*, 43 INTL J. PUB. ADMIN. 818 (2020). For further analysis of the duty of EU institutions' duty of care towards citizens and related procedural implications, *see* Chryssa Papathanassiou, *Fundamental rights and banking supervision*, 24 J. BANKING REG. 420 (2023); Cary Coglianese, *Administrative law in the automated state*, 150 DAEDALUS 104 (2021) (discussing control of human discretion through the automation of certain administrative tasks); Michèle Finck, *Automated Decision-Making and Administrative Law*, *in* Peter Cane et al. (eds), The Oxford Handbook of Comparative Administrative Law (2021), 657 ff. (discussing on how transparency and accountability of public institutions are put at risk by automated decisions); Izabela Wróbel, *Artificial Intelligence Systems and the Right to Good Administration*, 49 Rev. Eur. & Comp. L. 203 (2022).

imposes strict governance and compliance requirements.[19] Financial entities using or developing high-risk AI must implement comprehensive risk management frameworks,[20] conduct post-market monitoring,[21] and maintain technical documentation that ensures AI systems meet regulatory standards.[22] These measures are essential to prevent discriminatory outcomes and safeguard financial stability.[23] In other words, just as Dodd-Frank was intended to be a sweeping response to systemic risk, designed to rebuild trust, and ultimately reshaped compliance infrastructures across Wall Street, the AI Act is poised to reshape how US institutions manage technological risk in their European operations.

AI is being explored not only by financial institutions for commercial use, but also for regulatory and compliance purposes. The growing adoption of so-called 'RegTech' solutions reflects an increasing interest in harnessing AI to meet regulatory and compliance requirements more effectively and efficiently. Likewise, public authorities are examining the use of AI tools for regulatory, supervisory, and oversight functions—referred to as 'SupTech'. One of the most straightforward yet impactful applications in this field is the use of systematized regulatory reporting and auditable record-keeping—processes that often place a significant burden on supervised institutions.[24]

Moreover, the AI Act establishes a specialized oversight mechanism through the creation of the AI Office (AI Office),[25] which plays a crucial role in supervising AI systems across the

---

[19] Fausto Parente, *The AI Act and its impacts on the European financial sector*. The EUROFI Magazine (2024), https://www.eiopa.europa.eu/document/download/5dc730b7-29b6-44dd-819b-3a04476416ed_en?filename=ai-act-fausto-eurofi-magazine_ghent_february-2024%20128.pdf.

[20] *See*, among others, Article 9 of the AI Act.

[21] *See* Article 72 of the AI Act.

[22] *See*, among others, Articles 11, 16 and 18 of the AI Act.

[23] Alessio Azzutti, Pedro Magalhães Batista & Wolf-Georg Ringe, *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration* (2023). EBI Working Paper Series 2023, no. 140, https://ssrn.com/abstract=4430642.

[24] It is estimated that the sole Bank of England receives one billion rows of data every month, *see* Bank of England, *Future of Finance Report* (June 2019), https://www.bankofengland.co.uk/-/media/boe/files/report/2019/future-of-finance-report.

[25] *See* Section V.

EU, particularly those classified as high-risk. It acts as an enforcement body with the authority to conduct audits, request documentation, and ensure that financial institutions and other organizations deploying high-risk AI systems comply with the stringent requirements outlined in the Act.

The central feature of the AI Act is its risk-based categorization of AI systems, seemingly adopted to avoid over-regulation and to respect the principle of proportionality, while aiming at effectively tackling the issues inherent to AI use.[26] This classification divides AI systems into four tiers based on their potential impact on safety, fundamental rights, and public welfare: (1) unacceptable risk, (2) high-risk, (3) limited risk, and (4) minimal risk. AI systems falling under the "unacceptable risk" category, such as AI used for social scoring or manipulative technologies that can distort human behavior, are outright banned.[27] High-risk AI systems, which include applications in finance, healthcare, and law enforcement, are subject to stringent regulatory requirements. These requirements encompass robust risk management protocols,[28] mandatory transparency in data usage,[29] rigorous human oversight,[30] and security measures to protect individuals from misuse, discrimination, or harm caused by AI technologies.

---

[26] Martin Ebers, *Truly Risk-Based Regulation of Artificial Intelligence: How to Implement the EU's AI Act*, 15 Eur. J. Risk Regul. 1 (2024), https://doi.org/10.1017/err.2024.78 maintains that risk-based regulation should be the approach to AI regulation, but that the AI Act does not fully follow such direction. *See* Recital 26 of the AI Act. *See also* Claudio Novelli, Federico Casolari, Antonino Rotolo, Mariarosaria Taddeo & Luciano Floridi, *AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act*, 3 Digit. Soc'y (2023), n° 13; Claudio Novelli et al., *Taking AI Risks Seriously: A New Assessment Model for the AI Act*, 39 AI & Soc'y 1149 (2024), https://doi.org/10.1007/s00146-023-01723-z.

[27] Under Article 5 of the AI Act, banned practices include harmful manipulation and deception, harmful exploitation of vulnerabilities, social scoring, predictive policing, untargeted scraping of the internet or CCTV material to create or expand facial recognition databases, emotion recognition in workplaces and education institutions, biometric categorisation, and real-time remote biometric identification for law enforcement purposes in public spaces.

[28] *See*, among others, Article 9 of the AI Act.

[29] *See* Articles 13 and 50 of the AI Act, as well as Recitals 66, 72, 101 and 132.

[30] *See*, among others, Article 14 of the AI Act. *See also*, on keeping human oversight at the centre of AI use in finance, Ross P. Buckley, Dirk Andreas Zetzsche, Douglas W. Arner & Brian Tang, *Artificial Intelligence in Finance: Putting the Human in the Loop*, 43 Sydney Law Rev. 43 (2021).

The AI Act identifies high-risk AI systems as those that pose significant risks to health, safety, or fundamental rights. These systems are typically used in critical sectors, where their failure or misuse could have severe consequences. The AI Act provides a detailed list of high-risk AI systems in Annex III—including applications in critical infrastructure, education, employment, law enforcement, migration, justice, and democracy. In addition, an AI system is likely to be classified as high-risk if it is intended to function as a safety component of a product or constitutes a product subject to harmonised legislation requiring third-party conformity assessment.[31]

There are a number of steps that businesses should follow to effectively assess whether their AI systems fall under the "high-risk" category as defined by the AI Act.

First, businesses should review the specific use cases of their AI systems to see if they align with those listed in Annex III of the AI Act, or under the safety component definition of Article 6. For instance, high-risk AI systems in the financial sector may include those used for credit scoring, fraud detection, and algorithmic trading.

Second, one of the primary criteria for determining whether an AI system is high-risk is its potential impact on fundamental rights. Businesses must assess whether their AI systems could adversely affect individuals' rights to privacy, non-discrimination, and human dignity. This involves examining how the system processes personal data, makes decisions, and interacts with users.

Third, businesses should perform a comprehensive risk assessment to evaluate the potential risks associated with their AI systems. This includes identifying and analysing known and foreseeable risks, estimating their likelihood and impact, and determining appropriate risk management measures. The risk assessment should consider factors such as the system's

---

[31] *See* Article 6 of the AI Act; *see also* Paul Voigt & Nils Hullen, *The EU AI Act, Answers to Frequently Asked Questions* 47 (Springer 2024).

complexity, the sensitivity of the data it processes, and the potential consequences of its failure or misuse.

Fourth, the AI Act mandates that high-risk AI systems comply with stringent regulatory requirements, including risk management, data governance, technical documentation, record-keeping, human oversight, accuracy, robustness, cybersecurity, and quality management. Businesses should review these requirements to determine if their AI systems meet the criteria for high-risk classification.

Given the complexity of AI technologies and the evolving regulatory landscape, businesses may benefit from consulting with legal experts, industry specialists, and regulatory authorities. These consultations can provide valuable insights into the classification of AI systems and help ensure compliance with the AI Act.

Fifth, the regulatory environment for AI is dynamic, and updates to the AI Act or related guidelines may affect the classification of high-risk AI systems. Businesses should stay informed about any changes to the legislation and adjust their assessments accordingly.

