World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

RegTech Readiness for Financial Institutions in the AI Governance era: Emerging technology risk, internal control, and inclusive compliance modernization

Abdullahi Ibiyeye *, Tawakalit O. Ibiyeye and Femi Oke

Western Illinois University.

World Journal of Advanced Research and Reviews, 2025, 27(02), 2249-2264

Publication history: Received on 12 July 2025; revised on 24 August 2025; accepted on 29 August 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.27.2.3522

Abstract

Financial institutions increasingly rely on regulatory technology (RegTech), artificial intelligence (AI), machine learning, digital identity systems, workflow automation, and continuous auditing to satisfy anti-money laundering obligations, customer due diligence requirements, cybersecurity expectations, consumer protection duties, market conduct rules, and internal control documentation standards. These tools can improve the speed and consistency of compliance work, but their value depends on institutional readiness rather than technological capability alone. This conceptual review updates an earlier 2024 readiness analysis by incorporating recent scholarly and regulatory sources. It also situates the discussion within the authorial research trajectory on regulatory compliance, trade policy, technology-enabled supply chains, and AI-related legal, privacy, and cybersecurity risks. The review finds that RegTech can strengthen monitoring, regulatory reporting, audit documentation, fraud detection, and financial inclusion when it is implemented with reliable data, clear control ownership, explainable decision logic, vendor accountability, cybersecurity safeguards, and human oversight. However, the same technologies can amplify weak controls, obscure accountability, increase third-party dependence, and raise fixed costs for smaller institutions. The burden is particularly acute for community banks, credit unions, minority depository institutions, small investment firms, and banks serving underserved areas, which often face complex compliance expectations with limited staffing and technical capacity. The paper proposes an updated RegTech Readiness Pathway organized around nine dimensions: regulatory-to-control mapping, data governance, control ownership, automation fit, explainability and model governance, cybersecurity and privacy-by-design, third-party oversight, continuous audit evidence, and inclusion-oriented proportionality. The article contributes to compliance and governance scholarship by treating RegTech adoption as an internal-control transformation rather than a software procurement exercise.

Keywords: Regtech; Regulatory Compliance; Artificial Intelligence; Internal Control; Financial Institutions; Community Banks; Underserved Markets; Financial Inclusion; Audit Evidence

1. Introduction

Regulatory compliance in finance is no longer a narrow legal-support function. It is a core institutional infrastructure that enables banks, investment firms, credit unions, fintech platforms, broker-dealers, payment providers, and other intermediaries to onboard customers, extend credit, protect consumers, monitor transactions, report to regulators, and maintain public trust. When that infrastructure fails, the consequences are not limited to missed filings or technical documentation gaps. Weak compliance can permit illicit finance, conceal cybersecurity exposure, produce unfair or opaque customer outcomes, impair audit readiness, delay remediation, and weaken confidence in the institution itself.

The compliance environment has also changed in character. Financial institutions now operate in markets shaped by digital onboarding, real-time payments, cloud platforms, data analytics, AI-assisted monitoring, generative AI,

* Corresponding author: Abdullahi Ibiyeye

blockchain-enabled products, and increasingly automated supervisory expectations. Compliance staff must therefore interpret technology outputs rather than merely collect static documents. A sanctions alert, a suspicious-activity score, a cybersecurity anomaly, a model-generated credit recommendation, or an automated onboarding rejection does not speak for itself. It has to be evaluated within a control environment that shows who owns the decision, what data were used, whether the result can be explained, and how exceptions are escalated.

This paper extends a developing research trajectory. Ibiyeye et al. (2024) examined regulatory compliance in the finance and investment sector and identified the dual nature of emerging technologies: they can improve compliance efficiency while also creating new operational, privacy, and regulatory risks.

The present article builds on those works by asking a more specific readiness question: what must financial institutions have in place before they rely on RegTech and AI-enabled tools for compliance modernization?

The question is timely. Since 2024, regulators and standard setters have become more explicit about AI-related financial-sector risks. The U.S. Department of the Treasury (2024b) reported that AI can create opportunities in financial services while amplifying risks related to privacy, bias, third-party dependence, data integrity, and cybersecurity. The U.S. Government Accountability Office (GAO, 2025) similarly reviewed both the benefits and risks of AI use in financial services and examined how federal financial regulators oversee AI deployment. At the international level, the Financial Stability Board (FSB, 2024) warned that AI may influence financial stability through model risk, operational risk, third-party concentration, herding behavior, and interconnectedness. These developments make readiness more than an academic concern; they make it a practical governance requirement.

The burden is not distributed evenly. Large institutions may be able to hire model validators, compliance engineers, cybersecurity specialists, legal technologists, and data governance teams. Community banks, minority depository institutions, credit unions, smaller investment firms, and banks serving rural or underserved markets often cannot. Yet these institutions remain expected to manage AML, privacy, consumer protection, cybersecurity, fair access, internal control, and reporting obligations. The literature also complicates the assumption that RegTech necessarily reduces cost. Charoenwong et al. (2024) found that technology-driven compliance can raise information technology spending and reduce profitability, with especially important effects for smaller firms. A readiness framework therefore has to be both technologically serious and proportionate to institutional capacity.

This paper argues that compliance modernization should be treated as a governance transformation rather than a technology acquisition project. RegTech and AI can strengthen monitoring, reporting, audit trails, and inclusion, but they can also accelerate weak controls where data are unreliable, ownership is unclear, models are opaque, vendors are insufficiently supervised, and staff are not trained. The article proposes an updated RegTech Readiness Pathway to guide institutions before procurement, during pilot testing, and after deployment.

2. Methodological Orientation and Scope

This article uses a conceptual review method. A conceptual review is appropriate because the relevant literature spans financial regulation, accounting, internal audit, information systems, cybersecurity, explainable AI, financial inclusion, and policy governance. The objective is not to estimate a pooled effect size or to claim that any single technology improves compliance outcomes in all contexts. Instead, the objective is to synthesize recent literature and regulatory guidance into a practical readiness model that financial institutions can use before deploying RegTech or AI-enabled compliance tools.

The review incorporates peer-reviewed scholarly literature and selected authoritative policy sources relevant to contemporary financial-sector compliance modernization. Peer-reviewed sources were prioritized where they addressed RegTech, SupTech, AI and machine learning in finance, explainable AI, internal audit technology, AML and emerging technologies, fintech and financial inclusion, or compliance cost effects. Authoritative policy sources were included where they materially shaped the post-2024 governance environment, including reports from the U.S. Treasury, GAO, NIST, FSOC, FSB, the World Economic Forum, and the International Monetary Fund.

The review is intentionally interdisciplinary. RegTech readiness cannot be understood through technology literature alone because compliance failures often arise from legal interpretation, organizational ownership, audit evidence, privacy safeguards, cybersecurity controls, model governance, vendor dependence, and customer access. Nor can readiness be understood through financial law alone because the operational form of compliance is increasingly shaped by data pipelines, workflow systems, automated alerts, machine-learning tools, and dashboard reporting. The synthesis therefore evaluates both what technologies can do and what institutional conditions make their use defensible.

