BG Pulse Journal USA
ISSN:1947-2536 http://www.bgpulseusa.com/index.php/bg

ARTIFICIAL INTELLIGENCE GOVERNANCE IN FINANCIAL SERVICES: INTERNATIONAL REGULATORY APPROACHES AND FUTURE CHALLENGES

Abduraxmonov Biloliddin Ulug'bek o'g'li

University of Digital Economics and Agrotechnologies Digital Economics

Finance and financial technologies

E-mail: biloliddinabdurahmonov8@gmail.com

Doi: https://doi.org/10.5281/zenodo.22014846

Abstract. Artificial intelligence (AI) is moving from peripheral analytics into core financial functions, including credit assessment, fraud detection, insurance pricing, customer service, trading, compliance, and operational risk management. This transition creates a governance problem because AI combines conventional model risk with new concerns involving data provenance, opacity, autonomy, third-party concentration, cyber threats, and potentially system-wide feedback effects. This article compares major regulatory approaches to AI governance in financial services and evaluates their implications for future supervision. Using qualitative comparative document analysis, the study examines ten official legal, regulatory, and supervisory sources from the European Union, the United Kingdom, the United States, and international standard-setting bodies. The results identify three regulatory models: a horizontal risk-based statutory model in the European Union; an outcomes-focused, sector-led model in the United Kingdom; and a distributed, technology-neutral model in the United States supported by existing financial laws and risk-management frameworks. Despite institutional differences, the approaches converge around accountability, data governance, validation, human oversight, transparency, operational resilience, and continuous monitoring. The article argues that future policy should combine technology-neutral financial regulation with AI-specific controls for high-impact use cases, while strengthening third-party oversight, cross-border interoperability, and supervisory capacity for generative and agentic AI.

Keywords: artificial intelligence; financial regulation; model risk; algorithmic governance; generative AI; fintech; consumer protection; operational resilience

1. Introduction

Artificial intelligence has become an increasingly important component of financial intermediation. Banks, insurers, investment firms, payment providers, and fintech companies use machine learning and related techniques to identify fraud, classify customers, automate compliance, assess creditworthiness, personalize products, support trading, and improve internal operations. The acceleration of generative AI has expanded the range of possible applications because large language and multimodal models can process unstructured information and perform tasks that previously required substantial human input. Evidence from the United Kingdom illustrates the speed of this transition: in the 2024 joint Bank of England and Financial Conduct Authority (FCA) survey, 75% of responding firms reported that they were already using AI and another 10% planned to use it within three years. The same survey found that one third of AI use cases involved third-

party implementations, highlighting that AI governance is also becoming a supply-chain governance problem (Bank of England & Financial Conduct Authority, 2024).

The regulatory significance of AI is particularly high in finance because errors can affect both individual rights and the stability of institutions. A poorly designed credit model can discriminate, misprice risk, or deny access to essential financial services. A generative system can produce inaccurate compliance advice, disclose confidential information, or be manipulated by malicious inputs. Algorithmic trading and risk-management systems may create correlated behavior across institutions. Dependence on a small number of cloud, data, and foundation-model providers can concentrate operational risk. These concerns are layered on top of familiar requirements concerning prudential safety, market integrity, consumer protection, data privacy, outsourcing, cybersecurity, and senior-management accountability. The central policy question is therefore not whether AI should be regulated in finance, but how new AI-specific risks should be integrated into an already dense regulatory environment.

International practice reveals no single governance model. The European Union (EU) has adopted a horizontal AI statute that classifies systems by risk and imposes specific obligations on high-risk applications. The United Kingdom has largely retained a principles-based, outcomes-focused strategy that relies on existing sector regulators and existing financial rules. The United States also continues to apply technology-neutral financial laws and supervisory expectations, while adding AI-specific guidance and voluntary risk-management resources. International bodies, including the Basel Committee and the Financial Stability Institute, increasingly emphasize that traditional controls over data, models, outsourcing, operational resilience, and governance remain relevant but must be adapted to the scale, complexity, and autonomy of modern AI (Basel Committee on Banking Supervision, 2024; Crisanto et al., 2026).