Finally, to demonstrate compliance with the AI Act, businesses should also document their assessment process thoroughly. This includes maintaining records of risk assessments, consultations, and any measures taken to mitigate identified risks. Proper documentation can also facilitate audits and inspections by regulatory authorities.

Overall, this proactive approach by businesses not only ensures compliance with EU regulations but also promotes ethical and responsible use of AI technologies. For US financial institutions, this step-by-step compliance roadmap offers an immediate template. Even if Congress does not enact a federal AI law soon, adopting AI Act–style risk assessments and documentation practices can function as a form of 'future-proofing'—a strategic investment that minimizes the cost of scrambling once US regulators or courts begin to demand similar

standards. Think of it as training under European gravity: heavier, perhaps, but it builds the memory that will serve you in lighter regulatory environments.

Another defining innovation of the AI Act's is its focus on General Purpose AI (GPAI) models—[32]AI systems capable of performing a wide range of tasks, often developed with minimal constraints on their deployment. GPAI models, which are highly versatile and capable of operating across multiple domains, present unique regulatory challenges. Their broad application makes them integral to financial services, where they are used for everything from customer profiling to product design. The AI Act mandates that providers of GPAI models prioritize transparency by providing detailed technical documentation, including information on the training data used and the governance measures in place. The Act also emphasizes the importance of robust cybersecurity protocols for GPAI models to mitigate risks associated with their deployment, especially in sensitive areas like finance, where AI-driven models are increasingly targeted by cybercriminals. Such specific provisions targeting GPAI model providers are argued in the literature to be not fully consistent with a risk-based approach. Considering that GPAI models are deployed in a wide number of contexts across various industries, establishing clear standards for identifying systemic risks proves challenging. Accordingly, the AI Act does not define them precisely, and refers generally to their negative effects on certain values, such as safety and fundamental rights. This leaves providers with no

[32] Specifically, under Article 3(63) of the AI Act a GPAI-purpose model is defined as an "AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market". *See also* Recitals 97 and 111 of the AI Act. Notably, under Article 53(2) of the AI Act, obligations for providers of GPAI models do not apply as long as the models are released under a free and open-source license, unless they present systemic risks.

substantial guidance on what constitutes systemic risks, and marks a departure in the AI Act from a purely risk-based approach.[33]

In addition to providing detailed oversight mechanisms for high-risk AI systems, the AI Act recognizes the importance of coordination between sector-specific regulators, such as those in the financial industry, and AI-specific oversight bodies.[34] This is particularly significant in the financial sector, where the ECB and other financial supervisory authorities play key roles in ensuring that AI systems do not introduce new risks to financial stability.[35] The AI Act, while focused on technological regulation, complements existing financial regulatory frameworks by imposing AI-specific governance standards on financial institutions. For example, AI systems used in credit institutions must comply with both the AI Act and existing prudential requirements set by financial regulators, ensuring that AI deployment is both safe and aligned with financial stability goals.

3.1. BEFORE THE AI ACT: AI APPLICATIONS IN FINANCIAL MARKETS

The integration of AI into financial markets has been a transformative journey, characterized by steady advancements long before the advent of the AI Act. AI's presence in finance is not a recent phenomenon but one deeply rooted in decades of technological evolution. The foundational ideas laid by pioneers like Alan Turing and John McCarthy in the

[33] Martin Ebers, *Truly Risk-Based Regulation of Artificial Intelligence: How to Implement the EU's AI Act*, 15 Eur. J. Risk Regul. 1, 11 (2024), https://doi.org/10.1017/err.2024.78.

[34] *See* Recital 158 of the AI Act.

[35] *See*, on the purpose of maintaining financial stability after the global financial crisis, amongst many, Deniz Anginer et al., B*ank Regulation and Supervision Ten Years After the Global Financial Crisis*, World Bank Policy Research Working Paper No. 9044 (2020); Daniel K. Tarullo, *Financial Regulation: Still Unsettled a Decade After the Crisis*, 33 J. Econ. Persp. 61 (2019).

mid-20th century set the stage for the AI systems we see today.[36] From the 1980s onward, AI steadily gained traction within financial markets through the application of expert systems and basic algorithms. These early tools were used primarily for predictive modeling, data analysis, and automation of routine tasks. However, AI's capabilities have since expanded dramatically, driven by breakthroughs in machine learning (ML), deep learning (DL), and natural language processing (NLP), allowing financial institutions to utilize AI across a vast array of functions, from complex decision-making to real-time data analysis and autonomous trading.

Despite the significant media attention surrounding the AI Act, the legislation represents merely a regulatory response to an ongoing and long-established transformation, not the genesis of AI's role in finance. The financial industry has been leveraging AI-driven technologies for decades, particularly in areas such as algorithmic trading, high-frequency trading (HFT), risk management, fraud detection, and customer service automation.[37] For instance, algorithmic trading—powered by AI algorithms—has revolutionized stock markets by allowing institutions to execute trades at speeds and volumes far beyond human capability. HFT, which utilizes algorithms to analyze market conditions and execute trades in fractions of a second, became a game-changer as early as the 1990s. Today, the combination of AI and HFT has reshaped market dynamics by introducing unprecedented speed and complexity, but also raising new concerns regarding market volatility, flash crashes, and the concentration of trading power among a small number of players, overall threatening financial stability.[38]

---

[36] *See* Filippo Annunziata, Artificial Intelligence and the Regulation of Market Abuse. A European Perspective (2023), at 30.

[37] Regarding the ramifications of AI on decision-making withing organizations under corporate law, *see* Katja Langenbucher, *AI judgment rule(s)*, 2024, forthcoming. *See also* Maria Lillà Montagnani and Maria Lucia Passador, *Il consiglio di amministrazione nell'era dell'intelligenza artificiale: tra* corporate reporting*, composizione e responsabilità,* Rivista delle società 121 (2021); Maria Lucia Passador, *Il consiglio di amministrazione nell'era dell'intelligenza artificiale: l'importanza della motivazione rafforzata*, Giurisprudenza Italiana 2012 (2022).

[38] *See* Iñaki Aldasoro et al., *Generative artificial intelligence and cyber security in central banking*, BIS Papers No. 145 (2024), https://www.bis.org/publ/bppdf/bispap145.pdf, at 11.

In parallel, AI has become central to other financial services, such as robo-advisory platforms that offer automated, personalized financial advice based on algorithms analyzing individual investment goals, risk tolerance, and market data. These platforms have democratized access to investment management, making professional financial advice accessible to a broader segment of the population. However, while AI-based robo-advisors offer significant advantages in terms of scalability and cost-efficiency, they also present challenges regarding transparency and consumer trust. Clients often struggle to understand how algorithms arrive at specific investment decisions, and the absence of human oversight can lead to a loss of confidence, especially if the AI makes erroneous or suboptimal recommendations. Furthermore, issues of accountability arise when board members or financial advisors rely on AI models that operate as "black boxes,"[39] meaning the decision-making process is not fully explainable or interpretable by humans. This opacity creates regulatory challenges, as firms may face difficulties in justifying the outcomes generated by these systems, particularly if they lead to financial losses.

AI's integration into financial markets has not been without regulatory scrutiny. Long before the AI Act, regulatory frameworks were developed to address the risks associated with AI and automation in finance. For example, the Markets in Financial Instruments Directive (MiFID II) introduced specific provisions to govern algorithmic trading and HFT, mandating greater transparency and accountability from market participants. It required firms to implement robust systems and controls to manage the risks associated with automated trading,

---

[39] Carlos Zednik, *Solving the Black Box Problem: A Normative Framework for Explainable Artificial Intelligence*, 34 Philosophy & Technology 265 (2019); *see also* Alessio Azzutti, Pedro Magalhães Batista & Wolf-Georg Ringe, *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration* (2023), EBI Working Paper Series 2023, No. 140, https://ssrn.com/abstract=4430642, at 14; Alessio Azzutti, Wolf-Georg Ringe & H. Siegfried Stiehl, *Machine Learning, Market Manipulation, and Collusion on Capital Markets: Why the "Black Box" Matters*, 43 U. Pa. J. Int'l L. 79 (2021); *Cf.* Cynthia Rudin, *Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead*, 1 Nat. Mach. Intell. 206, 210 (2019).

including measures to monitor algorithms, conduct regular testing, and ensure appropriate risk management practices. Similarly, the European Securities and Markets Authority (ESMA) issued guidelines to regulate the use of robo-advisors, emphasizing the need for suitability assessments to ensure that automated advice meets the needs of individual clients. Despite these efforts, the rapid advancement of AI technologies has outpaced regulatory developments, leading to ongoing discussions about how to effectively manage the unique risks posed by AI without stifling innovation.