Recent developments in AI governance also matter. Earlier scholarship had already identified the rise of RegTech, AI-assisted monitoring, explainability gaps, cybersecurity exposure, and inclusion risks. Subsequent policy and technical literature made these concerns more concrete. NIST (2024) released its Generative AI Profile under the AI Risk Management Framework. Treasury issued reports on AI-specific cybersecurity risks and the broader uses, opportunities, and risks of AI in financial services (U.S. Department of the Treasury, 2024a, 2024b). GAO (2025) examined AI use and oversight in financial services. The IMF published guidance on generative AI for compliance risk analysis in tax and customs administration, which is relevant by analogy to risk-based compliance functions in finance (Aslett et al., 2025). The updated scope therefore captures a more mature regulatory and governance environment than the earlier April 2024 draft.

3. Prior Scholarship and the Progression Toward RegTech Readiness

The authorial progression is important because this paper is designed as a bridge between diagnostic compliance scholarship and later framework development. The 2024 IOSR article by Ibiyeye et al. examined current compliance practices, challenges, and the effect of emerging technologies in the finance and investment sector. Its main contribution was diagnostic: it identified regulatory complexity, technology-driven compliance pressures, data privacy concerns, and the need to balance innovation with legal accountability (Ibiyeye et al., 2024). The present paper retains that diagnostic foundation, extends the analysis, and translates the problem into a readiness pathway.

The author's 2024 policy and trade research also informs the institutional logic of this paper. Ibiyeye and Ibiyeye (2024) used multivariate regression to examine how U.S. trade policies and regulations affect business growth, emphasizing that regulatory choices can influence market outcomes rather than simply impose administrative obligations. Ibiyeye and Olayinka (2024) likewise argued that policy-driven and technology-enhanced supply chains can advance resilience, sustainability, and inclusive prosperity. Those works are not RegTech papers, but they support the broader proposition that law, policy, and technology should be analyzed as interacting systems. In financial compliance, the same point applies: regulatory obligations, digital tools, operational processes, and institutional capacity must be designed together.

The 2025 PriCyai Magazine essay adds a practitioner-facing AI governance dimension. Ibiyeye (2025) described the digital dilemma facing financial institutions that seek to harness AI while navigating legal, privacy, and cybersecurity pitfalls. This article develops that concern into a more formal scholarly readiness model. The result is a coherent progression: first, identify the compliance and emerging-technology problem; second, examine how regulation and technology shape business and institutional systems; third, translate AI risks into governance questions; and fourth, specify the readiness conditions required for responsible RegTech adoption.

A related 2024–2025 technical publication stream further sharpens the implementation logic behind this readiness model. Dopamu et al. (2024a) examined AI-assisted regulatory compliance for cybersecurity in U.S. financial institutions, while Dopamu, Okonkwo, Adeniji, and Oke (2024b) analyzed secure messaging controls grounded in cryptographic protections for confidentiality, integrity, authenticity, and nonrepudiation. Subsequent 2025 work moved toward implementation architecture: Oke et al. (2025c) proposed a real-time AI-driven communication layer for fraud detection in financial services; Adeniji et al. (2025) addressed cloud and Internet of Things cybersecurity threat surfaces; and Oke et al. (2025a, 2025b, 2025d) examined blockchain consent management, AI-ready infrastructure, and secure interoperable data systems in adjacent regulated settings. Those works are used here selectively because they speak to security, auditability, infrastructure readiness, privacy-by-design, and evidence capture.

4. Compliance as Institutional Infrastructure

4.1. Risk-Based Compliance and the Evidence Problem

Risk-based compliance begins with the idea that institutions should allocate resources according to the nature and severity of their risks. In practice, that requires obligation mapping, risk assessment, control design, monitoring, escalation, remediation, and evidence retention. A community bank focused on relationship lending will not have the same risk profile as a cross-border payment platform or a broker-dealer using algorithmic surveillance. Still, the basic compliance architecture is common: identify the obligation, connect it to an operational control, assign ownership, monitor results, remediate exceptions, and document what occurred.

Evidence is the weak point in many compliance programs. Policies and procedures are necessary but do not prove that controls operated effectively. Regulators, auditors, boards, and risk committees may need to know when a customer file

was reviewed, what data were used, why an alert was closed, whether the reviewer overrode an automated recommendation, who approved the override, and whether the root cause was remediated. This evidentiary chain is the practical link between legal obligation and institutional accountability.

RegTech can strengthen that link when it connects obligations to operational evidence. Freij (2020) described RegTech as a response to the increasing resource demands of financial regulatory compliance. McCarthy (2023) emphasized that RegTech and SupTech require consistency between regulatory principles and implementation practices. These findings suggest that RegTech should not be evaluated only by speed or cost reduction. Its deeper value lies in whether it makes compliance evidence more reliable, traceable, explainable, and useful for oversight.

4.2. Internal Audit, Continuous Assurance, and AI-Supported Review

Internal audit is central to compliance readiness because it evaluates whether controls work as designed and whether management's evidence is reliable. In technology-enabled compliance, auditability should be designed before deployment rather than reconstructed after a regulatory review or incident. A compliance tool that generates alerts but does not preserve source data, reviewer notes, approval history, or remediation logs may create visibility without assurance.

Continuous auditing research reinforces this point. Polizzi and Scannella (2023) argued that continuous auditing can support ongoing monitoring of internal controls and risk levels, but implementation requires organizational readiness and technical capacity. Wassie and Lakatos (2024) similarly concluded that AI may improve internal audit effectiveness by reducing routine work and supporting analysis, while still requiring data access, skills, governance, and institutional commitment. AI can help auditors see patterns earlier, but it does not remove the need for judgment, documentation, and control testing.

For smaller institutions, this insight is encouraging because continuous assurance does not require immediate adoption of complex AI systems. A community bank might start with automated exception registers, overdue customer-review reports, vendor due diligence checklists, or audit-ready evidence repositories. A small investment adviser might automate disclosure review evidence before deploying predictive compliance analytics. The readiness question is not whether the tool is advanced; it is whether the tool produces evidence that can be reviewed, challenged, and improved.

Table 1 Core Compliance Functions, RegTech Opportunities, and Readiness Risks

Compliance function	RegTech opportunity	Readiness risk
Regulatory mapping	Links obligations to products, processes, jurisdictions, and customer segments.	Automation may digitize ambiguity if legal interpretation and control ownership are unresolved.
Customer due diligence and AML monitoring	Supports onboarding checks, risk scoring, sanctions screening, suspicious activity review, and remediation.	False positives, false negatives, outdated records, and rigid documentation rules can impair both compliance and access.
Cybersecurity and privacy controls	Protects data, digital channels, cloud systems, vendor connections, and incident response processes.	AI tools can increase data concentration, prompt injection risk, model leakage, and third-party attack surfaces.
Internal audit and continuous monitoring	Provides assurance over control design, operation, evidence quality, and remediation status.	Dashboards without testable logs or source evidence can create visibility without accountability.
Regulatory reporting	Improves timeliness, consistency, and examination readiness.	Automated reporting can reproduce incorrect assumptions if data lineage, sign-off, and change control are weak.
Financial inclusion and customer access	Can support digital onboarding, remote service delivery, small business finance, and lower-cost compliance.	Opaque scoring, rigid portals, and unsupported customers can create algorithmic exclusion.