This article addresses two research questions. First, what are the principal similarities and differences among current international approaches to AI governance in financial services? Second, which emerging risks are most likely to challenge existing regulatory models over the next several years? The article contributes a structured comparison based on legal form, scope, risk classification, consumer protection, model and data governance, third-party oversight, and supervisory mechanisms. It argues that regulatory convergence is occurring at the level of governance outcomes even when jurisdictions choose different legal architectures.

2. Materials and Methods

The study uses qualitative comparative document analysis. The material consists of ten official or institutionally authoritative sources published between 2011 and 2026: two EU regulations, two UK regulatory publications, three U.S. regulatory or risk-management documents, and three international prudential or supervisory sources. Documents were selected because they either establish binding legal obligations, express current supervisory expectations, or provide widely used governance frameworks directly relevant to AI in financial services. The analysis reflects the regulatory position available as of 19 August 2026.

Each source was coded across seven dimensions: (1) legal character and institutional architecture; (2) scope of regulated AI activities; (3) risk classification or proportionality; (4) accountability and human oversight; (5) model, data, and explainability requirements; (6) operational, cyber, and third-party risk; and (7) supervisory and enforcement mechanisms. The

coded results were then compared to identify patterns of convergence and divergence. Because the study is doctrinal and comparative rather than statistical, the results describe regulatory structures and governance implications rather than causal effects. The method is appropriate for an emerging field in which formal rules, supervisory guidance, and risk-management standards evolve at different speeds across jurisdictions.

3. Results

3.1. European Union: risk-based statutory governance

The EU represents the most formalized of the three major approaches. Regulation (EU) 2024/1689, the Artificial Intelligence Act, establishes horizontal rules for AI across sectors while preserving the operation of existing financial-services legislation. Its central mechanism is risk classification. In financial services, AI systems used to evaluate the creditworthiness of natural persons or establish credit scores are classified as high-risk, except for systems used for financial-fraud detection. AI used for risk assessment and pricing in relation to natural persons in life and health insurance is also treated as high-risk (European Parliament & Council of the European Union, 2024). This classification directly links AI governance to decisions that can materially affect access to finance and essential protection.

For high-risk systems, the regulatory model requires lifecycle controls rather than a single technical test. Core obligations include risk management, appropriate data governance, technical documentation, record-keeping, transparency to deployers, human oversight, and adequate levels of accuracy, robustness, and cybersecurity. This approach places responsibility on providers and deployers and is designed to make compliance auditable. The financial sector must therefore integrate AI Act obligations with pre-existing requirements under banking, insurance, consumer, data-protection, and operational-resilience law. In practice, this creates a layered compliance model: the AI Act regulates the characteristics and governance of the AI system, while sectoral rules continue to regulate the financial activity and the institution using it.

The EU framework is also being adjusted as implementation experience develops. Regulation (EU) 2026/1744, the Digital Omnibus on AI, simplified parts of the framework and extended the application timetable for high-risk systems. In particular, requirements for high-risk systems listed in Annex III are now scheduled to apply from 2 December 2027, while high-risk AI embedded in certain regulated products under Annex I is subject to a later timetable (European Parliament & Council of the European Union, 2026). The 2026 amendment shows that even a comprehensive statutory model requires adaptive implementation to balance legal certainty, proportionality, and innovation.

3.2. United Kingdom: outcomes-focused sector regulation

The United Kingdom follows a different architecture. The FCA states that its approach to AI is principles-based and focused on outcomes and that it does not currently plan to introduce additional AI-specific financial regulations. Instead, firms are expected to comply with existing frameworks, including the Consumer Duty, senior-management accountability, governance rules, operational resilience expectations, and applicable data-protection requirements (Financial Conduct Authority, 2026). This model seeks to avoid technology-specific rules becoming obsolete while allowing supervisors to intervene where AI creates harmful outcomes.