One of the key challenges regulators face is the complexity and opacity of AI models, especially those using deep learning techniques that involve thousands or millions of parameters. These models can generate highly accurate predictions and insights, but their decision-making processes are often not easily interpretable by humans. This lack of transparency complicates efforts to ensure accountability, particularly when AI systems are used to make critical financial decisions. For instance, in high-frequency trading, AI models may execute trades based on patterns or correlations that are not readily apparent to human traders or supervisors. While these models can capitalize on fleeting market opportunities, they also increase the risk of sudden market disruptions if the AI misinterprets data or encounters unforeseen market conditions. Such risks underscore the importance of continuous monitoring and oversight of AI systems to prevent unintended consequences, such as flash crashes or systemic risks resulting from the concentration of AI-powered trading platforms.

To ensure that financial institutions deploy AI responsibly, one proposed approach is the introduction of "personal responsibility" systems. In the wake of the financial crisis, many jurisdictions adopted frameworks that hold directors and senior managers individually accountable through sector-specific regulations. For example, under the governance guidelines

of the European Banking Authority (EBA) and ESMA,[40] so-called key function holders must meet certain criteria—including a good reputation, independence, honesty, and integrity—and must dedicate sufficient time to their roles. This includes a concrete understanding of the key risks facing the business and the establishment of core internal legal and regulatory policies, along with appropriate governance and control systems. Building on this model, extending a system of personal responsibility to the use of technology—particularly AI—could reinforce the principle of human oversight by aligning incentives and ensuring direct accountability.[41]

In addition to these operational risks, AI poses significant challenges in terms of data security and privacy. The increasing reliance on AI for fraud detection and risk management requires access to vast amounts of sensitive financial data, raising concerns about data protection and cybersecurity. Cybersecurity risks associated with AI are multifaceted, and can stem from a variety of sources, including data poisoning, prompt injection attacks, and the exploitation of code vulnerabilities. There is also the risk of AI malfunctions or so-called "hallucinations," where models produce misleading inputs or incorrect outputs. Within the financial system, such risks can have significant consequences—not only for day-to-day operations but also for the reputations of market participants and regulators alike. This, in turn, can erode public *trust* in the banking system and potentially give rise to systemic risks.

Financial institutions must balance the need for advanced AI-driven tools with the imperative to protect clients' personal and financial information.[42] Unauthorized access to AI

---

[40] EBA & ESMA, *Joint Guidelines on the Assessment of the Suitability of Members of the Management Body and Key Function Holders* (ESMA35-36-2319; EBA/GL/2021/06) (2021), https://www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2021/EBA-GL-2021-06%20Joint%20GLs%20on%20the%20assessment%20of%20suitability%20%28fit%26propoer%29/1022127/Final%20report%20on%20joint%20EBA%20and%20ESMA%20GL%20on%20the%20assessment%20of%20suitability.pdf.

[41] Ross P. Buckley, Dirk Andreas Zetzsche, Douglas W. Arner & Brian Tang, *Artificial Intelligence in Finance: Putting the Human in the Loop*, 43 Sydney L. Rev. 43 (2021), 66 ff.

[42] For an analysis on cybersecurity in the financial sector, *see* Christian Calliess & Ansgar Baumgarten, *Cybersecurity in the EU: The Example of the Financial Sector—A Legal Perspective*, 21 GERMAN L.J. 1149 (2020).

systems or the disclosure of sensitive data could undermine trust in financial institutions and potentially threaten financial stability on a larger scale. Regulators are therefore focused on strengthening cybersecurity frameworks and ensuring that AI technologies comply with data protection laws, such as the General Data Protection Regulation (GDPR) in the European Union, which gives individuals the right to understand and challenge automated decisions that affect them.

Ultimately, while the AI Act represents a formal acknowledgment of AI's growing role in the financial sector, it is not the starting point of AI's involvement. Financial markets have long been at the forefront of technological innovation, and AI has been a critical enabler of this transformation. The challenge now lies in creating a balanced regulatory environment that fosters innovation while mitigating the inherent risks associated with AI. This requires a nuanced understanding of the various applications of AI in finance, from robo-advisors to algorithmic trading, and a willingness to adapt regulatory frameworks as the technology continues to evolve. In doing so, policymakers can ensure that AI serves as a tool for enhancing financial markets, rather than a source of systemic risk or consumer harm. Therefore, while the AI Act is an important step forward, it is only one part of a much larger and ongoing conversation about the role of AI in modern finance.

AI has seamlessly embedded itself within the financial sector, profoundly transforming numerous facets of banking, investment, and regulatory compliance. The incorporation of AI technologies has fostered remarkable progress in efficiency, precision, and customer service, whilst simultaneously introducing new challenges and risks that require prudent management.

One notable innovation lies in the deployment of AI-driven robo-advisors, which are revolutionising investment management by offering automated portfolio management tools. These systems utilise advanced algorithms to deliver bespoke investment advice tailored to the individual profiles of clients. To illustrate, tools such as Wealthfront's retirement planning

instrument and Betterment's AI-powered back-office functions serve as prime examples of how AI optimises client portfolios and enhances the overall investment process.[43]

Equally transformative is AI's role in credit risk assessment, where it significantly enhances the accuracy of models that predict creditworthiness. For banks, this capability is vital in managing risk exposure and making informed lending decisions. Institutions are actively considering the integration of AI across the entire credit life cycle.[44] Starting from client engagement, AI models can create highly personalized product offerings tailored to individual clients or firms. Then, during the credit decision and underwriting phases, AI can review documentation, identifying policy breaches or missing data, perform credit analyses, and produce first drafts of credit memos. Contracting processes may also be significantly streamlined through the use of AI automation. In terms of portfolio monitoring, AI tools can then aid portfolio managers in drafting risk reports, optimizing portfolio options, or even developing subsegment-specific strategies aligned with specific risk propensity. Finally, even customer assistance processes may be enhanced by generative AI systems, for instance by generating customized communications and identifying appropriate restructuring options where necessary or required.

AI also plays a crucial role in the detection of fraudulent activity. Through the analysis of transaction patterns and the identification of anomalies in real time, machine learning algorithms can learn from historical data to detect suspicious behaviour, thus preventing fraud before it escalates.

---

[43] *See* European Parliament, Study requested by the ECON Committee, Robo-advisors How do they fit in the existing EU regulatory framework, in particular with regard to investor protection? (June 2021), ESMA, Artificial intelligence in EU securities markets (Feb. 2023), https://www.esma.europa.eu/sites/default/files/library/ESMA50-164-6247-AI_in_securities_markets.pdf, and Filippo Annunziata, Artificial Intelligence and the Regulation of Market Abuse. A European Perspective (2023), at 38.

[44] Andreas Kremer et al., *Embracing Generative AI in Credit Risk*, McKinsey & Co. (July 1, 2024), https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/embracing-generative-ai-in-credit-risk.

Moreover, AI algorithms are at the forefront of algorithmic and high-frequency trading (HFT), executing orders at extraordinary speeds and volumes, sometimes within milliseconds. These systems analyse market data, identify trading opportunities, and execute trades with minimal human involvement.[45]

Several real-world examples from both sides of the Atlantic vividly illustrate the growing prominence of AI in the financial sector. For instance, leading American robo-advisors such as Wealthfront and Betterment rely on AI to deliver personalised investment advice and manage retirement planning. Wealthfront's "Path" tool employs AI to address queries regarding retirement preparedness and housing affordability, while Betterment utilises AI to streamline back-office functions such as cheque processing.