Note. The categories synthesize scholarship and policy sources on RegTech, internal audit, explainability, cybersecurity, financial inclusion, and AI governance (Ali et al., 2023; Freij, 2020; GAO, 2025; McCarthy, 2023; NIST, 2024; Polizzi & Scannella, 2023; Wassie & Lakatos, 2024).

5. Recent Regulatory and Technology Developments

5.1. RegTech Maturity and Cost Asymmetry

The post-2024 evidence base shows that RegTech is no longer a peripheral compliance concept. Charoenwong et al. (2024) provided one of the most important empirical contributions by showing that technology-driven compliance can affect profitability, operations, and market structure. Their findings that information technology budgets may rise and profits may fall, especially for smaller firms, challenge the common assumption that compliance automation automatically lowers costs. RegTech may reduce marginal monitoring costs, but it can increase fixed costs through vendor contracts, integration, cybersecurity, data governance, staff training, model validation, and audit review.

A broader literature review by El Khoury et al. (2024) also emphasized that RegTech has evolved from a narrow compliance efficiency tool into a broader governance and regulatory innovation mechanism. Similarly, Kanojia et al. (2024) reviewed fintech and RegTech literature and connected these technologies to business sustainability. Taken together, this literature suggests that RegTech readiness should be assessed at the level of institutional capability rather than vendor functionality alone.

5.2. AI Governance, Generative AI, and Financial-Sector Oversight

Recent policy and technical guidance has made AI governance more concrete for financial institutions. NIST's Generative AI Profile identifies risks that are novel to or exacerbated by generative AI and maps them to lifecycle risk management actions (NIST, 2024). Although the profile is cross-sectoral, its logic is directly relevant to financial institutions using generative AI for compliance summaries, customer communications, suspicious-activity narratives, policy analysis, training materials, or internal audit planning. Generative AI can support knowledge work, but it can also introduce hallucination, data leakage, information-integrity failures, bias, cybersecurity threats, and unclear responsibility.

Treasury's March 2024 report focused specifically on AI-related cybersecurity risks in the financial sector, noting both the potential of AI to improve cybersecurity and anti-fraud functions and the need to strengthen risk management against AI-enabled threats (U.S. Department of the Treasury, 2024a). The financial-services technical literature moved in the same direction. Dopamu et al. (2024a) framed AI-assisted cybersecurity compliance as a mechanism for real-time threat detection, automated compliance support, and proactive risk management, while Oke et al. (2025c) proposed a fraud-detection architecture that combines machine-learning scoring, real-time communication verification, and blockchain audit logging. Treasury's December 2024 report broadened the analysis to AI uses, opportunities, and risks across financial services, including data privacy, bias, model risk, third-party providers, fraud, and consumer protection (U.S. Department of the Treasury, 2024b). GAO (2025) then examined AI use and oversight in financial services and described how federal financial regulators supervise AI-related risks while also using AI tools in market and supervisory oversight. These sources confirm that financial institutions should expect AI governance to remain tied to existing obligations for risk management, consumer protection, cybersecurity, fraud control, and fair access rather than treated as a separate technology issue.

Generative AI also changes compliance staffing and training needs. The technical note by Aslett et al. (2025) on generative AI for compliance risk analysis in tax and customs administration is not a banking manual, but it is relevant to financial compliance because it describes how GenAI may support risk analysts while requiring responsible use, risk assessment, and training. For financial institutions, the analogous lesson is that GenAI should assist compliance judgment rather than replace it. Any use of GenAI in alert narratives, customer-risk summaries, policy interpretation, or audit documentation should preserve human review, source traceability, confidentiality controls, and quality assurance.

5.3. Financial Stability, Third-Party Risk, and Supervisory Expectations

Financial stability authorities have also emphasized AI's systemic implications. FSOC's 2024 annual report discussed AI as a financial-sector vulnerability and noted the importance of governance, risk management, and controls regardless of whether a tool is formally classified as AI (FSOC, 2024). The FSB (2024) identified potential AI-related financial-stability channels, including operational risk, cyber risk, model risk, third-party dependence, market concentration, and correlated behavior across firms. These concerns are especially relevant where many institutions rely on common cloud providers, shared AI tools, or concentrated data vendors.

The supervisory implication is straightforward: outsourcing a RegTech tool does not outsource responsibility. A financial institution may rely on a vendor for sanctions screening, AML monitoring, customer verification, cloud storage, workflow dashboards, or AI-supported risk scoring, but the institution remains responsible for understanding the tool's

purpose, data flows, limitations, incident procedures, audit rights, and exit risks. Third-party governance therefore belongs inside RegTech readiness, not outside it.

6. Persistent Compliance Challenges

6.1. Fragmented Control Ownership

Financial compliance problems often arise at the boundary between functions. Legal interprets the rule, compliance designs the policy, business units operate the process, technology teams manage systems, cybersecurity manages access, vendors provide tools, and internal audit tests the process afterward. Each function may appear to be performing its role, yet the institution may still lack end-to-end accountability. This is the compliance-audit-technology gap that RegTech can reduce only if it clarifies ownership rather than concealing fragmentation within a workflow.

A practical readiness model therefore requires a documented responsibility structure. Each alert, exception, override, report, data correction, vendor issue, and remediation item should have a named role or accountable owner. RACI matrices are useful only when they are connected to actual workflow evidence. If a dashboard shows an overdue customer review but no one is responsible for resolution, the dashboard is not a control. It is merely a display of an unresolved risk.

6.2. Data Quality and Explainability

AI-enabled compliance systems depend on customer data, transaction records, behavioral signals, device data, cybersecurity logs, prior investigations, and external watchlist or vendor data. Data quality is therefore a control issue. If beneficial ownership records are outdated, transaction codes are inconsistent, customer risk ratings are stale, or vendor data are not validated, automated monitoring may produce false confidence. The institution may process more data without improving compliance reliability.

Explainability is equally important. Arrieta et al. (2020) defined explainable AI in terms of concepts, taxonomies, opportunities, and challenges for responsible AI. Ali et al. (2023) further organized explainability around data, model, post hoc methods, and the assessment of explanations. More recently, Khan et al. (2025) reviewed model-agnostic explainable AI methods in finance and highlighted the need to balance interpretability, scalability, and practical usefulness. For compliance, explainability is not an abstract technical preference. It is the condition that allows staff, auditors, customers, boards, and regulators to understand why a system produced a result and whether that result should be accepted, overridden, or escalated.