The UK approach is supported by active monitoring. The 2024 Bank of England-FCA survey indicates both broad adoption and increasing reliance on third parties. It also found growing use of foundation models, which represented 17% of reported AI use cases, and identified data privacy, data quality, data security, and bias or representativeness among leading risk concerns (Bank of England & Financial Conduct Authority, 2024). The regulatory implication is that existing rules may remain formally technology-neutral, but supervisory practices need to become increasingly AI-aware. The UK's model therefore depends heavily on regulator expertise, thematic reviews, testing environments, and the ability to translate general principles into concrete expectations for specific use cases.

3.3. United States: distributed legal duties and risk-management frameworks

The United States continues to govern AI in financial services through a distributed combination of existing statutes, agency enforcement, prudential guidance, and voluntary risk-management frameworks. This structure is technology-neutral: the use of AI does not displace legal duties concerning fair lending, consumer disclosures, safety and soundness, fiduciary obligations, cybersecurity, or model governance. A clear example is the Consumer Financial Protection Bureau's Circular 2023-03, which states that creditors using AI or complex credit models must still provide specific and accurate principal reasons for adverse credit actions; generic explanations are not sufficient merely because the underlying model is complex (Consumer Financial Protection Bureau, 2023). This converts explainability from an abstract ethical preference into a concrete compliance obligation in credit decisions.

Prudential model-risk governance provides a second foundation. The Federal Reserve and the Office of the Comptroller of the Currency's supervisory guidance on model risk management emphasizes robust development, independent validation, ongoing monitoring, governance, and controls over vendor models (Board of Governors of the Federal Reserve System & Office of the Comptroller of the Currency, 2011). Although issued before the current generation of AI, its lifecycle logic remains highly relevant. NIST's AI Risk Management Framework adds a broader governance structure organized around the functions Govern, Map, Measure, and Manage, with attention to validity, reliability, safety, resilience, accountability, transparency, explainability, privacy, and fairness (National Institute of Standards and Technology, 2023). In February 2026, the U.S. Department of the Treasury released a Financial Services AI Risk Management Framework that adapts the NIST approach to financial-sector operational, regulatory, and consumer-protection considerations, reinforcing a preference for scalable, implementation-oriented risk governance rather than a single comprehensive financial AI statute (U.S. Department of the Treasury, 2026).

Table 1. Comparative regulatory architecture for AI in financial services

Jurisdiction	Regulatory architecture	Practical implications for financial institutions
European Union	Horizontal, risk-based statutory model under the AI Act, layered with financial-sector law.	High-impact financial use cases can be classified as high-risk; firms need documented lifecycle controls, human oversight, data governance, robustness, and auditable compliance.

United Kingdom	Principles-based, outcomes-focused sector regulation using existing FCA/PRA and data-protection frameworks.	Boards and senior managers remain accountable for customer and prudential outcomes; supervisory monitoring and testing translate broad rules into AI-specific practice.
United States	Distributed, technology-neutral system of financial laws, agency enforcement, prudential guidance, and voluntary AI risk frameworks.	Existing duties on fair lending, explanations, model validation, governance, cybersecurity, and third parties continue to apply regardless of AI complexity.

Across the three models, the legal form differs more than the governance objectives. The common elements are institutional accountability, proportionality based on use-case risk, reliable data, documented development and testing, independent challenge or validation, human oversight for consequential decisions, traceability, cybersecurity, third-party governance, and ongoing performance monitoring. International prudential work reinforces this convergence. The Basel Committee emphasizes responsible innovation, effective risk management of service providers, sufficient supervisory capabilities, and the continuing importance of human judgment (Basel Committee on Banking Supervision, 2024). The Financial Stability Institute similarly finds emerging convergence around data privacy, data quality, data security, and data governance, while warning that generative AI and third-party dependencies can exceed the assumptions of older frameworks (Crisanto et al., 2026).