Another compelling case from the US financial sector is JP Morgan's COiN (Contract Intelligence), a machine-learning system designed to review legal documents and extract critical data points, thus reducing the time required for document analysis and improving accuracy.

ZestFinance offers an alternative approach by employing AI in credit scoring, using alternative data sources to assess creditworthiness. This innovation enables lenders to evaluate individuals who may lack a traditional credit history, thereby broadening access to credit.

Finally, Kensho Technologies, acquired by S&P Global, harnesses AI to analyse financial markets and provide insights into trends. Their platform processes vast amounts of data to generate predictive analytics that support informed investment decisions.

As AI continues to revolutionise the industry, it offers an array of advancements designed to enhance efficiency, improve risk management, and refine customer service.

---

[45] ESMA, Artificial Intelligence in Securities Markets (Feb. 1, 2023), ESMA50-164-6247, https://www.esma.europa.eu/sites/default/files/library/ESMA50-164-6247-AI_in_securities_markets.pdf and CFA Institute, AI Pioneers in Investment Management (2019), https://www.cfainstitute.org/- /media/documents/survey/AI-Pioneers-inInvestment-Management.pdf

However, along with these advantages, the implementation of AI introduces substantial risks that must be judiciously managed to safeguard the stability and integrity of financial systems.

Among the many benefits AI presents is its capacity to automate routine tasks, such as data entry, transaction processing, and customer service interactions, thereby significantly reducing operational costs while enhancing overall efficiency. The introduction of AI-driven chatbots, for instance, enables instant responses to customer queries, delivering a more efficient and personalised service.

Equally important is AI's role in refining risk management practices. By analysing vast datasets to discern patterns and predict potential risks, AI becomes invaluable in areas like credit risk assessment, fraud detection, and market analysis. With the ability to process both conventional and alternative data, AI empowers financial institutions to make well-informed decisions.

AI's contribution to fraud detection should not be understated. Through machine learning algorithms, AI systems learn from historical data, allowing them to identify anomalies and suspicious activities in real-time. This capability is instrumental in preventing fraud and protecting both financial institutions and their clients from financial crime.

Optimising investment strategies is another arena where AI excels. Robo-advisors, for instance, employ algorithms to provide personalised investment advice and simultaneously analyse market trends to make data-driven decisions. This results in more efficient portfolio management, as demonstrated by platforms such as Wealthfront and Betterment, which exemplify how AI streamlines the investment process. These examples matter for US readers because they show how the very tools celebrated as innovations on Wall Street—robo-advisors, alternative credit scoring, automated contract review—are the ones most likely to trigger 'high-risk' classification under the EU Act. In other words: the US success stories are precisely the systems Europe now wants to regulate most tightly.

Moreover, AI aids financial institutions in meeting regulatory requirements by automating the analysis of large datasets. This capability minimises the risk of non-compliance and the penalties associated with it, ensuring that institutions remain aligned with legal standards.

Lastly, AI's ability to analyse customer data offers insights into behaviour and preferences, thereby allowing institutions to tailor products and services to individual needs. This not only enhances customer satisfaction but also fosters greater loyalty.

However, the benefits of AI are accompanied by certain risks. One significant concern is the potential for AI systems to perpetuate biases present in their training data, resulting in discriminatory outcomes. For instance, biased credit scoring models may unfairly disadvantage particular groups. Addressing fairness and transparency in AI decision-making is critical to mitigate such risks.

The lack of transparency and explainability within many AI models, particularly those based on deep learning, also poses challenges. These models often operate as 'black boxes,'[46] making it difficult to comprehend how decisions are reached. This opacity can undermine both regulatory compliance and customer trust.

Another key risk lies in cybersecurity. The intricate nature of AI systems renders them vulnerable to cyber-attacks and data manipulation. Safeguarding the security and integrity of AI-driven financial systems is imperative to prevent breaches that could expose sensitive data or disrupt operations.

---

[46] Carlos Zednik, *Solving the Black Box Problem: A Normative Framework for Explainable Artificial Intelligence*, 34 Philosophy & Technology 265 (2019); *see also* Alessio Azzutti, Pedro Magalhães Batista & Wolf-Georg Ringe, *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration* (2023), EBI Working Paper Series 2023, No. 140, https://ssrn.com/abstract=4430642, at 14; Alessio Azzutti, Wolf-Georg Ringe & H. Siegfried Stiehl, *Machine Learning, Market Manipulation, and Collusion on Capital Markets: Why the "Black Box" Matters*, 43 U. Pa. J. Int'l L. 79 (2021); *Cf.* Cynthia Rudin, *Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead*, 1 Nat. Mach. Intell. 206, 210 (2019).

Operational risks are inherent in AI models, which may fail unexpectedly. For example, errors in algorithmic trading systems can lead to substantial financial losses. Thus, comprehensive testing and validation processes are essential to ensuring AI systems' reliability.

Furthermore, the reliance on a limited number of AI technology providers introduces concentration risk. Should these providers face operational difficulties or if systemic issues with AI technology arise, widespread disruptions to banking operations could ensue.

Finally, regulatory frameworks may struggle to keep pace with AI's rapid advancement, creating challenges for financial institutions. Ensuring that AI applications remain compliant with existing regulations, while also adapting to emerging requirements, demands careful navigation.

3.2. BEFORE THE AI ACT: AI APPLICATIONS IN BANKING SUPERVISION

In the field of banking oversight, AI has emerged as a pivotal tool, helping to address some of the key challenges posed by the complexity and interconnectedness of modern financial systems. Following the 2008 financial crisis and the ensuing sovereign debt crisis, the need for stronger, more dynamic banking supervision within the European Union became critical.[47] The creation of the Single Supervisory Mechanism (SSM) was a direct response to this, designed to break the harmful link between banks and sovereign states and safeguard the stability of the eurozone's financial system.[48] However, as seen in the case of Landesbank

[47] Christoph Ohler, *Banking Supervision*, *in* The EU Law of Economic and Monetary Union, Fabian Amtenbrink & Christoph Herrmann (eds.) (2020), chapter 37, paragraph 37.83, at 1119 and 1136; Kern Alexander, *The European Central Bank and Banking Supervision: The Regulatory Limits of the Single Supervisory Mechanism*, 24 Eur. Comp. & Fin. L. Rev. 467 (2016), at 486, stating that: "[b]anking supervision, on the other hand, has a wider number of—often conflicting—objectives: financial stability, investor and depositor protection, consumer protection, and financial crime"; and Avinash D. Persaud, The Role of Policy and Banking Supervision in the Light of the Credit Crisis (2010), at 160.

[48] The origins of the SSM can be traced back to intense debates within the Delors Committee in the late 1980s and the development of the Maastricht Treaty in 1991, which expanded to conduct both pre-

Baden-Württemberg (LBBW), even with these reforms in place, significant structural and operational weaknesses remain.[49] LBBW's struggles exposed the limitations of traditional supervisory frameworks, highlighting the need for more advanced, adaptive, and technology-driven tools to keep pace with the evolving financial landscape.

AI holds the potential to revolutionise banking supervision by offering more efficient, precise, and forward-looking tools for both micro- and macro-prudential oversight. At the micro level, AI's ability to process vast datasets enables regulators to assess the specific risks faced by individual institutions with far greater accuracy. By deploying advanced predictive algorithms, AI can simulate how these risks could ripple through the financial system, potentially triggering wider macro-level disruptions. In the case of LBBW, AI could have been used to flag early signs of distress by identifying unusual patterns or irregularities in the bank's activities that might have gone unnoticed by conventional methods.

At the macro level, AI enables a more comprehensive view of systemic risks by analysing the complex interconnections between banks, markets, and sovereign entities. The case of LBBW highlighted how such interdependencies can exacerbate financial instability. With AI, supervisors could more effectively monitor these linkages, identifying vulnerabilities within the broader financial system that traditional models often fail to capture. This capability is

---

crisis prudential oversight and post-crisis resolution mechanisms. *See also* Kern Alexander, *The European Central Bank and Banking Supervision: The Regulatory Limits of the Single Supervisory Mechanism*, 33 Y.B. Eur. L. 417 (2014), at 418 and 422; Ohler Christoph, *Banking Supervision*, *in* The EU Law of Economic and Monetary Union, Amtenbrink Fabian & Christoph Herrmann (eds.) (2020), paragraph 37.20.