6.3. Cybersecurity, Privacy, and Generative AI Misuse

Cybersecurity and privacy risks are inseparable from RegTech adoption. Compliance automation often requires more data integration, more user access, more vendor connectivity, and more cloud-based workflows. These features can improve monitoring but also enlarge the attack surface. Dopamu et al. (2024a) argued that AI-assisted cybersecurity compliance can support real-time threat detection and risk management in U.S. financial institutions, while still requiring ethical implementation and privacy safeguards. Dopamu, Okonkwo, Adeniji, and Oke (2024b) also show why secure digital communication depends on confidentiality, integrity, authenticity, and nonrepudiation; those properties are directly relevant when compliance workflows transmit customer data, reviewer notes, escalation decisions, and audit evidence. Adeniji et al. (2025) extend the concern to cloud and Internet of Things environments, where distributed endpoints, cloud platforms, and connected devices can widen the cybersecurity perimeter. Treasury (2024a) similarly emphasized that AI can improve cybersecurity and anti-fraud functions but can also be exploited by threat actors.

Generative AI intensifies these concerns because it can be used both by institutions and by attackers. Financial institutions may use GenAI to summarize policies, draft narratives, classify documents, or support compliance training. Malicious actors may use similar tools to craft phishing messages, generate synthetic identity materials, imitate voices, or automate reconnaissance. Readiness therefore requires controls around approved use cases, data input restrictions, prompt and output logging where appropriate, human review, incident response, and staff training.

6.4. Algorithmic Exclusion and Proportionality

Modern compliance systems can also affect access. Fuster et al. (2022) showed that machine learning can change outcomes in credit markets across borrower groups. This does not mean that machine learning should be avoided, but it does mean that financial institutions should evaluate how automated systems affect different customer populations. In onboarding, rigid document checks or conservative risk scores can delay or deny legitimate customers. In credit,

predictive models may improve average accuracy while creating fairness, explainability, or customer-communication concerns. In fraud monitoring, automated filters may produce disproportionate friction for customers whose transaction patterns are unfamiliar but legitimate.

Financial inclusion scholarship suggests that technology can expand access when designed responsibly. Erel and Liebersohn (2022) found that fintech lenders expanded access to Paycheck Protection Program loans, including in underserved and lower-income areas. Morgan (2022) reviewed fintech and financial inclusion in Southeast Asia and India and emphasized digital finance's potential to reach excluded groups. Schuetz and Venkatesh (2020) argued that blockchain adoption could reduce some financial inclusion barriers, including geographic distance, high cost, unsuitable products, and limited financial literacy. These studies support a balanced view: technology can widen access, but it can also exclude if systems are opaque, unsupported, or poorly calibrated.

7. Emerging Technologies: Compliance Uses and Failure Modes

7.1. RegTech and SupTech

RegTech refers to technology used by regulated entities to support compliance, while SupTech refers to technology used by supervisors to support oversight. The distinction matters because supervision is becoming more data intensive, and institutions increasingly need systems capable of producing reliable, comparable, and timely evidence. McCarthy (2023) argued that RegTech and SupTech should be consistent in principle and practice. That principle also applies inside institutions: a compliance system should operationalize a regulatory purpose rather than merely automate an administrative task.

RegTech is most defensible where the compliance process has a repeatable structure. Examples include obligation inventories, filing calendars, control libraries, sanctions screening workflows, training attestations, complaint tracking, issue registers, remediation dashboards, and evidence repositories. These use cases may be less impressive than advanced AI, but they address common causes of compliance failure: missed deadlines, incomplete records, unclear ownership, and weak escalation. For smaller banks, these basic capabilities may deliver more immediate value than deploying a complex machine-learning model.

7.2. AI, Machine Learning, and Explainable Compliance Analytics

AI and machine learning are useful where compliance work requires triage across large volumes of data. Goodell et al. (2021) and Pattnaik et al. (2024) both documented the rapid expansion of AI and machine-learning research in finance across risk management, fintech, forecasting, fraud detection, and operational applications. In compliance, the strongest candidates for AI support are anomaly detection, alert prioritization, cyber-event triage, document review, customer-risk updates, transaction monitoring, and audit sampling. Oke et al. (2025c) provide a financial-services-specific example by proposing a layered fraud-detection model that combines machine-learning risk scoring, a real-time communication verification layer, and immutable audit logging; the design illustrates why AI readiness should include escalation channels and evidence capture, not only predictive accuracy.

The risk is that prediction may be mistaken for judgment. A model can rank alerts, but a reviewer must evaluate context. A cyber system can flag anomalous behavior, but escalation depends on risk appetite and incident response policy. A customer risk model can suggest enhanced due diligence, but compliance staff must determine whether the evidence justifies that treatment. Oke et al. (2025c) make this point operationally by pairing automated fraud detection with real-time human or customer verification rather than treating an AI flag as a final decision. Raji et al. (2020) proposed internal algorithmic auditing as an end-to-end accountability framework, and Mökander et al. (2022) emphasized conformity assessments and post-market monitoring for high-risk AI. Both approaches support the same conclusion: AI governance should begin before deployment and continue throughout the system lifecycle.

7.3. Blockchain, Digital Identity, and Traceability

Blockchain and distributed ledger technologies can support traceability, record integrity, and some forms of financial inclusion. They may improve reconciliation, create auditable transaction histories, and support lower-cost cross-border processes. In a directly financial-services context, Oke et al. (2025c) use blockchain audit logging as part of a fraud-response architecture to preserve decisions, verification steps, and outcomes for later review. Cross-sector work on blockchain-enabled consent management also illustrates how distributed ledgers can support privacy, consent traceability, and auditability when they are integrated with interoperable data standards rather than used as standalone databases (Oke et al., 2025a). However, blockchain tools can also create illicit-finance risks if institutions do not understand anonymity features, wallet structures, cross-border flows, mixers, decentralized platforms, or custody

arrangements. Akartuna et al. (2022) used an international policy Delphi study to identify money-laundering and terrorist-financing risks associated with emerging technologies, including cryptocurrencies and digital-only financial services. The lesson is not that blockchain is inherently safe or unsafe. The lesson is that each use case should be assessed according to its data flows, counterparties, evidence, anonymity, consent model, and control design.

Digital identity tools create similar trade-offs. Strong identity verification can reduce fraud and onboarding risk, but poorly designed digital identity processes may reject customers with nonstandard documents, limited broadband access, disability-related barriers, or low digital literacy. Community banks and credit unions serving underserved areas should therefore combine digital verification with human support, manual review paths, and clear procedures for resolving documentation problems.

7.4. Regulatory Sandboxes and Internal Pilots

Regulatory sandboxes allow financial innovations to be tested under controlled conditions. Goo and Heo (2020) argued that sandboxes can support fintech development and open innovation. Even where a financial institution is not part of a formal regulatory sandbox, the same logic can be applied internally. Before deploying a RegTech tool, an institution can test it on historical cases, compare automated outputs with human review, examine false positives and false negatives, validate documentation, and gather staff feedback.

A pilot should not be a loophole. It should have defined boundaries, approved data use, privacy controls, acceptance criteria, user access limits, incident procedures, and a plan for addressing errors. Internal pilot design is especially important for smaller institutions because it allows phased modernization. Oke et al. (2025b) argue in an adjacent regulated setting that AI readiness depends on aligning infrastructure, data governance, processes, people, and ethical oversight; the same logic applies to financial compliance pilots. A bank can begin with a limited use case, such as missing KYC documentation alerts, before moving to more complex AI-supported transaction monitoring or customer risk scoring.