4. Discussion

The comparative results suggest that a durable regulatory strategy should distinguish between legal architecture and governance substance. The EU chooses an AI-specific statute, while the UK and United States rely more heavily on existing sectoral rules. Yet all three approaches increasingly require firms to know where AI is used, assign accountable owners, assess materiality, control data, test models, monitor performance, manage vendors, and provide effective human challenge. This convergence is significant because it creates a possible basis for international interoperability even where legal texts remain different. A global financial institution does not necessarily need identical laws in every jurisdiction if it can maintain a common internal control system that satisfies the shared governance outcomes and then map local legal requirements onto that system.

The first major future challenge is the transition from relatively stable predictive models to generative and agentic systems. Traditional model-risk management assumes a definable model, identifiable inputs and outputs, periodic validation, and controlled changes. Foundation models can be updated by external providers, combined with retrieval systems, connected to tools, and altered through prompts or fine-tuning. Agentic AI may plan and execute sequences of actions with limited human intervention. These characteristics make static approval processes less effective. Governance will need to move toward continuous evaluation, behavioral testing, usage constraints, real-time monitoring, and explicit escalation rules. Institutions should assess not only the base model but also the full system architecture, including prompts, retrieval data, tools, permissions, and downstream decisions.

Second, explainability will remain a difficult regulatory boundary. In high-stakes financial decisions, firms must be able to justify outcomes to customers, auditors, courts, and supervisors. The CFPB's adverse-action guidance demonstrates that model complexity does not excuse a failure to provide specific reasons for a credit decision (Consumer Financial Protection Bureau, 2023). However, some advanced AI systems do not naturally produce faithful causal explanations. This creates a design requirement: institutions may need to restrict certain use cases, employ interpretable surrogate methods, maintain reason-code architectures, or preserve human review where legal rights depend on understandable decisions. Explainability should therefore be treated as a use-case-specific control objective, not as a generic requirement that every internal parameter of a model be understandable.

Third, data governance is becoming more difficult as models use larger, more heterogeneous, and more externally sourced data sets. Generative AI can mix public, licensed, proprietary, personal, synthetic, and user-provided data. Financial institutions need reliable information about data lineage, lawful use, quality, representativeness, retention, and access controls. Crisanto et al. (2026) note that existing data-protection frameworks provide an important foundation but can be difficult to apply across the AI lifecycle, especially where third-party providers limit visibility. This challenge connects privacy, fairness, intellectual-property risk, cybersecurity, and model performance. Weak data governance can therefore create multiple regulatory failures simultaneously.

Fourth, third-party and concentration risk may become a central prudential issue. The 2024 UK survey already showed that a substantial share of AI use cases depend on third-party implementations (Bank of England & Financial Conduct Authority, 2024). Advanced AI may deepen dependence on a small group of cloud platforms, chip suppliers, data providers, and foundation-model developers. A single provider outage, security compromise, model defect, or policy change could affect many institutions at once. Existing outsourcing frameworks are useful but may not provide sufficient transparency into training data, model updates, testing methods, or subcontracting chains. Supervisors may therefore need stronger expectations for exit planning, substitutability, concentration mapping, incident reporting, contractual audit rights, and resilience testing of critical AI services.

Fifth, the systemic dimension of AI may become more important than the current institution-by-institution focus. If many firms use similar models, data sources, or optimization objectives, AI can increase correlated behavior. In trading and liquidity management, rapid model reactions could amplify volatility. In credit, common data and models could produce synchronized tightening. In cybersecurity, AI can increase the speed of both attacks and defensive responses. These channels suggest that microprudential controls should be complemented by macroprudential monitoring of common providers, correlated models, automated decision speeds, and cross-market dependencies. The Basel Committee's emphasis on responsible innovation and human judgment is relevant because a financial system optimized for speed and uniformity may also become more fragile when models fail in similar ways (Basel Committee on Banking Supervision, 2024).

