Journal of Banking and Financial Dynamics
Vol. 10, No. 7, 1-16, 2026
ISSN(E): 2576-6821
DOI: 10.55220/2576-6821.v10.1341

Artificial Intelligence Governance and Banking Regulatory Compliance: A Multiple-Case Study of Commercial Banks in Uganda

KIKOMEKO, Joseph[1] ✉
OGBE, Augustine Alloysius[2]

[1,2]*School of Graduate Studies Muteesa I Royal University (MRU), Kampala, Uganda.*
(✉ Corresponding Author)

Abstract

The rapid deployment of Artificial Intelligence (AI) in commercial banking has outpaced traditional oversight structures, creating compliance vulnerabilities within developing regulatory ecosystems. This study investigated the nexus between AI governance and banking regulatory compliance within commercial banks in Uganda. Guided by institutional theory and sociotechnical systems theory, it examined three specific objectives: evaluating algorithmic accountability structures, assessing data privacy compliance frameworks, and analyzing systemic risk mitigation protocols. The researchers adopted a qualitative multiple-case study design, purposively sampling 24 key informants, including Chief Risk Officers, Compliance Heads, and IT Directors, across four Tier-1 commercial banks in Uganda. Semi-structured interviews and institutional document analysis served as the primary data collection methods. Using an abductive thematic synthesis approach, the analysis revealed that while banks have robust technical capabilities, their AI deployment is severely constrained by fragmented internal governance, a lack of local algorithmic auditing protocols, and significant gaps in Bank of Uganda regulatory oversight. The research concludes that banking regulatory compliance in the digital era cannot be achieved through passive adherence to legacy frameworks; it requires a proactive, sociotechnical approach to algorithmic transparency. The study recommends that the Bank of Uganda issue explicit, risk-based AI governance guidelines, and that commercial banks establish independent algorithmic oversight committees to ensure operational resilience and consumer protection.

Keywords: Algorithmic accountability, Artificial intelligence governance, Banking regulatory compliance, Commercial banks, Data privacy, Financial risk, Uganda.

1. Introduction and Background of the Study

The financial services sector has entered an era of unprecedented transformation driven by the deployment of Artificial Intelligence (AI), machine learning models, and advanced predictive analytics. Globally, commercial banks have transitioned from legacy automation to autonomous decision-making systems that drive credit scoring, algorithmic trading, fraud detection, and customer relationship management (Arner et al., 2020). However, the systemic implementation of these technologies has outpaced the evolution of regulatory frameworks, precipitating profound compliance dilemmas (Truby et al., 2020). Financial institutions are now caught in a structural tension between market-driven pressures to adopt autonomous systems and the rigid, historical mandates of banking regulatory compliance (Magnuson, 2020). This friction highlights the critical necessity of AI governance, defined as the overarching architecture of rules, practices, ethical frameworks, and institutional structures designed to monitor, audit, and direct algorithmic behaviors (Jobin et al., 2019).

Historically, banking regulation evolved to manage human-centric and manual operational risks. The Basel Accords (Basel I, II, and III) systematically established capital adequacy requirements, risk-weighted asset classifications, and supervisory review processes intended to mitigate credit, market, and operational risks stemming from quantifiable financial transactions and human oversight (Shetty & Bhat, 2024). The global financial crisis of 2007–2008 accelerated the codification of macroprudential regulation, forcing financial institutions to implement granular compliance frameworks to guarantee institutional soundness and systemic market stability (Brummer, 2011). Concurrently, the emergence of financial technology (FinTech) in the early 2010s introduced complex automated systems into the banking value chain. This phase fundamentally shifted the regulatory focus from static balance-sheet inspections to dynamic operational compliance, giving rise to RegTech (regulatory technology) and SupTech (supervisory technology) frameworks (Buckley, 2017).

By the late 2010s, the integration of deep learning and neural networks in banking introduced a qualitative shift in risk profiles. Autonomous systems began executing credit decisions and anti-money laundering (AML) screenings without explicit human-coded logic, creating the "black-box" phenomenon where internal algorithmic mechanics remain opaque to both bank operators and regulators (Liebergen, 2017). This technological shift triggered a global re-evaluation of financial governance, culminating in major legislative responses such as the European Union's Artificial Intelligence Act (EU AI Act), which established strict risk-based compliance obligations for high-risk AI deployments in financial assessment and credit scoring (European Parliament, 2024).

Within contemporary academic and policy discourse, AI governance in banking has emerged as a central pillar of macroprudential stability. In the global literature, the debate centers on balancing algorithmic efficiency with ethical, legal, and operational compliance (Zetzsche et al., 2020). Scholars argue that autonomous systems amplify existing financial vulnerabilities, including algorithmic bias, data expropriation, and systemic monoculture, where multiple banks utilize identical underlying open-source machine learning models, leading to correlated herd behaviors during market shocks (Danı́elsson et al., 2021).

In the African context, this technological imperative interacts with distinct structural and socio-economic dynamics. Financial markets across Sub-Saharan Africa have leveraged digital infrastructure to drive financial inclusion, skipping traditional brick-and-mortar banking lifecycles in favor of mobile-centric, algorithmic micro-lending and digital wallets (Yaramolu, 2025). However, African regulatory landscapes remain fragmented. While regional hubs like South Africa, Kenya, and Nigeria have advanced their fintech oversight, explicit codification of AI-specific banking mandates remains sparse, leaving commercial entities to navigate a highly ambiguous legal environment (Ebers, 2025).

In Uganda, this phenomenon manifests within a banking sector overseen by the Bank of Uganda (BoU) under the Financial Institutions Act (FIA, 2004) and its subsequent 2016 amendments. The Ugandan banking sector has experienced intensive digital transformation, with Tier 1 commercial banks deploying AI models to process massive alternative datasets for credit scoring, customer churn prediction, and automated compliance screening (Bank of Uganda, 2023). This digital push occurs alongside systemic structural realities, such as an expanding informal economy, limited centralized credit history infrastructure, and the recent operationalization of the Data Protection and Privacy Act (2019).

The intersection of these dynamics creates deep regulatory vulnerabilities. Ugandan commercial banks are adopting sophisticated AI systems developed in Western or Asian contexts, which are frequently trained on datasets that do not reflect local socio-economic realities (Awonde, 2024). Consequently, these institutions must achieve regulatory compliance within a domestic governance framework that lacks explicit statutory guidelines regarding algorithmic transparency, explainability, and liability. Furthermore, this digital transformation takes place amid broader systemic forces, including globalization, cross-border capital flows within the East African Community (EAC), and intense institutional pressures to minimize operational costs through automation (Kasekende, 2022).

Emerging trends post-2020 underscore the urgency of these challenges. The COVID-19 pandemic catalyzed an aggressive pivot toward touchless digital banking in Uganda, forcing institutions to rely heavily on automated fraud detection systems and machine learning-driven risk assessments (Nanziri, 2022). Yet, empirical evaluations reveal growing tensions. Recent scholarly work highlights a rise in algorithmic exclusion, where alternative credit scoring models disproportionately penalize low-income and informal market actors due to biased data inputs (Gwagwa et al., 2022).