Table 2 Emerging Technology Uses and Compliance Failure Modes

Technology use	Compliance value	Primary failure mode
RegTech workflow tools	Map obligations, assign owners, manage deadlines, capture evidence, and track remediation.	Automating unclear legal interpretation or fragmented ownership.
AI and machine-learning analytics	Prioritize alerts, detect anomalies, support fraud review, cyber triage, and audit sampling.	Treating prediction as judgment; weak validation, bias review, or human oversight.
Generative AI	Summarize policies, draft training content, support compliance risk analysis, and improve knowledge retrieval.	Hallucination, confidential-data exposure, unsupported conclusions, and inadequate source traceability.
Blockchain and digital traceability	Improve record integrity, transaction visibility, reconciliation, and certain inclusion use cases.	Underestimating illicit-finance risk, anonymity, cross-border complexity, and evidence gaps.
Continuous auditing dashboards	Provide more frequent visibility into controls, exceptions, and remediation status.	Creating visual reporting without reliable data, escalation rules, or audit trails.
Vendor-provided RegTech platforms	Give smaller institutions access to capabilities they may not build internally.	Relying on black-box vendor logic without audit rights, incident reporting, validation evidence, or exit planning.

Note. The table synthesizes RegTech, AI governance, blockchain, cybersecurity, and audit literature and post-2024 policy sources (Akartuna et al., 2022; Aslett et al., 2025; Dopamu et al., 2024b; FSB, 2024; NIST, 2024; Oke et al., 2025a, 2025c; U.S. Department of the Treasury, 2024a, 2024b).

8. Inclusive Compliance Modernization for Small Banks and Underserved Areas

8.1. Why Small Institutions Need a Different Starting Point

Compliance modernization is often described from the perspective of large institutions. That perspective is incomplete. Community banks, credit unions, minority depository institutions, rural banks, and small investment firms often serve customers who are not well served by larger financial institutions. They may provide relationship-based lending, local market knowledge, language support, and trust in communities where digital-only models are insufficient. Yet they may have limited budgets for data scientists, model validators, compliance engineers, and enterprise-grade RegTech platforms.

The cost asymmetry identified by Charoenwong et al. (2024) has direct inclusion implications. If compliance technology increases fixed costs, smaller institutions may delay modernization, reduce product offerings, or rely on conservative risk controls that limit access. Conversely, if they adopt complex tools without readiness, they may create vendor dependence, cybersecurity weaknesses, opaque decisions, and customer friction. The proper response is not to avoid technology. It is to adopt proportionate RegTech: lower-complexity tools that improve evidence, escalation, documentation, and risk visibility without overwhelming the institution.

For a small bank serving an underserved area, early RegTech priorities might include a reliable compliance calendar, automated reminders for overdue customer reviews, standardized evidence capture, branch-level issue tracking, vendor due diligence templates, plain-language customer communications, staff training logs, and management dashboards for open exceptions. These tools may not be advanced AI, but they directly reduce compliance risk and improve audit readiness. More sophisticated analytics can be introduced once the institution has stronger data, governance, and oversight capacity.

8.2. Avoiding Algorithmic Exclusion

Algorithmic exclusion occurs when automated or semi-automated systems deny, delay, or discourage access without adequate explanation, review, or correction. In financial compliance, exclusion can occur through customer-risk scores, fraud filters, digital identity checks, rigid document rules, or automated account monitoring. The risk is not only legal; it is also reputational and social. A compliance system that excludes legitimate customers can undermine financial inclusion and weaken the institution's community role.

Table 3 Compliance Modernization Priorities by Institution Type

Institution type	Primary compliance benefit	Implementation priority
Large banks and investment firms	Scalable monitoring across products, business lines, jurisdictions, and large data volumes.	Enterprise model governance, explainability, data integration, independent validation, and board-level risk reporting.
Community banks and credit unions	Reduced manual burden, stronger audit readiness, faster issue tracking, and more consistent customer due diligence.	Modular workflows, evidence capture, staff training, vendor oversight, and phased adoption.
Minority depository institutions and banks in underserved areas	Ability to offer digital access while managing fraud, AML, privacy, and consumer protection risks.	Inclusive onboarding, customer education, human review, plain-language procedures, and protection against algorithmic exclusion.
Fintech and digital finance firms	Embedded compliance controls in product design and real-time regulatory evidence.	Compliance-by-design, cybersecurity, privacy controls, explainable AI, vendor governance, and supervisory documentation.
Small investment advisers and broker-dealers	Improved suitability documentation, disclosure controls, surveillance, and investor protection evidence.	Control mapping, recordkeeping, conflict monitoring, analytics governance, and exception escalation.

Note. The priorities reflect RegTech cost evidence, financial inclusion research, and AI governance scholarship (Charoenwong et al., 2024; Erel & Liebersohn, 2022; Fuster et al., 2022; Morgan, 2022; Schuetz & Venkatesh, 2020).

A practical inclusion-oriented approach does not require weaker compliance standards. It requires better evidence about how systems affect customers. Institutions should monitor whether automated onboarding fails

disproportionately for certain customer segments, whether manual review is available, whether explanations are understandable, whether staff know how to resolve documentation problems, and whether complaint channels identify technology-driven barriers. Goyal and Kumar (2021) showed that financial literacy is a substantial area of research; this is relevant because customers cannot benefit from digital finance if they do not understand procedures, risks, or correction routes.

For underserved communities, human review remains an inclusion safeguard. Automated systems should support staff by reducing manual burden, not replace staff where judgment and customer assistance are essential. A readiness pathway should therefore require manual review routes, accessible procedures, customer-impact reviews, and plain-language communication as part of compliance automation.

9. An Updated RegTech Readiness Pathway

The preceding analysis supports an updated RegTech Readiness Pathway with nine dimensions. The pathway is designed for management, compliance officers, internal auditors, legal teams, information technology staff, cybersecurity professionals, vendor managers, and board risk committees. It can be used before procurement, during pilot testing, and after deployment. The purpose is to make governance conditions explicit before a technology tool becomes embedded in compliance operations.

The first dimension is regulatory-to-control mapping. Institutions should identify the legal or regulatory obligation attached to each process, product, customer segment, jurisdiction, and vendor arrangement. The output should be an obligation-to-control matrix that links legal interpretation to policy, procedure, system control, evidence, owner, and escalation route.

The second dimension is data governance. Compliance data should be accurate, complete, timely, secure, and traceable. This includes data dictionaries, access rights, retention procedures, data lineage, quality checks, and change management. AI and analytics cannot compensate for unreliable source data. Cross-sector work on secure interoperable data systems similarly shows that AI-enabled governance depends on standardized data exchange, encryption, consent management, and compliance tracking rather than data aggregation alone (Oke et al., 2025d).

The third dimension is control ownership. Each alert, exception, report, override, remediation item, and data correction should have an accountable owner. Ownership should distinguish business responsibility, compliance oversight, technology support, cybersecurity responsibility, vendor management, and audit review.

The fourth dimension is automation fit. Some compliance tasks are rules-based, some are analytics-supported, and some are judgment-intensive. Institutions should begin with repeatable tasks where the control logic is clear and retain human review for decisions that affect suspicious activity judgments, account access, credit outcomes, customer vulnerability, or complex remediation.