[49] Filippo Annunziata, *I «postumi» del caso* Landesbank vs. BCE, Analisi Giuridica dell'Economia 409 (2018) (multiple issues connected to the operational structure of financial regulation and supervision in the EU are analysed, starting from pointing out that the ECB is entrusted with responsibilities and powers of prudential supervision over all credit institutions in the Euro-area falling under the SSM. The ECB exercises these powers directly with regard to relevant banks, and mandates the exercise of these duties concerning less significant banks to national supervisory authorities. In the *Landesbank Baden-Württemberg* case, the Court refers to this structure as a "decentralized implementation" of supervisory powers, which, according to the Author, brings to the forefront the fundamental challenge of clear delineation of the roles between the ECB and national authorities under the SSM system).

especially important in a financial environment where risks are increasingly spread across markets and jurisdictions, requiring a more holistic and integrated approach to supervision.

One of AI'S most valuable contributions is in its ability to offer real-time monitoring of financial institutions.[50] Traditional supervisory approaches often rely on periodic reviews of data, which can result in delays between the identification of risks and the response. AI, by contrast, processes data continuously, enabling supervisors to detect emerging risks in real time and take pre-emptive action. In the context of LBBW, the ability to monitor the bank's health on a continual basis could have facilitated earlier intervention, potentially mitigating the severity of its difficulties before they escalated into a larger crisis.

Furthermore, AI can process unstructured data sources such as financial statements, market sentiment, or even social media trends through advanced techniques like natural language processing (NLP). This allows supervisors to gain insights that go beyond what traditional financial metrics reveal, providing a fuller understanding of the risks facing an institution. In the case of LBBW, AI could have been instrumental in identifying less obvious risk factors or shifts in market sentiment that contributed to the bank's problems.

AI also offers the advantage of ensuring greater consistency and transparency in the application of supervisory standards. Given the fragmented nature of banking supervision across the EU, where national competent authorities (NCAs) and the ECB must work together under the SSM, AI could provide a more unified approach to supervision. By using rule-based algorithms and data-driven tools, AI can help ensure that supervisory measures are applied evenly across different jurisdictions, reducing the risk of inconsistencies that could undermine the effectiveness of the overall system. In the case of LBBW, such tools might have helped

[50] Financial institutions are subject to the monitoring obligations of deployers to ensure the proper functioning of high-risk AI systems. They must report any serious incidents or malfunctioning to the competent authorities and take corrective measures (Articles 21 and 26 of the AI Act).

streamline communication and cooperation between the ECB and German supervisory authorities, enabling a more coordinated and efficient response.

However, even though AI holds significant promise for strengthening banking supervision, it also raises important concerns around governance and accountability. As powerful as these technologies are, they must be carefully integrated into existing supervisory frameworks to ensure that human judgment and oversight are not entirely displaced. In the case of LBBW, for instance, AI might have uncovered risks earlier, but the final decisions about how to address those risks must ultimately rest with human supervisors, who are responsible for ensuring that regulatory interventions are proportionate and fair.

Hence, AI offers a profound opportunity to transform banking supervision, providing the tools necessary to address the structural challenges brought to light by cases such as LBBW. By enabling more precise risk assessments, facilitating real-time monitoring, and promoting greater consistency in the application of supervisory standards, AI can play a crucial role in strengthening the resilience of the financial system. Nonetheless, as regulators integrate AI into their processes, they must do so in a way that upholds the principles of sound governance and ensures that human oversight remains central to the supervisory process.

4. AI ACT ERA: THE EUROPEAN UNION'S WORLDWIDE REGULATORY AMBITIONS AND TRANSATLANTIC IMPLICATIONS

The AI Act represents a significant milestone in the EU's regulatory strategy, positioning the European Union as a key global leader in the governance of emerging technologies. In the context of comparative financial market regulation, it extends the EU's influence, much like the GDPR, by setting stringent standards that transcend EU borders. The Act not only regulates artificial intelligence but also shapes the international regulatory discourse,

particularly in the financial sector, where AI is becoming increasingly integral. The EU expressly acknowledges its "distinctive approach to AI", which includes capitalizing on its strengths, such as having a large single market with one set of harmonized rules aligned with EU values, like the AI Act. At the same, the EU recognizes the importance of facilitating compliance with the AI Act, particularly for smaller innovators.[51]

Financial markets are rapidly evolving, driven by AI's capabilities in areas such as high-frequency trading, algorithmic risk assessment, fraud detection, and regulatory compliance automation. The AI Act imposes a structured and risk-based approach to AI development and deployment, which contrasts with more laissez-faire models, notably the United States' more market-driven and fragmented approach to AI governance, exemplified by the patchwork of state-level initiatives and federal agency guidance rather than comprehensive federal legislation. This regulatory divergence underscores the EU's intent to establish a more ethical, accountable, and transparent framework that places a strong emphasis on human oversight and societal impact. In doing so, the AI Act contributes to a broader comparative legal framework that is deeply embedded in the EU's regulatory philosophy, which seeks to mitigate systemic risks and safeguard public interests, particularly in critical sectors such as finance.

Within the comparative regulatory landscape, the AI Act can be seen as part of the EU's broader effort to assert itself as a standard-setter in global financial markets, particularly in the governance of digital technologies. This effort is also evident in the Markets in Crypto-Assets Regulation (MICAR), which similarly seeks to regulate emerging technologies and their impact on financial systems. The AI Act's extraterritorial scope—requiring compliance from any non-EU companies that market or deploy AI systems within the EU—mirrors the extraterritoriality

[51] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. AI Continent Action Plan, COM (2025) 165 final (Apr. 9, 2025), https://digital-strategy.ec.europa.eu/en/library/ai-continent-action-plan.

of the GDPR and reflects the EU's broader ambition to extend its regulatory influence globally. This aspect is particularly important in financial markets, where AI systems used for trading, analytics, and risk management have far-reaching implications, not only for market efficiency but also for systemic stability and investor protection.

The AI Act's focus on risk management is central to its framework. It introduces a tiered system of AI categorization based on risk, with the highest-risk AI systems subject to the most stringent regulatory requirements, in addition to outright bans for "unacceptable" risks.[52] In financial markets, this could mean that AI systems used in critical functions—such as market-making algorithms or fraud detection tools—would face rigorous scrutiny to ensure they meet the EU's safety, transparency, and fairness standards. This is in stark contrast to the US approach, which is largely reactive and driven by industry self-regulation rather than comprehensive legislative frameworks.

Moreover, the AI Act enhances the EU's role in shaping international financial law by integrating AI regulation into corporate governance frameworks. As companies increasingly rely on AI for decision-making, compliance, and operations, the AI Act imposes a direct obligation on firms to ensure their AI systems adhere to principles of accountability, transparency, and robustness. This approach aligns with the broader trend in EU law to enhance corporate responsibility, particularly as seen in other regulatory initiatives like the Corporate Sustainability Reporting Directive (CSRD).[53] This integration of AI governance into

---

[52] See Section II of this Paper; *see also* Article 5 of the AI Act.

[53] *See* Tatiana Pantazi, *The Introduction of Mandatory Corporate Sustainability Reporting in the EU and the Question of Enforcement*, 25 Eur. Bus. Org. L. Rev. 509 (2024), https://doi.org/10.1007/s40804-024-00320-x; Marloes Brans, Ronnie Bloemberg & Felix Felder, *Reporting under the 'E' of the CSRD: An Overview of Legal Requirements and a Comparison With Existing Obligations under Environmental Law, Focusing on the Netherlands*, 33 Eur. Energy & Env't L. Rev. 232 (2024), https://doi.org/10.54648/eelr2024015; Felix E. Mezzanotte, *Corporate Sustainability Reporting: Double Materiality, Impacts, and Legal Risk*, 23 J. Corp. L. Stud. 633 (2023), https://doi.org/10.1080/14735970.2024.2319058.

corporate law reinforces the EU's holistic regulatory approach, blending technology, corporate responsibility, and financial market stability into a unified framework.