Furthermore, the implementation of the National Data Protection and Privacy Act (2019) under the National Information Technology Authority Uganda (NITA-U) has created a regulatory point of friction with the BoU's traditional prudential rules. Banks face significant compliance challenges trying to reconcile the data minimization mandates of NITA-U with the data-intensive training demands of advanced AI models (Ssekiziyivu, 2023). This contradiction underscores an institutional gap: Uganda's financial regulatory architecture remains functionally organized around human-driven operations, lacking the technical instrumentation required to inspect, audit, and regulate autonomous software agents.

This study's significance and justification reside at theoretical, empirical, policy, and practical levels. Theoretically, this research extends the application of institutional and sociotechnical system frameworks to the nascent domain of digital financial regulation in developing economies, offering novel insights into how organizations navigate technological shifts amid regulatory ambiguity. Empirically, it addresses a major gap in sub-Saharan financial literature by providing granular, multi-case qualitative data on the actual deployment and governance of AI within commercial banks, moving beyond purely speculative or high-level global paradigms.

At a policy level, the study provides a diagnostic baseline for the Bank of Uganda, NITA-U, and financial policymakers to draft risk-based, contextualized AI governance guidelines that safeguard systemic stability without stifling innovation. Practically, it delivers an actionable strategic roadmap for bank executives, risk officers, and compliance managers to structure internal algorithmic accountability frameworks, optimize data protection architectures, and build resilient risk-mitigation protocols that protect institutional soundness and consumer welfare within the Ugandan market.

2. Problem Statement

The systemic integration of Artificial Intelligence within Uganda's commercial banking sector has created a critical operational paradigm shift: autonomous algorithms now dictate credit access, evaluate balance-sheet risk, and manage regulatory screening processes (Ssekiziyivu, 2023),(Bank of Uganda, 2023). Existing financial governance literature establishes that while these technologies drive unprecedented operational efficiencies, reduce transaction costs, and enhance fraud detection capabilities, they simultaneously introduce severe vulnerabilities regarding algorithmic opacity, data privacy breaches, and novel vectors of systemic risk ("The Black Box Society: The Secret Algorithms That Control Money and Information," 2015),(Arner et al., 2020). Globally, regulatory bodies have responded by initiating structural reforms, such as the EU AI Act, to enforce algorithmic traceability and strict accountability parameters (European Parliament, 2024). Nationally, the Bank of Uganda has maintained a traditional microprudential oversight regime focused on capital adequacy and human-centric operational controls under the Financial Institutions Act (2004), alongside the generalized enforcement of the Data Protection and Privacy Act (2019) by NITA-U.

Despite these established regulatory architectures, a fundamental mismatch exists between the high-velocity, autonomous nature of AI deployments and the static, legacy compliance frameworks operating within Uganda. The core problem is that commercial banks in Uganda are aggressively embedding advanced, black-box AI systems into their core operations without formal, standardized internal AI governance protocols or explicit regulatory guidance from the central bank. This governance deficit creates a severe compliance exposure. Automated systems operate with minimal algorithmic accountability, creating unmonitored liabilities where unfair credit exclusions, data privacy violations, and structural risks can propagate silently across bank balance sheets. Legacy prudential auditing techniques are fundamentally unequipped to inspect machine learning pipelines, meaning these algorithmic vulnerabilities remain largely invisible during standard regulatory reviews (Awonde, 2024).
This problematic state of affairs highlights several distinct research gaps:

Existing financial frameworks fail to conceptually integrate algorithmic accountability into traditional definitions of operational risk, leaving banks without theoretical models to govern autonomous decision agents (Nwachukwu et al., 2025). Prior scholarship heavily favors quantitative metrics evaluating AI's operational efficiency, leaving a significant lack of deep, qualitative case studies that explore the complex governance adjustments and structural challenges facing risk officers (Birkstedt et al., 2023). The vast majority of AI governance literature focuses on advanced economies with mature institutional ecosystems (e.g., the US and EU), leaving the specific institutional realities of Sub-Saharan Africa, and Uganda in particular, largely unexamined (Birkstedt et al., 2023; Roche et al., 2022). There is a distinct lack of actionable, context-specific frameworks to help Ugandan compliance executives align intensive data-driven AI modeling with the strict requirements of the country's Data Protection and Privacy Act (2019) (Okello, 2013; Oriji et al., 2023)

Failing to conduct this research leaves the Ugandan financial sector highly exposed to systemic disruption. If banks continue to deploy ungoverned AI systems within a regulatory vacuum, the likelihood of widespread algorithmic bias, systemic credit mispricing, and large-scale data privacy failures will increase, potentially eroding public trust in the digital banking infrastructure. This study is therefore a direct response to these unresolved challenges, offering the empirical insights and structural frameworks needed to build a resilient, compliant, and ethically sound digital banking ecosystem in Uganda.

3. Purpose of the Paper

The purpose of this study is to investigate the relationship between Artificial Intelligence governance frameworks and banking regulatory compliance within commercial banks in Uganda, establishing actionable strategies for algorithmic accountability, data privacy, and systemic risk mitigation.

4. Research Objectives

The study was guided by the following three research objectives:

1. To evaluate the effectiveness of algorithmic accountability and explainability structures in ensuring regulatory compliance within commercial banks in Uganda.
2. To assess the structural alignment of AI data pipelines with the provisions of the Data Protection and Privacy Act (2019) within Ugandan commercial banks.
3. To examine the systemic and operational risk mitigation protocols deployed by commercial banks in Uganda to manage AI-driven financial vulnerabilities.

5. Research Questions

This study addresses the following three central research questions:

1. How do commercial banks in Uganda configure algorithmic accountability and explainability structures to satisfy banking regulatory compliance requirements?
2. In what ways do the AI data training and deployment pipelines of Ugandan commercial banks align with the provisions of the Data Protection and Privacy Act (2019)?
3. What systemic and operational risk mitigation protocols do commercial banks in Uganda employ to manage AI-driven financial and operational vulnerabilities?

6. Significance of the Study

This study provides important theoretical, practical, policy, and societal contributions by generating deeper insights into AI governance and regulatory adaptation within Uganda's commercial banking sector. As financial institutions increasingly integrate artificial intelligence into decision-making processes, understanding how banks govern these technologies has become essential for ensuring regulatory compliance, operational resilience, and public trust.