The fifth dimension is explainability and model governance. Institutions using AI should document model purpose, data sources, assumptions, validation results, limitations, bias risks, human oversight, monitoring cadence, and override procedures. Explainability should be meaningful to compliance staff and auditors, not only data scientists.

The sixth dimension is cybersecurity and privacy-by-design. Data security, privacy, identity access management, encryption, incident response, prompt/input restrictions, and approved-use policies should be built into the RegTech design rather than added after deployment. This is especially important where generative AI, cloud vendors, customer communication tools, or connected endpoints are involved. Secure messaging and cloud/IoT research reinforce that cryptographic safeguards, endpoint protection, and controlled communication channels are components of compliance evidence in data-intensive environments (Adeniji et al., 2025; Dopamu et al., 2024b).

The seventh dimension is third-party oversight. Vendor due diligence should address data use, model logic where available, service-level expectations, audit rights, incident reporting, subcontractors, regulatory access, business continuity, and exit planning. Vendor convenience should not replace institutional accountability.

The eighth dimension is continuous audit evidence. A compliance system should generate records that internal audit can test, including data changes, alerts, reviewer notes, approvals, escalations, overrides, remediation steps, closure evidence, and periodic performance reports.

The ninth dimension is inclusion-oriented proportionality. Institutions should assess whether a tool improves compliance without creating unjustified barriers for legitimate customers or imposing unsustainable burdens on smaller institutions. This includes customer-impact review, manual review routes, plain-language procedures, staff training, and complaint analysis.

Table 4 Updated RegTech Readiness Pathway

Readiness dimension	Diagnostic question	Minimum evidence before deployment
Regulatory-to-control mapping	Which obligation does the tool operationalize, and how is it translated into a control?	Obligation inventory, control matrix, risk ranking, legal/compliance approval, and change-control record.
Data governance	Are source data accurate, complete, timely, secure, and traceable?	Data dictionary, lineage map, quality checks, access controls, retention procedures, and data-owner sign-off.
Control ownership	Who owns alerts, exceptions, overrides, reports, remediation, and issue closure?	RACI matrix, escalation policy, reviewer roles, approval logs, and management reporting cadence.
Automation fit	Is the task rules-based, analytics-supported, AI-assisted, or judgment-intensive?	Use-case inventory, risk rating, pilot plan, acceptance criteria, and human review requirements.
Explainability and model governance	Can staff explain inputs, outputs, limits, validation, bias risks, and monitoring?	Model card, validation report, limitation statement, bias review, override log, and post-deployment monitoring plan.
Cybersecurity and privacy-by-design	Does the design protect confidential data and address AI-specific security risks?	Data protection impact review, access controls, approved-use policy, incident response procedure, and secure logging.
Third-party oversight	Can the institution supervise vendor performance, risks, incidents, and exit arrangements?	Vendor due diligence file, audit rights, service-level commitments, incident notification terms, subcontractor review, and exit plan.
Continuous audit evidence	Will the system generate records that internal audit and management can test?	Audit trail, exception log, evidence repository, remediation tracker, reporting template, and periodic testing plan.
Inclusion-oriented proportionality	Does the tool strengthen compliance without excluding legitimate customers or overburdening small institutions?	Customer-impact review, manual review route, plain-language procedures, complaint path, staff training, and monitoring for exclusion effects.

Note. The pathway updates the earlier readiness model by incorporating post-2024 AI governance, generative AI, cybersecurity, cloud/IoT, fraud-detection, data-interoperability, and financial-sector oversight sources (Adeniji et al., 2025; Aslett et al., 2025; FSOC, 2024; FSB, 2024; GAO, 2025; NIST, 2024; Oke et al., 2025b, 2025c, 2025d; U.S. Department of the Treasury, 2024a, 2024b).

10. Implementation Implications

10.1. For Community Banks, Credit Unions, and Minority Depository Institutions

Smaller institutions should not begin with the most complex version of AI compliance automation. They should begin with the highest-friction compliance processes that are repeatable, evidence-heavy, and costly to manage manually. Examples include overdue KYC reviews, missing documentation alerts, training attestations, vendor review dates, policy acknowledgment tracking, complaint escalation logs, and remediation dashboards. These use cases create visible compliance value without requiring immediate deployment of black-box analytics.

A phased approach also protects institutional relationships. Community banks and credit unions often know their customers in ways that large-scale digital platforms may not. Compliance modernization should preserve that relationship advantage by reducing administrative burden while keeping human review available for unusual or

vulnerable cases. In underserved markets, this can help institutions remain compliant without retreating from products and customers that require additional support.

10.2. For Larger Institutions and Fintech Firms

Larger institutions face a different risk: automation sprawl. They may have multiple AI, analytics, onboarding, monitoring, and reporting tools across business lines and jurisdictions. Without a common readiness pathway, each tool may have its own data assumptions, ownership model, vendor contract, monitoring process, and audit evidence. A readiness framework can impose governance discipline by requiring consistent documentation, explainability standards, control ownership, and post-deployment monitoring across the enterprise.

Fintech firms should treat compliance as part of product design rather than a downstream review function. Compliance-by-design requires legal, risk, cybersecurity, customer-experience, and audit considerations to be integrated into the product lifecycle. This is especially important for digital onboarding, automated credit, payment products, investment platforms, and customer-facing AI tools.

10.3. For Regulators and Policymakers

Regulators and policymakers should recognize the proportionality challenge. If compliance modernization depends only on expensive enterprise platforms, it may unintentionally favor large institutions and weaken community financial infrastructure. Policymakers can support responsible adoption by encouraging interoperable standards, shared control templates, vendor transparency, pilot programs, sandboxes, and technical guidance for smaller institutions. Regulatory clarity should focus not only on what institutions must achieve, but also on the evidence they should maintain to show that automated controls operate responsibly.

Supervisors should also expect institutions to explain AI and RegTech systems in operational terms. The relevant question is not whether a vendor claims that a tool uses AI. The relevant question is whether the institution can connect the tool to a legal obligation, identify the data used, document the control owner, explain the output, preserve audit evidence, manage exceptions, monitor performance, and protect affected customers.

11. Discussion

The central finding of this review is that RegTech readiness is a governance condition. The finance and investment sector cannot rely indefinitely on manual controls, spreadsheet tracking, and fragmented documentation. At the same time, institutions cannot assume that AI, blockchain, workflow software, or dashboards will automatically create better compliance. Technology changes the form of compliance risk. It can make monitoring faster, evidence richer, and reporting more consistent, but it can also introduce opacity, privacy exposure, cybersecurity vulnerabilities, third-party dependence, and disproportionate costs.