In terms of comparative regulatory impact, the AI Act challenges the dominance of the traditional U.S.-led model of technology regulation, which has historically influenced global tech governance through Silicon Valley's market leadership. The American model, characterized by minimal interference, tends to prioritize rapid technological advancement and market efficiency, often at the expense of regulatory oversight. In contrast, the EU's AI Act imposes a precautionary, human-centric framework that prioritizes ethical considerations, consumer protection, and systemic risk mitigation. This divergence not only highlights a fundamental difference in regulatory philosophy but also positions the EU as a counterbalance to US influence in global financial market governance.

The AI Act's influence will likely ripple beyond Europe's borders, affecting multinational corporations and financial institutions that use AI in their global operations. These entities will need to navigate a complex regulatory landscape, balancing compliance with the EU's stringent AI requirements against more lenient jurisdictions. This could create a "compliance spillover," where companies standardize their AI practices globally to meet the highest regulatory requirements—those of the EU—thus exporting EU standards worldwide, much as the GDPR has done in data protection. The extraterritoriality effect[54] ensure that AI systems used within the EU meet strict standards of safety, transparency, and respect for fundamental rights, irrespective of the geographic location of the companies involved. [55] Major US financial institutions with European operations, such as JP Morgan, Goldman Sachs, and Citigroup, are

[54] Article 2(1)(c) of the AI Act states that its scope of application extends to "providers placing on the market or putting into service AI systems or placing on the market general-purpose AI models in the Union, irrespective of whether those providers are established or located within the Union or in a third country".

[55] On the extraterritorial effects of the AI Act and MICAR, *see* Maria Lucia Passador, *Transcending Boundaries in the Age of International Corporate and Financial Law: between American Echoes and European Whispers*, 39 Emory Int'l L. Rev. 569 (2025).

already adapting their AI systems to meet EU requirements, demonstrating the Act's practical influence on American financial practices. Hence, for a US compliance officer or general counsel, this means that the AI Act is not optional reading: it is already shaping boardroom decisions in Manhattan and regulatory strategies in Washington. Indeed, the question is not whether the US will feel the ripple effects, but how quickly. Firms that wait for domestic regulators to act may find themselves playing catch-up to competitors that have internalized the EU model early on.

Of particular note is the broad scope of the Act, which applies to any organisation offering AI systems in the EU market, regardless of its base of operations. This necessitates compliance from non-EU businesses, should they wish to provide AI products or services to European customers.

Non-EU companies are subject to the same rigorous obligations as their EU counterparts, especially in relation to high-risk AI systems. These obligations encompass the need for thorough risk assessments, adherence to stringent data quality standards, maintenance of detailed technical documentation, and the implementation of robust human oversight mechanisms.

Additionally, the Act places great emphasis on transparency and accountability. Businesses from outside the EU must clearly explain the workings of their AI systems and ensure these systems are open to audit. This includes providing summaries of the training data used and ensuring that copyright is respected.

The legislation also enforces high ethical standards, prohibiting certain AI practices such as social scoring and manipulative activities. To remain compliant, non-EU companies must ensure their AI systems do not partake in any of these banned activities.

In comparative politics terms, the AI Act also illustrates the emergence of competing governance models: the EU's rights-based regulatory state, the US market-driven system, and

China's state-centric, security-oriented approach. Financial markets become one of the arenas where these philosophies clash and converge, with global firms forced to arbitrate among them.

For businesses outside the EU, the implications of the AI Act are manifold. Chief among these is the necessity to comply with the Act in order to maintain or gain access to the lucrative EU market. Achieving this compliance ensures that companies can continue to offer their services without facing legal obstructions.

Furthermore, the Act may compel non-EU companies to re-evaluate and adjust their operational practices. This could include revamping data governance structures, increasing transparency efforts, and reinforcing their risk management frameworks.

However, aligning with the AI Act's requirements can also offer distinct advantages. Businesses that demonstrate compliance may be able to distinguish themselves by offering AI solutions that are perceived as more trustworthy and reliable. Such alignment not only bolsters a company's standing in the global market but also showcases a commitment to ethical and responsible innovation.

The risks of non-compliance are significant, with the Act imposing fines of up to €35 million or 7% of a company's annual global turnover for the most serious violations.[56] Thus, it is imperative that non-EU businesses assess these risks with care and take proactive measures to mitigate them. Unlike in Europe, where enforcement will be primarily administrative, American firms must also anticipate the possibility of private litigation. Class actions—long a feature of the US legal landscape—could emerge around AI bias, discrimination, or algorithmic opacity, especially if plaintiffs' attorneys frame EU compliance gaps as evidence of negligence in US courts.

[56] See Article 99 of the AI Act.

Beyond its regulatory challenges, the AI Act fosters an environment conducive to responsible innovation. By adhering to its guidelines, non-EU companies can not only ensure the safety and ethics of their technologies but also collaborate more effectively with EU-based entities in a harmonised regulatory framework.

So, the EU's AI Act imposes stringent obligations on companies outside the EU that wish to engage with the European market. While adapting to these regulations poses certain operational challenges, it also offers opportunities to innovate within a framework that prioritises ethical standards, transparency, and the safeguarding of fundamental rights.

Finally, the AI Act contributes to the evolving concept of International Corporate and Financial Law (ICFL) by introducing a new layer of governance in the cross-border use of AI technologies within financial markets. As financial institutions increasingly adopt AI across various jurisdictions, the AI Act's regulatory framework will interact with other national regulations, potentially creating both convergence and conflict. This interaction may lead to new forms of regulatory harmonization in international financial law, with the EU's AI governance model serving as a template for other jurisdictions, including the U.S., where discussions on AI regulation are still in nascent stages. Ultimately, the AI Act underscores the EU's growing role as a global regulatory leader, setting standards that not only shape the internal EU market but also influence global financial systems and corporate governance frameworks. Overall, the European Union recognizes that the AI Act constitutes only an initial step in the regulation of a complex, swiftly advancing technology. The development of standards and codes of practice will be paramount, and the European Commission will need to provide constant guidance on the application of the Act within relevant sectoral legislation. During the initial phase of the Act's application the Commission will engage in public consultations, and overall focus on identifying any further measure that might be needed to

facilitate streamlined and simple application of the Act, taking into account especially the needs of smaller companies.[57]

5. GOVERNANCE IN THE AGE OF THE AI ACT

The AI Act proposes a comprehensive governance framework,[58] involving national and supranational entities, with the express purpose of overseeing the advancements in AI models (including GPAI models), the interaction with the scientific community, and playing a fundamental role in enforcement, investigations and testing. With, admittedly, a *global vocation*.[59]

The governance framework consists of several key EU entities. First, the AI Board which, comprising representatives from Member States and with the European Data Protection Supervisor acting as an observer, provides guidance and support to both the EU Commission and Member States on AI-related issues, thereby ensuring a consistent and effective application of the AI Act.[60] It is expected to serve as a key facilitator of coordination among Member States and other relevant stakeholders, promoting best practices, providing consultation, and fostering cooperation in AI governance and awareness initiatives. [61] Moreover, it extends its support to national competent authorities by offering guidance on regulatory sandboxes and other compliance measures, assisting them in their implementation of the AI Act.

---

[57] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. AI Continent Action Plan, COM (2025) 165 final (Apr. 9, 2025), https://digital-strategy.ec.europa.eu/en/library/ai-continent-action-plan.

[58] See Paul Voigt, Nils Hullen, *The EU AI Act, Answers to Frequently Asked Questions*, 162 ff. (Springer 2024).

[59] *See* Recital 5 of the Commission Decision C(2024) 390 final of 24 January 2024 establishing the European Artificial Intelligence Office, 2024 O.J. (C 1459) 1.

[60] *See* Article 65 of the AI Act, as well as Recitals 148 and 149.

[61] Claudio Novelli et al., *A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities*, 15 Eur. J. Risk Regul. 1, 11 (2024).