- From an **academic perspective**, this study contributes to the growing body of literature on digital financial regulation, technological governance, and institutional adaptation in emerging markets. While existing AI governance research has largely focused on developed economies with mature regulatory systems, limited empirical evidence exists from African financial ecosystems (Oriji et al., 2023). By providing qualitative insights from the Ugandan banking context, this study extends scholarly understanding of how organizations in developing economies respond to emerging technological challenges, regulatory uncertainty, and institutional pressures. The findings provide a foundation for future research exploring AI governance, digital transformation, and technology-enabled regulatory compliance in similar emerging market contexts.
- For financial industry practitioners, including bank executives, risk managers, compliance officers, information technology leaders, and governance professionals, this study provides practical insights into the challenges and opportunities associated with implementing AI governance frameworks. The research offers a diagnostic perspective for assessing internal AI management practices, strengthening algorithmic accountability, improving data governance mechanisms, and reducing technology-related compliance risks.

By identifying critical governance gaps and organizational capabilities required for responsible AI adoption, the study supports financial institutions in developing more resilient and sustainable governance structures.

- For policymakers and regulatory institutions, including the Bank of Uganda, the National Information Technology Authority–Uganda (NITA-U), and government agencies responsible for financial sector development, this study provides empirical evidence that can inform the development of balanced and context-sensitive AI regulations. Rather than adopting overly restrictive regulatory approaches, the findings highlight the importance of risk-based governance frameworks that protect financial stability, consumer rights, and data privacy while enabling innovation and competitiveness within the banking sector.
- From a societal perspective, this study contributes to the protection of financial consumers by emphasizing the importance of ethical AI deployment, algorithmic fairness, and responsible data management. As banks increasingly rely on automated decision-making systems for services such as credit assessment, fraud detection, and customer profiling (Mazzini & Bagni, 2023), there is a growing need to ensure that AI systems do not reinforce discriminatory practices or create unjust barriers to financial access. By promoting transparent and accountable AI governance, the study contributes to strengthening public confidence in Uganda's financial system and supporting more inclusive digital financial services.

7. Scope of the Study

The scope of this study is defined across five key dimensions: geographical, population, conceptual, temporal, and methodological limitations. These dimensions establish the boundaries within which the investigation was conducted and clarify the specific context in which the findings should be interpreted.

- Geographical Scope. The study was conducted in Kampala, Uganda, which serves as the country's primary financial and technological hub. Kampala was selected because it hosts the headquarters of licensed commercial banks, central risk management departments, information technology divisions, compliance offices, and strategic decision-making functions. The location therefore provides direct access to the institutional actors responsible for designing, implementing, and overseeing AI governance practices within Uganda's banking sector.
- Population Scope. The study targeted senior-level professionals with direct responsibility for technology governance, regulatory compliance, and organizational risk management within commercial banks. The participants included Chief Risk Officers (CROs), Heads of Compliance, Chief Information Officers (CIOs), Data Protection Officers (DPOs), and Legal Directors from selected Tier-1 commercial banks. These participants were selected because of their strategic roles in managing AI-related risks, ensuring regulatory compliance, overseeing digital transformation initiatives, and shaping institutional responses to emerging technologies.
- Conceptual Scope. Conceptually, the study focused on the relationship between AI Governance and Banking Regulatory Compliance. AI Governance was examined through dimensions including algorithmic accountability, data governance structures, transparency mechanisms, human oversight, and risk management protocols. Banking Regulatory Compliance was examined through institutional adherence to regulatory requirements, including Bank of Uganda supervisory expectations, obligations under the Financial Institutions Act (2004), and data protection requirements established under Uganda's data privacy framework. The study therefore explored how commercial banks develop governance mechanisms that enable responsible AI adoption while maintaining compliance with financial sector regulations and ethical technology standards.
- Temporal Scope. The study focused on the period 2021–2026, representing the post-pandemic era characterized by accelerated digital transformation, increased adoption of artificial intelligence applications, and the strengthening of Uganda's digital governance environment. This period captures significant developments in digital banking expansion, data protection implementation, and increasing regulatory attention toward emerging technologies.
- Limitations and Boundaries of the Study. Given the adoption of a qualitative multiple-case study design, the findings are intended to provide analytical and conceptual transferability rather than statistical generalization to all financial institutions. The study provides an in-depth understanding of AI governance practices among selected commercial banks but does not claim universal representation across all categories of financial institutions. Furthermore, access to proprietary AI systems, algorithmic models, and internal governance documentation was limited due to institutional confidentiality and cybersecurity concerns. To address this limitation, the study employed methodological triangulation by combining key informant interviews with publicly available regulatory documents, institutional reports, and policy statements. This approach enhanced the credibility and trustworthiness of the findings while respecting organizational confidentiality requirements.

8. Theoretical Framework

This study is anchored in an integrated theoretical framework that combines Institutional Theory (DiMaggio & Powell, 1983) and Sociotechnical Systems (STS) Theory (Trist & Bamforth, 1951). The combination of these two perspectives provides a comprehensive analytical lens for understanding artificial intelligence (AI) governance within Uganda's commercial banking sector. While Institutional Theory explains the external forces that influence banks to establish AI governance structures, STS Theory explains the internal organizational processes through which these governance mechanisms are implemented and operationalized. Together, the theories enable an examination of AI governance as both an institutional response to regulatory expectations and a sociotechnical challenge requiring alignment between technology, people, and organizational systems.

8.1. Institutional Theory

Institutional Theory, developed by DiMaggio and Powell (1983), argues that organizations are shaped not only by considerations of efficiency and performance but also by pressures to achieve legitimacy within their institutional environments. Organizations often adopt particular structures, practices, and policies because they are expected by regulators, professional communities, and other influential stakeholders. In this study, Institutional Theory explains why commercial banks in Uganda develop AI governance mechanisms in response to changing regulatory expectations, technological uncertainty, and global standards of responsible AI adoption.

The theory identifies three main forms of institutional pressure: coercive, mimetic, and normative isomorphism. Coercive pressures arise from formal and informal demands imposed by powerful external actors, such as government agencies, regulators, and legal institutions. In the context of AI governance, Ugandan commercial banks experience coercive pressures from institutions such as the Bank of Uganda through prudential supervision requirements and from data protection authorities through obligations related to responsible data management and privacy protection. These pressures encourage banks to establish formal AI oversight structures, risk management frameworks, and compliance mechanisms.

Mimetic pressures occur when organizations imitate practices adopted by successful or highly legitimate institutions, particularly under conditions of uncertainty (Lieberman & Asaba, 2006). Because AI governance remains an emerging field in many developing economies, Ugandan commercial banks may adopt governance models developed by international financial institutions or frameworks such as those emerging from global AI regulatory initiatives. Such imitation enables banks to reduce uncertainty, demonstrate technological maturity, and maintain credibility among investors, international partners, and customers.

Normative pressures emerge from professional expectations, industry standards, and shared values among experts and practitioners (Christensen et al., 2024). In AI governance, these pressures include expectations for ethical technology use, professional accountability, cybersecurity standards, and responsible decision-making. Therefore, Institutional Theory provides a valuable explanation of how external regulatory, professional, and societal expectations shape the formal AI governance arrangements adopted by commercial banks.