The literature supports a cautious but constructive position. RegTech can improve compliance management when aligned with control design and institutional capacity (El Khoury et al., 2024; Freij, 2020; McCarthy, 2023). AI and machine learning can support fraud detection, risk management, cyber monitoring, and audit analytics, but they require explainability, validation, monitoring, secure communication channels, and human oversight (Ali et al., 2023; Dopamu et al., 2024a, 2024b; Goodell et al., 2021; Khan et al., 2025; Oke et al., 2025c; Pattnaik et al., 2024). Recent official reports show that financial-sector AI governance increasingly focuses on privacy, bias, cybersecurity, third-party risk, model risk, and supervisory oversight (FSB, 2024; GAO, 2025; NIST, 2024; U.S. Department of the Treasury, 2024a, 2024b).

The updated readiness pathway contributes by making the preconditions for responsible adoption explicit. Capability language can obscure readiness. A dashboard is not a control if the data are unreliable. A model is not a compliance decision-maker if its use cannot be explained and challenged. A vendor workflow is not an accountability structure if the institution lacks audit rights or exit procedures. An onboarding portal is not inclusive if customers cannot correct errors or obtain human assistance. Readiness makes these issues visible before they become operational failures.

For underserved markets, the paper's contribution is also practical. Small banks and community institutions need compliance systems that are affordable, modular, auditable, and service-preserving. Proportionate RegTech can help them maintain access to financial services by reducing manual burden and improving control evidence. However, the same tools can harm inclusion if they produce rigid risk scoring, unexplained denials, or excessive documentation requirements. Responsible modernization therefore requires both risk discipline and customer-protection discipline.

Limitations and Future Research

This article has limitations. It is a conceptual review rather than an empirical study, and it does not test the proposed pathway using institution-level data. It does not evaluate specific vendors, compare software platforms, or measure the effect of RegTech on audit findings, remediation speed, compliance costs, regulatory sanctions, or customer access outcomes. The review is also multidisciplinary, which creates breadth but limits the ability to draw definitive conclusions for every regulatory regime or institution type.

Future research should test the updated RegTech Readiness Pathway in different institutional settings. Useful contexts would include community banks, credit unions, minority depository institutions, small investment advisers, fintech lenders, and public agencies with financial or compliance oversight responsibilities. Researchers could examine whether regulatory mapping improves remediation time, whether automated evidence capture reduces audit findings, whether explainability reviews improve staff trust in AI outputs, or whether inclusion-oriented controls reduce wrongful onboarding denials.

There is also room for tool development. The literature would benefit from compliance gap diagnostic instruments, model cards for compliance AI, vendor due diligence checklists, AI monitoring templates, regulatory reporting workflows, audit-trail specifications, and staff training curricula. These practical artifacts would move research from diagnosis toward implementation while preserving the caution that technology must be governed, explained, audited, and proportionate.

12. Conclusion

Regulatory compliance in financial institutions is being reshaped by the combined force of regulatory complexity and emerging technology. Traditional compliance practices remain necessary, but they are increasingly insufficient when institutions must govern digital onboarding, AI-assisted monitoring, cybersecurity threats, cloud vendors, blockchain-related risks, data-intensive reporting, and cross-functional control obligations. The solution is not to automate every compliance task. The solution is to build readiness before automation.

This paper has proposed an updated RegTech Readiness Pathway. The pathway emphasizes regulatory-to-control mapping, data governance, control ownership, automation fit, explainability and model governance, cybersecurity and privacy-by-design, third-party oversight, continuous audit evidence, and inclusion-oriented proportionality. These dimensions are especially important for smaller institutions and banks in underserved areas, where compliance burdens can be high and technical capacity may be limited.

The broader contribution is to frame compliance automation as an internal-control transformation. Financial institutions need technology, but they also need legal interpretation, reliable data, accountable ownership, human judgment, vendor discipline, audit evidence, staff capability, customer protection, and proportional implementation. Used well, RegTech can strengthen monitoring, reporting, audit readiness, financial inclusion, and institutional trust. Used poorly, it can deepen opacity, increase dependency, and accelerate weak controls. Readiness is what makes the difference.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Akartuna, E. A., Johnson, S. D., & Thornton, A. (2022). Preventing the money laundering and terrorist financing risks of emerging technologies: An international policy Delphi study. Technological Forecasting and Social Change, 179, Article 121632. https://doi.org/10.1016/j.techfore.2022.121632

[2] Adeniji, S. A., Oke, F., Okolo, J., & Dopamu, O. (2025). Cybersecurity in the age of cloud computing and IoT: Emerging threats and advanced protective technologies. TechRxiv. https://doi.org/10.36227/techrxiv.175459370.08259901/v1

[3] Ali, S., Abuhmed, T., El-Sappagh, S., Muhammad, K., Alonso-Moral, J. M., Confalonieri, R., Guidotti, R., Del Ser, J., Díaz-Rodríguez, N., & Herrera, F. (2023). Explainable artificial intelligence (XAI): What we know and what is left to attain trustworthy artificial intelligence. Information Fusion, 99, Article 101805. https://doi.org/10.1016/j.inffus.2023.101805

[4] Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., García, S., Gil-López, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2020). Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. Information Fusion, 58, 82-115. https://doi.org/10.1016/j.inffus.2019.12.012

[5] Aslett, J., Cantens, T., Chastel, F., Crown, E., & Hamilton, S. (2025). Generative artificial intelligence for compliance risk analysis: Applications in tax and customs administration. IMF Technical Notes and Manuals, 2025(013). International Monetary Fund. https://doi.org/10.5089/9798229012430.005

[6] Charoenwong, B., Kowaleski, Z. T., Kwan, A., & Sutherland, A. G. (2024). RegTech: Technology-driven compliance and its effects on profitability, operations, and market structure. Journal of Financial Economics, 154, Article 103792. https://doi.org/10.1016/j.jfineco.2024.103792

[7] Dopamu, O., Adesiyan, J., & Oke, F. (2024a). Artificial intelligence and US financial institutions: Review of AI-assisted regulatory compliance for cybersecurity. World Journal of Advanced Research and Reviews, 21(3), 964-979. https://doi.org/10.30574/wjarr.2024.21.3.0791

[8] Dopamu, O., Okonkwo, C., Adeniji, S., & Oke, F. (2024b). Secure messaging application using Java Cryptographic Architecture (JCA). World Journal of Advanced Research and Reviews, 22(2), 2056-2063. https://doi.org/10.30574/wjarr.2024.22.2.1670

[9] El Khoury, R., Alshater, M. M., & Joshipura, M. (2024). RegTech advancements-a comprehensive review of its evolution, challenges, and implications for financial regulation and compliance. Journal of Financial Reporting and Accounting. https://doi.org/10.1108/JFRA-05-2024-0286

[10] Erel, I., & Liebersohn, J. (2022). Can FinTech reduce disparities in access to finance? Evidence from the Paycheck Protection Program. Journal of Financial Economics, 146(1), 90-118. https://doi.org/10.1016/j.jfineco.2022.05.004

[11] Financial Stability Board. (2024). The financial stability implications of artificial intelligence. https://www.fsb.org/uploads/P14112024.pdf

[12] Financial Stability Oversight Council. (2024). 2024 annual report. U.S. Department of the Treasury. https://home.treasury.gov/system/files/261/FSOC2024AnnualReport.pdf

[13] Freij, A. (2020). Using technology to support financial services regulatory compliance: Current applications and future prospects of RegTech. Journal of Investment Compliance, 21(2/3), 181-190. https://doi.org/10.1108/JOIC-10-2020-0033