Second, the AI Office. Specifically introduced by the AI Act and located within the EU Commission's Directorate-General for Communication Networks, Content, and Technology (DG-CNECT), this entity, whose precise internal composition and organizational structure remains to be clarified, has been tasked with overseeing compliance with the AI Act itself,[62] encouraging ethical AI practices, promoting collaboration among a wide range of stakeholders, preventing misuse, supporting innovation, and providing expert guidance.[63] The AI Office is overall expected to focus on regulatory oversight and enforcement, with functions to a certain extent to a certain extent to those of the AI Board.[64]

Hence, it undertakes a pivotal role in supervising AI systems, particularly high-risk and General Purpose AI (GPAI) models.[65] Its functions encompass a wide array of responsibilities.

The AI Office is entrusted with the task of monitoring and enforcing compliance with the AI Act.[66] In this capacity, it engages in structured dialogues with AI providers, requesting information and documentation,[67] conducting thorough evaluations, and taking measures to ensure regulatory compliance or mitigate potential risks.[68]

Further, the AI Office takes proactive steps to prevent the misuse of AI systems by promoting the creation of codes of practice and voluntary guidelines. In close collaboration

---

[62] *See* Recital 148 of the AI Act.

[63] Moreover, the EU Commission will establish AI testing support structures for market surveillance and compliance (Article 84 of the AI Act), create a common EU database for registering high-risk AI systems, and require providers to implement post-market monitoring systems and comply with AI Act regulations.

[64] For an analysis of the functions of the AI Office, *see also* Maria Lucia Passador, *AI in the Vault: AI Act's Impact on Financial Regulation. Bocconi Legal Studies Research Paper No. 4898828,* 56 Loy. U. Chi. L. Rev. (2025), forthcoming, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4898828.

[65] *See* Recitals 162 and 164 of the AI Act.

[66] Penalties for non-compliance can reach up to 35 million EUR or 7% of annual worldwide turnover for prohibited AI practices (Articles 99(3) and 101(1) of the AI Act). Confidentiality obligations will apply to all actors involved in the AI Act's application, respecting intellectual property rights and trade secrets (Articles 53(1)(b), and 78, as well as Recitals 107, 151, 154 and 167).

[67] *See* Article 92(7) of the AI Act and Recital 164.

[68] *See* Articles 92(1) and 93 of the AI Act, as well as Recital 164.

with national competent authorities, civil society organisations, experts, and other AI bodies, it seeks to foster the development of trustworthy and ethical AI frameworks.[69]

As an expert body, the AI Office offers crucial support to national authorities by sharing expert knowledge, assisting the AI Board, and facilitating joint investigations conducted by market surveillance authorities.[70]

Public outreach is another key responsibility, with the AI Office coordinating communication efforts aimed at raising awareness of the AI Act's obligations. It also provides a platform for disseminating information and maintains a public register of AI sandboxes.

In addition to overseeing the implementation of the AI Act, the AI Office ensures that all regulatory obligations are met, and it also guarantees procedural rights to economic operators of GPAI models, enabling them to challenge any alleged infringements of the Act.

Recently, the European Commission has announced that a special AI Service Desk will be created inside the AI Office, aiming at becoming a central point of contact for providing information and guidance to businesses. Essentially, the AI Service Desk will work as a central information hub, allowing all stakeholders to receive tailor-made answers, providing free access to information, which will be especially useful to smaller AI providers and deployers, fostering innovation horizontally. Its use will not be limited to private market operators, as also public authorities from all member states will be able to get answers and have access to tools to help them in the implementation of the AI Act.[71]

---

[69] *See* Articles 56, 57 and 62 of the AI Act, as well as Recitals 116 and 117. With regard to regulatory sandboxes, *see also* Articles 57, 66 and 76, as well as Recitals 138, 139 and 140.

[70] *See* Article 75 of the AI Act.

[71] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. AI Continent Action Plan, COM (2025) 165 final (Apr. 9, 2025), https://digital-strategy.ec.europa.eu/en/library/ai-continent-action-plan.

Besides the abovementioned two key institutions, the AI Act also introduces certain other supranational entities. Namely, the Scientific Panel[72] and the Advisory Forum.[73] These partially autonomous groups offer technical advice to the AI Board and the European Commission, reinforcing the regulatory and developmental foundations of AI in the EU.

Additionally, the AI Act involves the establishment of certain national bodies. Specifically, Notifying Authorities,[74] Notified Bodies,[75] Market Surveillance Authorities[76] and National Competent Authorities.[77]

Notifying Authorities are designated or established by each Member State, and are responsible for setting up the necessary assessment, monitoring and notification procedures at the Member State level. On the other hand, Notified Bodies are third-party, independent bodies, designated by the member states, that assess the conformity of AI systems with the AI Act's requirements. Finally, Market Surveillance Authorities are essentially single points of contact, responsible for monitoring the AI market to ensure compliance of AI systems with the AI Act's obligations, and taking appropriate measures to counter risks, or outright breaches of the Act. Finally. at the national level, Member States are required to appoint national competent authorities (NCAs) to oversee AI systems, establish regulatory sandboxes for testing innovative AI technologies, and ensure that they operate autonomously and impartially to effectively implement the AI Act.[78]

To further ensure compliance, the AI Governance Framework allows for the imposition of substantial penalties for non-compliance, with fines for providers of high-risk AI systems

---

[72] *See* Articles 68 and 90 of the AI Act, as well as Recital 163.

[73] *See* Article 67 of the AI Act.

[74] *See* Articles 28 and 30 of the AI Act.

[75] *See* Articles 29 to 39 of the AI Act, as well as Recitals 125, 126 and 145.

[76] *See*, among others, Articles 74, 75, 76, 78, 79, 80 and 85 of the AI Act, as well as Recitals 36, 130, 149, 156, 159, 160, 161 and 162.

[77] *See*, among others, Articles 57, 58 and 70 of the AI Act, as well as Recitals 116, 126, 138, 139, 153, 154 and 156.

[78] *See* Articles 57 to 61 of the AI Act.

reaching up to 35 million EUR or 7% of annual turnover, depending on the severity of the infringement.[79] This robust penalty structure underscores the importance of adhering to AI regulatory standards.

Overall, the AI Governance Framework represents a pioneering approach in regulating AI technologies, balancing the need for innovation with the ethical and safety concerns surrounding AI deployment. It sets a global precedent by fostering an environment where AI can be developed responsibly and used safely, while providing clear oversight mechanisms to safeguard fundamental rights and prevent the misuse of AI.

6. BUILDING BRIDGES: AI OFFICE, ECB PARTNERSHIP, AND US REGULATORY COORDINATION

The establishment of the AI Office necessitates a close working relationship with existing financial regulatory bodies, such as the ECB and national competent authorities. This collaboration is essential for achieving a cohesive and comprehensive approach to AI governance within the financial sector.[80]

The ECB, in its capacity as a prudential supervisor, intersects with the AI Office's mandate to oversee high-risk AI systems used in financial services.[81] It is likely that the ECB will need to integrate the requirements of the AI Act into its supervisory activities, especially regarding the supervision of GPAI models. The paths of the ECB and the AI Office are expected to intersect through risk assessment in the banking industry, the creation of standards and codes of practice for the specific use of AI deployment in the sector, international

[79] *See* Articles 99, 100 and 101 of the AI Act.

[80] For further elaboration and an extended discussion of this theme, *see* Maria Lucia Passador, *AI Act and the ECB: Steering Financial Supervision in the EU*, 30 Colum. J. Eur. L. 259 (2025).

[81] For a general perspective on the necessary coordination on AI between European bodies, *see* Claudio Novelli et al., *A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities*, 15 Eur. J. Risk Regul. 1 (2024).

collaboration on financial stability, and the overall oversight of digital and technological innovation, particularly considering the growth of the digital economy. This will involve exchanging information on internal testing, safeguards, and risk mitigation procedures.