8.2. Sociotechnical Systems (STS) Theory

While Institutional Theory focuses on external influences, Sociotechnical Systems (STS) Theory provides insight into the internal organizational dynamics involved in implementing AI governance. Originally developed by Trist and Bamforth (1951), STS Theory argues that organizations operate through the interaction of two interconnected components: the technical subsystem and the social subsystem (Lund et al., 2024). The technical subsystem includes technologies, algorithms, digital platforms, automated processes, and information systems, while the social subsystem includes employees, leadership structures, organizational culture, skills, and decision-making practices.

The central assumption of STS Theory is that organizational effectiveness depends on achieving alignment between these two subsystems (Durán, 2021). Technology alone cannot guarantee successful organizational transformation; rather, technological systems must be designed and managed in harmony with human capabilities and organizational realities. This perspective is particularly relevant to AI governance because AI systems introduce new forms of decision-making, risk, and accountability.

Within commercial banking, AI applications such as automated credit scoring systems, fraud detection algorithms, and anti-money laundering monitoring tools require more than technical deployment (Kruse et al., 2019). Their effectiveness depends on whether employees possess the necessary analytical skills, whether governance responsibilities are clearly defined, and whether organizational cultures support ethical and transparent AI use (Kruse et al., 2019). For example, deploying an advanced AI-based credit assessment system without adequate employee training, human oversight mechanisms, or accountability structures may create sociotechnical misalignment, increasing the likelihood of operational and compliance failures (Srinadi, 2023).

Therefore, STS Theory enables this study to examine how commercial banks integrate AI technologies with human expertise, organizational processes, and governance arrangements to achieve responsible AI adoption.

The integration of Institutional Theory and Sociotechnical Systems Theory provides a multidimensional framework for analyzing AI governance in Uganda's commercial banking sector. Institutional Theory explains the macro-level forces that encourage banks to develop AI governance structures, including regulatory requirements, industry expectations, and pressures for legitimacy. Conversely, STS Theory explains the micro-level organizational processes through which these governance structures are translated into operational practices.

This combined framework moves beyond viewing AI governance as merely a technological or regulatory issue. Instead, it conceptualizes AI governance as a complex organizational phenomenon involving the interaction between external institutional demands and internal sociotechnical capabilities. The framework recognizes that effective AI governance requires both institutional legitimacy and internal organizational readiness.

In the Ugandan banking context, commercial banks must simultaneously respond to evolving regulatory expectations while ensuring that their employees, technological infrastructure, and organizational processes are capable of supporting responsible AI implementation. Consequently, the integration of Institutional Theory and STS Theory provides a holistic understanding of how banks navigate the challenges of adopting AI governance systems within a developing financial ecosystem.

Overall, this theoretical framework guides the study in examining how external institutional pressures influence AI governance adoption and how internal sociotechnical alignment determines the effectiveness, sustainability, and ethical implementation of AI systems within commercial banks.

9. Literature Review

The literature review is organized around three primary thematic dimensions derived from the research objectives: Algorithmic Accountability and Explainability, Data Privacy and Security in AI Pipelines, and Systemic and Operational Risk Mitigation.

9.1. Theme 1: Algorithmic Accountability and Explainability

Algorithmic accountability in financial services refers to the distinct allocation of liability, ethical obligation, and auditability for decisions made by autonomous software agents ("The Black Box Society: The Secret Algorithms That Control Money and Information," 2015). A core challenge in modern banking is the lack of explainability in deep learning models, often referred to as the "black-box" problem. Traditional credit risk models, such as logistic regression, provide easily traceable pathways showing exactly how an applicant's income or debt ratio drives their credit score. In contrast, deep neural networks analyze thousands of non-linear variables, making it incredibly difficult to explain the specific rationale behind a denied loan or a flagged transaction (Burrell, 2016).

Globally, the push for explainable AI (XAI) has moved from an academic debate to a core regulatory requirement. Financial bodies like the US Federal Reserve (SR 11-7 guidelines) and the European Banking Authority demand that any model used for credit decisions must be explainable, mathematically verifiable, and open to third-party audits (Reserve, 2011), (European Banking Authority, 2023). Empirical research indicates that failing to enforce algorithmic transparency often leads to systemic discrimination, where models inadvertently learn and replicate historical human biases against marginalized groups (O'Neil, 2016).

In the African and Ugandan contexts, these accountability challenges are amplified by unique structural and economic realities. African banking systems are rapidly deploying AI models to score borrowers who lack formal credit histories, using alternative data points such as mobile money histories, airtime purchases, and social media activity. However, these alternative datasets are frequently full of noise and historical biases that reflect the economic vulnerabilities of informal markets (Dang, 2025).

In Uganda, commercial banks have begun adopting digital banking platforms (Pantserev, 2022). Studies show that these systems are rarely calibrated for the local socio-economic environment, resulting in high rates of arbitrary credit denials for informal workers and small-scale agricultural enterprises (García et al., 2023). This creates a significant regulatory problem: the Bank of Uganda requires banks to maintain fair, non-discriminatory lending practices, but local compliance officers lack the specialized software tools and data science skills required to audit these imported black-box models (Chongomweru et al., 2025).

Consequently, a major contextual gap persists. While global literature focuses on complex algorithmic frameworks like SHAP (Shapley Additive exPlanations) or LIME (Local Interpretable Model-agnostic Explanations), there is very little empirical research showing how compliance officers in developing financial systems can realistically implement these advanced tools given their resource constraints and the lack of explicit guidance from local regulators.

9.2. Theme 2: Data Privacy and Security in AI Pipelines

The operational success of any AI system depends on continuous access to massive volumes of high-quality data. This data dependency creates an institutional tension with modern data protection laws, which are built on principles of data minimization, purpose limitation, and explicit consumer consent (Finck & Biega, 2021). In the banking industry, building an AI pipeline requires gathering, cleaning, and storing extensive datasets to train machine learning models. This process often conflicts with data privacy rules, which explicitly state that institutions should only collect the minimum amount of data necessary for a specific transaction (Olabanji et al., 2024).

Globally, the General Data Protection Regulation (GDPR) in Europe has established strict boundaries for automated processing, granting consumers the explicit "right to an explanation" when automated decisions impact them (Union, 2016). Financial institutions that violate these rules face severe penalties, forcing global banks to invest heavily in privacy-preserving technologies like federated learning and synthetic data generation (Developer & Rachapalli, 2022).

Regionally, Sub-Saharan Africa has seen an acceleration in data privacy legislation, exemplified by Uganda's Data Protection and Privacy Act (2019). This statute enforces strict rules regarding consumer consent, data localization, and mandatory registration for data controllers under the Personal Data Protection Office (PDPO) at NITA-U. However, implementing these rules within AI banking operations has proven highly problematic.

According to Ssekiziyivu (2023), Ugandan banks often face major operational contradictions trying to reconcile the consumer protection mandates of NITA-U with the traditional prudential requirements of the Bank of Uganda. For instance, while NITA-U champions a consumer's right to have their data deleted, BoU's Anti-Money Laundering guidelines require banks to retain detailed financial records for at least 10 years to support financial intelligence investigations.