Sixth, regulatory fragmentation can itself become a risk. Firms operating across borders may face different definitions of AI, different classifications of high-risk use cases, different documentation requirements, and different expectations for automated decisions. The EU's statutory obligations, the UK's outcomes-based approach, and the U.S. combination of agency law

and voluntary frameworks are not inherently incompatible, but compliance costs can rise if similar controls must be demonstrated in different formats. International coordination should therefore focus on interoperable evidence: common concepts for AI inventories, risk tiers, testing records, incident reporting, data lineage, model-change documentation, and third-party assurance. Complete legal harmonization is unlikely, but comparable supervisory evidence is achievable.

Finally, supervisory capacity is a limiting factor. Effective oversight requires regulators to understand model architecture, data pipelines, vendor arrangements, cybersecurity, statistical validation, and the legal consequences of automated decisions. The same scarcity of AI expertise that affects smaller financial institutions also affects public authorities. A proportionate future framework should therefore combine enforceable accountability with regulatory sandboxes, shared testing resources, specialist supervisory teams, cross-agency cooperation, and international exchange of technical evidence. The goal should not be to eliminate AI risk, which is impossible, but to ensure that material risks are identified early, assigned to accountable decision-makers, monitored continuously, and contained before they create consumer harm or threaten financial stability.

5. Conclusion

AI governance in financial services is converging toward a common set of control objectives even as jurisdictions retain different regulatory architectures. The EU has chosen a detailed risk-based statutory framework; the UK relies on principles-based sector regulation and existing outcome duties; and the United States combines existing financial law, model-risk supervision, enforcement, and sector-specific risk-management tools. Across these systems, responsible AI increasingly means clear accountability, reliable data, risk-based validation, human oversight, transparency where decisions affect rights, operational resilience, third-party governance, and continuous monitoring.

The next phase of regulation will be shaped less by conventional predictive models and more by generative, foundation, and agentic systems that are dynamic, externally supplied, and capable of greater autonomy. These technologies challenge static validation, traditional outsourcing controls, and institution-specific supervision. The most effective future framework is therefore likely to be hybrid: technology-neutral financial regulation should remain the foundation, while AI-specific requirements should apply to high-impact uses and to risks that existing frameworks do not adequately capture. International cooperation should prioritize interoperable governance evidence and oversight of common third-party dependencies. Such an approach can preserve innovation while maintaining the trust, fairness, resilience, and accountability on which financial systems depend.

References:

1. Bank of England, & Financial Conduct Authority. (2024, November 21). Artificial intelligence in UK financial services - 2024. https://www.bankofengland.co.uk/report/2024/artificial-intelligence-in-uk-financial-services-2024
2. Basel Committee on Banking Supervision. (2024). Digitalisation of finance. Bank for International Settlements. https://www.bis.org/bcbs/publ/d575.htm

3. Board of Governors of the Federal Reserve System, & Office of the Comptroller of the Currency. (2011). Supervisory guidance on model risk management (SR 11-7/OCC 2011-12). https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm
4. Consumer Financial Protection Bureau. (2023, September 19). CFPB Circular 2023-03: Adverse action notification requirements and the proper use of the CFPB's sample forms provided in Regulation B. https://files.consumerfinance.gov/f/documents/cfpb_adverse_action_notice_circular_2023-09.pdf
5. Crisanto, J. C., Currat, A., Ehrentraud, J., & Wu, W. (2026). In data we trust? Emerging policy and supervisory approaches to AI data use in financial services (FSI Insights No. 73). Bank for International Settlements. https://www.bis.org/fsi/publ/insights73.htm
6. European Parliament, & Council of the European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/1689/oj
7. European Parliament, & Council of the European Union. (2026). Regulation (EU) 2026/1744 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2026/1744/oj
8. Financial Conduct Authority. (2026, February 13). AI and the FCA: Our approach. https://www.fca.org.uk/firms/innovation/ai-approach
9. National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0) (NIST AI 100-1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1
10. U.S. Department of the Treasury. (2026, February 19). Treasury releases two new resources to guide AI use in the financial sector. https://home.treasury.gov/news/press-releases/sb0401