Although the AI Office and the ECB will inevitably need to collaborate on overseeing AI applications within the financial sector, potential differences in their regulatory priorities may complicate this process. The AI Office is chiefly concerned with safeguarding fundamental rights, data privacy, transparency, and non-discrimination. Its mandate includes trustworthiness and human-centricity of AI systems, focusing on ethical considerations and the prevention of harm to individuals. Conversely, the ECB's primary mandate looks at maintaining financial stability. While the ECB acknowledges the importance of ethical considerations, and its special status does not exempt it from adhering to fundamental rights, as ruled by the European Court of Justice in *Steinhoff and Others v ECB,*[82] its focus is inherently more aligned with systemic risk management, operational resilience, and the soundness of financial institutions. These differing priorities could generate issues in regulatory coordination, especially in areas characterized by trade-offs between transparency, privacy and resilience of the system.[83] For instance, the AI Office may push for guidelines that enhance transparency requirements in light of data protection needs, whereas the ECB may look at market stability, and therefore prioritize the confidentiality of certain data. This divergence does not necessarily represent an issue, as the focus on different priorities and mandates may help creating balanced, appropriate regulatory measures and nudges. However, in this regard

---

[82] European Court of Justice, Case T-107/17, *Frank Steinhoff and Others v European Central Bank* (May 2019), ECLI:EU:T:2019:353, paragraph 98 (stating that the special status conferred on the ECB by the fundamental Treaties of the European Union does not exempt it from respecting fundamental rights of the EU).

[83] Still, it is worth noting that, from a political science perspective, the transatlantic dialogue on AI governance is not merely technical coordination. It is also a theater of soft power competition, where regulatory philosophies embody broader political values: Europe's precautionary ethos versus America's innovation-first pragmatism.

it will be essential that structured dialogue and clear(er) delineation of roles between the AI Office and the ECB are put in place. Further, in the absence of coordinated oversight, financial institutions could face regulatory fragmentation, where divergent compliance requirements generate legal uncertainty and inefficiencies.

To facilitate effective collaboration, robust mechanisms for the exchange of information between the AI Office, the ECB, and national competent authorities will be essential. This includes the sharing of insights related to AI risks, opportunities, challenges, and best practices.

Further, the AI Office may offer advisory support to the ECB on AI governance matters, including the development of standards and codes of practice for AI deployment in banking.

Both the AI Office and the ECB are expected to engage in international collaborations with organisations such as the GPAI and the Organisation for Economic Co-operation and Development (OECD). By harmonising their international efforts, these bodies will help ensure a unified stance on global AI governance from the EU. In addition, both the AI Office and the ECB may engage in joint initiatives, such as the establishment of regulatory sandboxes for testing innovative AI systems in a controlled environment. Such initiatives allow both institutions to combine their expertise in promoting innovation while ensuring regulatory compliance.

In the U.S., the National Institute of Standards and Technology ("NIST"), a federal agency under the Department of Commerce, plays a central role in establishing frameworks for risk management in connection with emerging technologies and, specifically, AI. The NIST does not possess direct regulatory authority, but its frameworks are recognized by financial institutions and *de facto* largely respected, constituting soft law. The NIST AI Risk Management Framework, specifically, is designed to be compatible with existing financial regulations, expressly ensuring that its adoption does not conflict with banks' obligations under sector-

specific regulations.[84] This is evidently the result of a collaborative approach between technical entities and other stakeholders, such as financial regulators, which fosters non-conflicting strategies, and ultimately produces clearer outputs and more predictable results. This collaborative model has influenced discussions between US and EU regulators, with both jurisdictions exploring how to harmonize their approaches while respecting their distinct regulatory philosophies. The comparison with NIST is instructive: what the U.S. currently treats as voluntary frameworks, Europe is hard-coding into binding obligations. That contrast is a reminder that 'soft law' at home can quickly transform into 'hard law' abroad—and that US institutions straddling both worlds must learn to speak both dialects fluently.

In the European Union, the AI Act introduces the AI Office and the AI Board, each playing a crucial role in fostering ethical and effective AI governance. Their interaction with existing financial regulatory institutions, particularly the ECB, will be vital to balancing the objectives of maintaining financial stability with promoting innovation in AI technologies across the EU.

7. CONCLUDING REMARKS

This discussion has delved deeply into the multifaceted implications of the AI Act, offering a comprehensive examination of its transformative potential within the realm of financial regulation. Central to this analysis are (i) its risk-based framework, which classifies AI systems by their potential impact on safety, rights, and systemic stability, establishing a

[84] The AI Risk Management Framework was created in collaboration with both the private and the public sector, allowing for several drafts for public comments, and it is expressly intended to build on AI risk management efforts by others: *see* NIST, *Artificial Intelligence Risk Management Framework (AI RMF) 1.0*, https://www.nist.gov/itl/ai-risk-management-framework (last visited Apr. 19, 2025). *See also* Bank Policy Inst., *Request for Information on the Artificial Intelligence Risk Management Framework (Docket No. [210726–0151])* (Sept. 2, 2021), https://www.nist.gov/system/files/documents/2021/09/17/ai-rmf-rfi-0103.pdf, requesting to ensure that the AI Risk Management Framework is consistent with existing regulatory requirements.

meticulous balance between fostering innovation and enforcing rigorous oversight; and (ii) the critical interplay between the AI Act's governance mechanisms—embodied by the AI Office and AI Board—and the ECB prudential supervisory mandate, revealing opportunities for synergistic collaboration that harmonises technological progress with the ethical imperatives of financial stability.

Furthermore, it illuminated the dual challenges and opportunities that the AI Act presents. On the one hand, it demands significant compliance efforts, particularly for institutions deploying high-risk AI systems, potentially engendering market consolidation and systemic risk mitigation. On the other, it positions the EU as a global standard-setter, with the Act's extraterritorial provisions setting a benchmark for ethical and transparent AI governance that could inspire regulatory emulation across jurisdictions. This duality underlines the AI Act's role not only as a regulatory instrument but as a catalyst for dialogue on the evolving responsibilities of financial institutions and regulators alike.

Key takeaways for stakeholders include the imperative for financial entities to embrace a proactive approach to compliance, leveraging the AI Act's frameworks not merely as regulatory constraints but as enablers of responsible innovation. For policymakers, the AI Act represents a blueprint for regulatory harmonisation, underscoring the importance of international cooperation in governing AI's integration into global financial systems.

Hence, this study has provided a layered perspective on the AI Act's role within financial regulation, framing it not merely as a response to technological disruption but as a forward-looking initiative to redefine the nexus of innovation, governance, and systemic resilience. As the global financial landscape continues to evolve, the insights and frameworks articulated here will hopefully serve as a cornerstone for both scholarly discourse and practical adaptation. Looking forward, compelling avenues for further inquiry might include the long-term impact of the AI Act's extraterritorial reach on global financial markets merits close scrutiny, as does

the efficacy of regulatory sandboxes in fostering safe innovation. The transatlantic implications of these developments, and particularly the adaptation strategies of US financial institutions operating in Europe, warrant continued examination as a case study in cross-border regulatory compliance. In the end, US readers should treat the AI Act not as an (or the most recent) exotic European regulation but as a mirror held up to the future of US finance. Just as the GDPR became the global shorthand for data privacy, the AI Act may well become the lingua franca of responsible AI in finance. The lesson is clear: prepare now, or risk being regulated later on someone else's terms. Equally significant is the need to explore the operational dynamics of collaboration between the AI Office and the ECB, particularly in addressing the opacity and accountability challenges inherent in complex AI systems.

On the one hand, for US executives, the message is quite simple: treat the AI Act as a strategic compliance horizon, not a foreign curiosity. Just as Sarbanes-Oxley or Dodd-Frank forced firms to overhaul governance structures, the AI Act will do the same for AI systems. The choice is whether to prepare early, turning compliance into competitive advantage, or to wait until regulators and markets leave you no choice.

On the other hand, for political scientists, another layer of inquiry concerns legitimacy. Can a technocratic framework such as the AI Act command democratic trust? Its success will depend not only on enforcement but on whether citizens perceive algorithmic oversight as aligned with their rights and values. In this sense, the AI Act is also an experiment in building legitimacy for supranational governance in a domain—AI—that touches everyday life in deeply political ways.