Furthermore, empirical reviews highlight an implementation gap regarding consent tracking in machine learning pipelines, underscoring the need for clear studies exploring how banks can build compliant data pipelines.

9.3. Theme 3: Systemic and Operational Risk Mitigation

Deploying AI in banking introduces distinct forms of systemic and operational risks that differ fundamentally from traditional financial hazards. In classic banking models, operational risks center on human error, internal process breakdowns, or external events like infrastructure failures (Goodhart, 2011). In contrast, AI-driven operational risks are characterized by algorithmic instability, data drift, where a model's performance degrades because real-world economic conditions diverge from its training data, and cybersecurity vulnerabilities unique to machine learning, such as data poisoning and adversarial manipulation (Danielsson et al., 2021). On a macroprudential level, widespread adoption of identical AI models can create dangerous market monocultures. If multiple commercial banks deploy the same open-source machine learning architectures for risk management, these systems can generate highly correlated, automated responses to market fluctuations. This algorithmic herd behavior can strip liquidity from the market and amplify systemic volatility during an economic downturn(Frimpong, 2026). In Uganda, these risk profiles are shaped by a highly concentrated banking sector where a few Tier 1 institutions drive the vast majority of digital financial innovation (Bank of Uganda, 2023). This concentration heightens the risk of systemic monoculture. If two or three dominant banks utilize similar automated credit scoring engines, an uncorrected error or inherent bias in that software could simultaneously restrict credit across key sectors of the Ugandan economy, such as agriculture or retail trade (Kasekende, 2022). Despite these clear dangers, empirical tracking shows that Uganda's macroprudential frameworks remain largely unequipped for algorithmic risks. The Bank of Uganda's Risk Management Guidelines continue to focus heavily on manual audits, physical security, and traditional credit review committees (Bank of Uganda, 2010).

As Nanziri (2022) observes, there is a distinct lack of institutional mandates requiring banks to perform regular algorithmic stress testing or maintain independent model validation units. This creates a clear methodological and practical gap: while global financial centers are establishing advanced sandboxes and real-time algorithmic monitoring setups, Ugandan banks are left navigating high-risk technological shifts with outdated risk toolkits. This study directly addresses this vulnerability by evaluating the real-world operational protocols currently used by local institutions to bridge this governance gap.

10. Methodology

10.1. Research Paradigm and Philosophical Grounding

This study is positioned within the critical realist research paradigm (). Critical realism posits a stratified ontology consisting of three distinct domains: the Real, the Actual, and the Empirical.

- The Real: The deepest domain, containing objective structures, generative mechanisms, and causal powers that exist independently of human observation (e.g., statutory banking laws, central bank enforcement powers, and the hardcoded architecture of AI software pipelines) (Lawani, 2020).
- The Actual: The domain where these generative mechanisms are activated, generating specific events and outcomes (e.g., an automated credit denial or a regulatory audit trail) (Lawani, 2020).
- The Empirical: The domain of human experience and direct perception, which is socially constructed through historical institutional structures, language, and professional subjectivities (e.g., compliance officers' interpretations of regulatory mandates) (Lawani, 2020).

For an investigation into Artificial Intelligence (AI) governance and banking compliance, critical realism offers significant analytical advantages over pure positivism or interpretivism. A positivist approach would reduce compliance to quantitative logs or deterministic software metrics, thereby missing the complex socio-political struggles and institutional dynamics involved in governance. Conversely, a purely interpretivist approach would treat regulatory compliance as merely a subjective narrative, ignoring the objective constraints of central bank penalties, statutory liabilities, and the concrete structural mechanics of machine learning algorithms.

By adopting a critical realist lens, this study systematically analyzes both the objective, independent structures of AI codebase behaviors and statutory mandates (the Real and Actual) alongside the subjective, real-world experiences of the compliance executives tasked with navigating them (the Empirical).

10.2. Research Approach and Strategy

This study employed a qualitative research approach governed by an abductive research strategy (). Abduction entails a continuous, iterative movement between empirical data collection, contextual analysis, and theoretical frameworks. This systematic movement allowed the study to utilize the structural constructs of Institutional Theory and Sociotechnical Systems (STS) Theory as initial conceptual scaffolding while remaining fully receptive to discovering novel, unexpected behavioral patterns within the empirical data.

Given the highly volatile nature of machine learning deployments (Kour, 2023) and the continuous updates to digital financial law in 2026 (Khazratkulov, 2026), an abductive approach ensured that the final analysis remained theoretically grounded yet tightly coupled with real-time operational shifts within the financial sector.

10.3. Research Design: Multiple-Case Study

The operational strategy utilized a qualitative multiple-case study design. Single-case study designs were rejected due to their narrow institutional focus, which leaves findings highly vulnerable to idiosyncratic corporate cultures or single-bank anomalies. By analyzing multiple distinct commercial banks as independent cases, the study facilitated a rigorous cross-case synthesis, revealing systemic structural vulnerabilities across the broader banking industry rather than isolated institutional occurrences.

The unit of analysis is defined as the Formal AI Governance and Regulatory Compliance Architecture within a banking institution. Four distinct Tier-1 commercial banks in Uganda were selected to represent diverse institutional profiles. To preserve strict institutional anonymity, these cases are designated as follows:

- Case Bank Alpha: A large, multinational financial institution with an extensive regional retail footprint across East Africa.
- Case Bank Beta: A prominent domestic commercial bank focused heavily on retail financial inclusion and mobile-centric digital lending applications.
- Case Bank Gamma: A major subsidiary of an international banking group characterized by deep corporate lending portfolios and institutional asset management.
- Case Bank Delta: A rapidly expanding, digital-first commercial bank catering primarily to small and medium enterprises (SMEs) and open-banking fintech integrations.

10.4. Target Population and Information Power

The target population comprised senior executive leaders and specialized technical directors who wield direct oversight over technology risk, corporate governance, data privacy, and regulatory compliance. Lower-level operational staff were excluded from the sampling frame because they lack the strategic oversight required to articulate institutional governance choices or interpret relational dynamics with the central bank.

Rather than relying on statistical power formulas appropriate only for quantitative sampling, the sample size was determined using the framework of information power. Information power dictates that sample adequacy depends on the study's core aim, sample specificity, theoretical grounding, dialogue quality, and analytical strategy (Malterud et al., 2015). Given the highly specialized focus of this investigation, the precise alignment of the elite sample, and the rich theoretical grounding, a sample of 24 key informants, six symmetrically selected per case bank—provided high information power and successfully achieved theoretical saturation.

Table 1. Sampling Matrix and Informant Profile.