[14] Fuster, A., Goldsmith-Pinkham, P., Ramadorai, T., & Walther, A. (2022). Predictably unequal? The effects of machine learning on credit markets. The Journal of Finance, 77(1), 5-47. https://doi.org/10.1111/jofi.13090

[15] Goo, J. J., & Heo, J.-Y. (2020). The impact of the regulatory sandbox on the fintech industry, with a discussion on the relation between regulatory sandboxes and open innovation. Journal of Open Innovation: Technology, Market, and Complexity, 6(2), Article 43. https://doi.org/10.3390/joitmc6020043

[16] Goodell, J. W., Kumar, S., Lim, W. M., & Pattnaik, D. (2021). Artificial intelligence and machine learning in finance: Identifying foundations, themes, and research clusters from bibliometric analysis. Journal of Behavioral and Experimental Finance, 32, Article 100577. https://doi.org/10.1016/j.jbef.2021.100577

[17] Goyal, K., & Kumar, S. (2021). Financial literacy: A systematic review and bibliometric analysis. International Journal of Consumer Studies, 45(1), 80-105. https://doi.org/10.1111/ijcs.12605

[18] Ibiyeye, T. (2025). The digital dilemma: How financial institutions can harness AI while navigating legal, privacy, and cybersecurity pitfalls. PriCyai Magazine.

[19] Ibiyeye, T., & Ibiyeye, A. (2024). Analyzing economic impact of U.S. trade policies and regulations on business growth using multivariate regression models. Iconic Research and Engineering Journals, 8(5), 276-286.

[20] Ibiyeye, T., & Olayinka, A. A. (2024). Shaping global economic prosperity: The role of policy-driven and technology-enhanced supply chains. Iconic Research and Engineering Journals, 8(6), 1-14.

[21] Ibiyeye, T. O., Iornenge, J. T., & Adegbite, A. (2024). Evaluating regulatory compliance in the finance and investment sector: An analysis of current practices, challenges, and the impact of emerging technologies. IOSR Journal of Economics and Finance, 15(6, Ser. I), 1-8. https://doi.org/10.9790/5933-1506010108

[22] Kanojia, S., Kaur, S., & Bhavya. (2024). Business sustainability in the era of Fintech and Regtech: A systematic literature review. Discover Sustainability, 5, Article 525. https://doi.org/10.1007/s43621-024-00767-5

[23] Khan, F. S., Mazhar, S. S., Mazhar, K., AlSaleh, D. A., & Mazhar, A. (2025). Model-agnostic explainable artificial intelligence methods in finance: A systematic review, recent developments, limitations, challenges and future directions. Artificial Intelligence Review, 58, Article 232. https://doi.org/10.1007/s10462-025-11215-9

[24] McCarthy, J. (2023). The regulation of RegTech and SupTech in finance: Ensuring consistency in principle and in practice. Journal of Financial Regulation and Compliance, 31(2), 186-199. https://doi.org/10.1108/JFRC-01-2022-0004

[25] Mhlanga, D. (2020). Industry 4.0 in finance: The impact of artificial intelligence (AI) on digital financial inclusion. International Journal of Financial Studies, 8(3), Article 45. https://doi.org/10.3390/ijfs8030045

[26] Mökander, J., Axente, M., Casolari, F., & Floridi, L. (2022). Conformity assessments and post-market monitoring: A guide to the role of auditing in the proposed European AI Regulation. Minds and Machines, 32(2), 241-268. https://doi.org/10.1007/s11023-021-09577-4

[27] Morgan, P. J. (2022). Fintech and financial inclusion in Southeast Asia and India. Asian Economic Policy Review, 17(2), 183-208. https://doi.org/10.1111/aepr.12379

[28] National Institute of Standards and Technology. (2024). Artificial intelligence risk management framework: Generative artificial intelligence profile (NIST AI 600-1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.600-1

[29] Oke, F., Adeniji, S. A., Oyeneye, B., Dopamu, O., & Ajibade, B. S. (2025a). Blockchain-enabled consent management in FHIR-compliant oncology platforms. TechRxiv. https://doi.org/10.36227/techrxiv.174918103.37396756/v1

[30] Oke, F., Bolaji, O., Umakor, M., & Dopamu, O. (2025b). Building AI-ready infrastructure for U.S. healthcare: A product management perspective. World Journal of Advanced Research and Reviews, 27(2), 588-603. https://doi.org/10.30574/wjarr.2025.27.2.2892

[31] Oke, F., Bolaji, O., Umakor, M., & Dopamu, O. (2025c). Designing a real-time, AI-driven communication layer for fraud detection in financial services. IOSR Journal of Computer Engineering, 27(4, Ser. 3), 32-45. https://doi.org/10.9790/0661-2704033245

[32] Oke, F., Oyeneye, B., Dopamu, O., Olatunji, A. P., Ibiyeye, A. O., & Ojerinde, S. (2025d). Revolutionizing electronic health records data security and interoperability: Harnessing artificial intelligence with FHIR, fast healthcare interoperability. TechRxiv. https://doi.org/10.36227/techrxiv.174918083.36507291/v1

[33] Pattnaik, D., Ray, S., & Raman, R. (2024). Applications of artificial intelligence and machine learning in the financial services industry: A bibliometric review. Heliyon, 10(1), Article e23492. https://doi.org/10.1016/j.heliyon.2023.e23492

[34] Polizzi, S., & Scannella, E. (2023). Continuous auditing in public sector and central banks: A framework to tackle implementation challenges. Journal of Financial Regulation and Compliance, 31(1), 40-59. https://doi.org/10.1108/JFRC-02-2022-0011

[35] Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J., Theron, D., & Barnes, P. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. In Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (pp. 33-44). Association for Computing Machinery. https://doi.org/10.1145/3351095.3372873

[36] Schuetz, S., & Venkatesh, V. (2020). Blockchain, adoption, and financial inclusion in India: Research opportunities. International Journal of Information Management, 52, Article 101936. https://doi.org/10.1016/j.ijinfomgt.2019.04.009

[37] U.S. Department of the Treasury. (2024a). Managing artificial intelligence-specific cybersecurity risks in the financial services sector. https://home.treasury.gov/news/press-releases/jy2212

[38] U.S. Department of the Treasury. (2024b). Artificial intelligence in financial services: Report on the uses, opportunities, and risks of artificial intelligence in the financial services sector. https://home.treasury.gov/system/files/136/Artificial-Intelligence-in-Financial-Services.pdf

[39] U.S. Government Accountability Office. (2025). Artificial intelligence: Use and oversight in financial services (GAO-25-107197). https://www.gao.gov/products/gao-25-107197

[40] Wassie, F. A., & Lakatos, L. P. (2024). Artificial intelligence and the future of the internal audit function. Humanities and Social Sciences Communications, 11, Article 386. https://doi.org/10.1057/s41599-024-02905-w

[41] World Economic Forum. (2025). Artificial intelligence in financial services. https://reports.weforum.org/docs/WEF_Artificial_Intelligence_in_Financial_Services_2025.pdf