Respondent Designation	Alpha	Beta	Gamma	Delta	Total	Selection Criteria / Inclusion Mapping
Chief Risk Officer (CRO)	1	1	1	1	4	Strategic oversight of institutional and systemic risk vectors.
Head of Regulatory Compliance	1	1	1	1	4	Direct point of contact for Bank of Uganda (BoU) statutory audits.
Chief Information Officer (CIO)	1	1	1	1	4	Responsible for technical infrastructure deployment and AI architecture.
Data Protection Officer (DPO)	1	1	1	1	4	Manages compliance with NITA-U data privacy regulations.
Director of Legal Affairs	1	1	1	1	4	Oversees contractual liability and statutory financial law compliance.
Head of Credit Risk Analytics	1	1	1	1	4	Direct operational oversight of automated algorithmic scoring models.
Total Key Informants	6	6	6	6	24	

10.5. Sampling Technique and Selection Criteria

The study selected participants using purposive sampling, applying a rigorous criterion-based selection strategy (Gentles et al., 2015). Random sampling methods were rejected as structurally inappropriate, as they fail to isolate the specialized expertise required to evaluate complex algorithmic governance. To qualify for inclusion in the final sample, informants had to meet three mandatory criteria:

1. Hold a senior management or executive-level position within one of the selected Tier-1 commercial banks.
2. Possess a minimum of five years of documented professional experience within banking operations, technology risk management, or regulatory financial law in Uganda.
3. Maintain direct accountability for or active participation in the design, approval, evaluation, or auditing of automated algorithmic decision systems within their respective institutions.

10.6. Data Collection Methods and Instruments

This study deployed a dual-source data collection strategy combining semi-structured key informant interviews and institutional document analysis. The integration of these distinct empirical streams enabled methodological triangulation (Torrance, 2012), cross-verifying the subjective accounts of key institutional actors against the formal, documented governance mechanisms through which banks manage AI risks.

10.6.1. Semi-Structured Key Informant Interviews

Semi-structured interviews served as the primary empirical source, striking a balance between standardized, thematic inquiry and exploratory flexibility. A rigorously designed interview guide maintained consistency across all 24 sessions while allowing informants the latitude to articulate nuanced operational realities. The instrument was structured into three thematic modules, each containing four targeted, open-ended questions derived from Institutional and Sociotechnical Systems theories:

Section A: Algorithmic Accountability and Explainability Structures

- Q1. What internal governance protocols guide the approval and deployment of autonomous AI models within your bank?
- Q2. How does your institution explain "black-box" machine learning decisions to consumers who are denied credit?
- Q3. What specific methodologies or software tools do your compliance teams use to audit automated models for algorithmic bias?
- Q4. In what ways do the Bank of Uganda's current audit procedures evaluate your bank's algorithmic decision pipelines?

Section B: Data Privacy Compliance Frameworks

- Q5. How are consumer data minimization mandates integrated into your bank's machine learning data pipelines?
- Q6. What mechanisms does your bank employ to ensure explicit and traceable consumer consent when training AI models?
- Q7. How does your institution resolve operational contradictions between NITA-U data deletion rules and BoU data retention policies?
- Q8. What technical and organizational controls protect your bank's AI data repositories from unauthorized cross-border access?

Section C: Systemic and Operational Risk Protocols

- Q9. What operational procedures does your bank have in place to monitor and correct machine learning model drift over time?
- Q10. How does your institution evaluate the threat of market monoculture if competitive banks deploy similar open-source AI algorithms?
- Q11. What specific business continuity and backup protocols are triggered if a core automated AI system experiences an unexplainable operational failure?
- Q12. How are novel algorithmic risks systematically integrated into your bank's formal corporate risk register and capital adequacy assessments?

10.6.2. Institutional Document Analysis

To triangulate the interview transcripts, a formal documentary analysis was conducted on both internal corporate artifacts and relevant external regulatory materials. This process provided an objective baseline to assess whether stated organizational behaviors matched codified institutional policies. The analyzed corpus included:

- Internal corporate risk registers and capital allocation frameworks.
- Information technology governance policies and AI procurement guidelines.
- Formal Data Privacy Impact Assessments (DPIAs).
- Annual integrated corporate and sustainability reports.
- Internal compliance audit logs and model validation reports.
- Bank of Uganda (BoU) regulatory circulars, letters, and banking supervisory guidelines.

10.7. Data Analysis Approach: Abductive Thematic Synthesis

The qualitative data corpus was analyzed using an **abductive thematic synthesis approach** (). This strategy systematically reconciled inductive insights emerging directly from the lived experiences of banking executives with deductive thematic structures derived from Institutional and Sociotechnical Systems theories.

The analytical workflow followed a disciplined, five-phase procedure:

- Phase One: Data Preparation and Familiarization: Audio recordings were transcribed verbatim. Transcripts were subjected to double-blind validation against the raw audio to guarantee absolute textual accuracy before being loaded into NVivo qualitative analysis software.
- Phase Two: Inductive Open Coding: Textual segments were subjected to initial open coding. First-order codes captured emergent, descriptive phenomena directly from the informants' own terms, focusing on operational friction points, technical blockages, and institutional anxieties without forcing the data into preconceived categories.
- Phase Three: Deductive Theoretical Mapping: The first-order inductive codes were systematically matched against the core constructs of Institutional Theory (e.g., coercive, mimetic, and normative pressures) and Sociotechnical Systems Theory (e.g., technical-structural alignment, human capability constraints).
- Phase Four: Theme Development and Cross-Case Synthesis: The mapped codes were synthesized into higher-order themes across all four institutional cases. This cross-case synthesis isolated sector-wide patterns, structural commonalities, and variance driven by specific corporate profiles.
- Phase Five: Abductive Interpretation and Theoretical Refinement: The final phase integrated the cross-case themes into a unified critical realist narrative, explaining how underlying structural mechanisms (such as regulatory contradictions or software properties) manifest as empirical challenges within the Ugandan banking ecosystem.

10.8. Methodological Rigor and Trustworthiness

To establish methodological rigor equivalent to Q1 publication requirements, the researchers operationalized Lincoln and Guba's (1985) criteria for qualitative trustworthiness.

- Credibility (Internal Validity): Secured via methodological triangulation (corroborating interview transcripts with corporate policies) and formal member-checking, wherein verbatim transcripts and preliminary thematic matrix summaries were returned to a subset of informants to verify interpretive accuracy.
- Dependability (Reliability): Documented via a highly transparent audit trail. Every modification to the codebook, relational mapping choice, and case selection rationale was explicitly cataloged to ensure the study's analytical trajectory is entirely reproducible.
- Transferability (External Validity): Facilitated by providing thick, highly contextual descriptions of the institutional, technological, and regulatory landscape unique to East African emerging markets, allowing subsequent researchers to accurately evaluate the contextual boundaries of the insights.
- Confirmability (Objectivity): Maintained through continuous reflexive journaling and independent double-coding by an external qualitative research peer, ensuring that the primary research team's personal biases or industry preconceptions did not color data collection or thematic synthesis.

10.9. Ethical Procedures and Regulatory Compliance

This study adhered strictly to established institutional and national ethical guidelines. Formal institutional gatekeeper clearance was granted by the executive management boards and research review units of all four participating commercial banks. Every participant voluntarily reviewed and signed a comprehensive informed consent form detailing their right to unconditional withdrawal, zero organizational penalty, and complete identity protection.

To ensure absolute institutional and personal anonymity, all identifiable data points were stripped during the transcription phase. All primary audio recordings, transcripts, and proprietary internal corporate files were heavily encrypted using AES-256 protocols and stored within a multi-factor authenticated, secure cloud environment accessible exclusively to the core research team. This protocol fully satisfies the statutory mandates of Uganda's Data Protection and Privacy Act (2019).

11. Interview Findings

11.1. Objective 1: Algorithmic Accountability and Explainability Structures

The thematic analysis of empirical data from the four case banks revealed a significant structural gap between the deployment of advanced machine learning models and the creation of internal accountability frameworks. Across all cases, participants confirmed that AI engines are extensively used for credit profiling, algorithmic fraud detection, and transactional monitoring. However, the internal mechanisms designed to govern these technologies are largely fragmented. The primary theme that emerged from the interviews was The Principle of the Opaque

Algorithm, characterized by a reliance on third-party software vendors and a lack of local explainability structures. As the Head of Regulatory Compliance at Case Bank Alpha noted:

"We have integrated highly sophisticated neural networks for automated credit scoring, primarily to handle mobile banking loan approvals. However, when the system rejects an applicant, our compliance officers cannot extract the exact mathematical reason for that rejection. We rely almost entirely on the validation certificates provided by the external fintech vendors in Europe. In practice, our internal audit trail stops where the machine learning pipeline begins."

This finding aligns with global concerns raised by (Pasquale, 2016) regarding the growth of a "black-box society" within regulated financial markets, where corporate transparency is often sacrificed for automated efficiency. This dynamic exemplifies a sociotechnical mismatch, a concept rooted in the sociotechnical theory established by Trist and Bamforth (1951) and (Lund et al., 2024): the technical subsystem (the imported AI engine) operates at a level of complexity that completely overwhelms the diagnostic capabilities of the social subsystem (the bank's compliance team).

When compared across cases, Bank Beta exhibited a slightly different approach, utilizing a hybrid scoring system that combines classical logistic regression with machine learning overrides. The Head of Credit Risk Analytics at Case Bank Beta explained:

"We noticed our machine learning model was systematically locking out informal market vendors in Kampala because they lacked formal digital footprints. Because the model's logic was opaque, we couldn't fine-tune it. We had to implement a manual credit committee override to ensure we weren't violating fair lending principles."

This finding highlights a distinct contextual reality in Uganda: the dominance of the informal economy undermines standard Western AI models, which are built assuming users have formal digital histories (Isabirye & Bitalo, 2025).

In Uganda, banks face clear financial and technical barriers that prevent them from adopting these advanced auditing tools, creating an institutional vulnerability where local compliance teams must accept vendor assertions without independent verification (Isabirye & Bitalo, 2025).

The Bank of Uganda's supervisory role was widely described as passive and outpaced by technology. This issue is driven by normative and coercive pressures that have yet to adapt to the digital age. The Director of Legal Affairs at Case Bank Gamma observed:

"The central bank's periodic on-site inspections are completely human-centric. They review paper trails, minutes of credit committee meetings, and static risk registers. They do not request access to our algorithmic pipelines, nor do they possess the technical code-auditing tools to inspect our machine learning models. This regulatory silence creates a form of mimetic safety—we copy global banking layouts not because BoU mandates them, but because it protects us from reputational liability if things go wrong."

This empirical insight reveals that the coercive pressures typically exerted by financial regulators (DiMaggio & Powell, 1983) are practically non-existent regarding AI governance in Uganda. This absence forces commercial banks to rely on mimetic isomorphism, copying international standards to signal legitimacy to global stakeholders.

Ultimately, these findings show that algorithmic accountability within Ugandan commercial banks is performative rather than substantive. The convergence between empirical data and global literature confirms that the black-box problem leads to unfair exclusions and unmonitored institutional liabilities. However, the divergence lies in how banks respond: while global institutions deploy technical explainability layers, Ugandan banks rely on manual interventions or vendor compliance certificates to navigate the gap.

From a sociotechnical perspective, this state of affairs creates a dangerous imbalance where advanced technical systems operate without adequate human supervision or regulatory oversight. This operational deficit directly undermines the integrity of traditional banking compliance frameworks.

11.2. Objective 2: Data Privacy Compliance Frameworks in AI Pipelines

The second major theme identified across the multi-case analysis was Regulatory Friction and Structural Fragmentation in Data Pipelines. This theme captures the operational difficulties banks face when attempting to feed large amounts of consumer data into their AI engines while complying with Uganda's Data Protection and Privacy Act (2019). The data show that while all four banks have appointed Data Protection Officers (DPOs) to satisfy NITA-U mandates, their underlying machine learning pipelines frequently bypass data minimization and purpose limitation principles. The Data Protection Officer at Case Bank Delta summarized this operational tension:

"To train our predictive fraud detection models, the data science team needs access to everything, transaction locations, historical mobile money velocities, browsing behavior on our app, and demographic information. If we strictly enforce NITA-U's data minimization rule, our AI models lose their predictive accuracy. There is a silent, ongoing struggle within the bank between the technology team pushing for data maximization and the compliance team trying to avoid regulatory fines."

Table 2. From an institutional perspective, Ugandan banks find themselves caught between conflicting coercive demands from two regulatory bodies.

Regulatory Body	Core Statutory Mandate	Operational Requirement for Banks	Impact on AI Pipelines
Bank of Uganda (BoU)	Financial Institutions Act (2004) and AML Guidelines	Retain detailed transaction and customer records for 10 years.	Mandates data maximization and long-term storage.
Personal Data Protection Office (NITA-U)	Data Protection and Privacy Act (2019)	Enforce data minimization, purpose limitation, and user data deletion.	Restricts data collection and demands data purging.

This statutory contradiction emerged repeatedly across all four cases. The CIO at Case Bank Alpha noted:

"A customer can formally request the bank to delete their data under the 2019 Act. However, if that customer was flagged by our automated AML system, the Bank of Uganda's anti-money laundering rules require us to preserve those records for at least a decade. We currently lack a unified technical architecture to partition data so that it satisfies NITA-U's deletion rules without triggering severe policy violations with the central bank."

This structural gap highlights a clear methodological and practical deficiency within Uganda's financial infrastructure. While global banks use advanced privacy-preserving tools like federated learning or differential privacy to anonymize data during model training (Dash et al., 2022), Ugandan commercial banks continue to process raw consumer data within traditional centralized storage arrays (Ssekiziyivu, 2023). Furthermore, the cross-case synthesis reveals that consent mechanisms are often performative. Consumers are forced to accept long, complex Terms and Conditions documents when opening digital accounts, giving the bank broad, permanent rights to use their data for algorithmic analysis.

The Director of Legal Affairs at Case Bank Beta admitted:

"The consent we obtain is rarely 'informed' or 'specific' in the spirit of the law. It is bundled into the digital onboarding process. If a user declines to share their data for algorithmic profiling, they are simply denied access to our digital banking services. This is a practical compromise that our industry takes because the current regulatory oversight from NITA-U lacks the enforcement capacity to audit corporate data workflows."

This finding critiques the optimistic view that local data protection laws automatically safeguard consumer rights in digital-first economies (Ebers, 2025). In practice, structural market imbalances allow commercial banks to prioritize technical performance over privacy rules, using performance-driven compromises that remain unpunished due to weak regulatory enforcement. These findings demonstrate that conflicting regulatory mandates and a lack of advanced privacy engineering tools severely hinder data privacy compliance within AI pipelines. The empirical evidence shows that banks routinely prioritize the technical demands of their AI models over data protection laws, relying on broad, bundled user consent to minimize legal liability.

Viewed through Sociotechnical Systems Theory, this situation reflects a failure to align the bank's technical data architectures with the legal rules of the social subsystem. This lack of structural integration creates significant long-term compliance risks, exposing institutions to potential legal battles and sudden regulatory penalties as data privacy enforcement matures in Uganda.

11.3. Objective 3: Systemic and Operational Risk Mitigation Protocols

The third theme that emerged across all cases was The Algorithmic Drift and Market Monoculture Exposure, which highlights the distinct operational vulnerabilities created by unmanaged machine learning models. The key informants stated that while their banks have comprehensive disaster recovery plans for physical infrastructure and legacy core banking software, their risk mitigation protocols are unequipped to handle complex algorithmic anomalies such as model drift, data poisoning, or systemic herd behavior. The Chief Risk Officer (CRO) at Case Bank Gamma emphasized this issue:

"We use a machine learning engine to re-evaluate our corporate loan portfolio risk every week. However, during periods of economic instability or sharp inflation spikes in Uganda, the model's predictive value degrades rapidly—a phenomenon known as model drift. Our risk department lacks the quantitative tooling to continuously track this decay. We usually only realize the model is mispricing risk after non-performing loans start showing up on our balance sheet."

This insight supports the arguments of Danielsson et al. (2022) and (Daníelsson et al., 2019), who state that AI models create a false sense of security because they are unequipped to manage structural shifts or sudden economic anomalies that deviate from their historical training data. Within the framework of Sociotechnical Systems Theory, this represents a dangerous breakdown: the social subsystem (the risk management department) blindly trusts the automated outputs of the technical subsystem, failing to realize that the underlying software is quietly degrading due to shifting real-world conditions. The cross-case analysis also revealed a significant structural risk regarding market monoculture, driven by identical choices across competing institutions. The CIO at Case Bank Beta explained:

"Due to high development costs, almost all Tier-1 banks in Uganda source their core risk analytics and fraud detection software from the same two or three international suppliers. These vendors utilize identical underlying open-source machine learning frameworks. If an inherent error or systemic bias exists within those core models, it will impact multiple major banks simultaneously. During a major financial shock, our automated systems could execute identical, correlated risk-mitigation actions, like cutting off credit lines to specific sectors—which would amplify a market downturn across Uganda."

This empirical finding highlights a major macroprudential concern that is rarely addressed in emerging market policy documents (Kasekende, 2022). While traditional banking regulation focuses on idiosyncratic risk management at individual banks, the widespread deployment of standardized AI models creates a highly interconnected risk profile across the entire financial sector(Frimpong, 2026). The study found that the Bank of Uganda's Risk Management Guidelines (2010) are completely silent on these interconnected dangers, failing to mandate independent algorithmic validation or cross-institutional model stress-testing (Nanziri, 2022). Consequently, banks continue to manage these advanced technological risks using legacy corporate frameworks. The Head of Credit Risk Analytics at Case Bank Delta noted:

"Our formal risk register treats AI simply as an IT system uptime metric. If the server is running and the software is processing transactions, the risk is marked as green. The deeper structural hazards, such as biased credit scoring, data drift, and vendor lockdown—are completely missing from our regulatory capital calculations. We are flying blind into an algorithmic future using an analog radar."

These insights demonstrate that current risk mitigation protocols in Ugandan commercial banks are fundamentally unequipped to handle the unique challenges of machine learning operations. The convergence of empirical data across all four case banks shows an over-reliance on vendor-supplied solutions and a lack of proactive internal tracking structures.

Viewed through Institutional Theory, this state of affairs highlights a significant regulatory gap: the central bank's legacy oversight tools fail to incentivize banks to build modern algorithmic risk controls. As a result, banks continue to prioritize short-term automation over long-term operational resilience, leaving the entire Ugandan financial ecosystem vulnerable to sudden, systemic algorithmic disruptions.

12. Discussion

The findings of this multiple-case study provide a detailed diagnostic examination of the complex relationship between artificial intelligence governance and banking regulatory compliance within an emerging financial ecosystem. By analyzing four Tier-1 commercial banks in Uganda, this research shows how internal corporate structures adapt to advanced technologies amidst significant regulatory ambiguity. The discussion below is organized around the study's three core research objectives, detailing how the empirical insights connect to existing literature, theoretical frameworks, and practical governance models.

12.1. Objective 1: Algorithmic Accountability and Explainability Structures

The first objective sought to evaluate the effectiveness of algorithmic accountability and explainability structures in ensuring regulatory compliance within commercial banks in Uganda. The empirical findings reveal a performative approach to governance, where banks deploy complex machine learning models for high-stakes decisions such as credit scoring while remaining dependent on external vendors for model validation. This lack of direct operational transparency creates what this study calls. The Principle of the Opaque Algorithm, where local compliance teams cannot independently audit or explain automated outcomes. This state of affairs confirms the broader warnings of Pasquale (2015) and Burrell (2016), who argue that the growth of black-box algorithms within financial markets erodes institutional accountability and undermines consumer protection. Globally, advanced regulatory frameworks such as the EU AI Act address this challenge by enforcing strict traceability mandates and a consumer's explicit "right to an explanation" for automated choices (European Parliament, 2024).

However, the empirical evidence shows a sharp divergence in Uganda: local commercial banks lack the specialized software infrastructure and advanced data science skills required to run explainable AI (XAI) frameworks such as SHAP or LIME. Instead, they rely on vendor-supplied certificates to satisfy basic corporate governance reviews (Awonde, 2024). Viewed through Sociotechnical Systems Theory (Trist & Bamforth, 1951), this issue highlights a severe structural friction between a bank's technical subsystem (the imported neural network) and its social subsystem (the compliance department). Because compliance officers cannot unpack how an algorithm operates, they are functionally unable to monitor its fairness or intervene when it displays bias. Furthermore, the data show that the Bank of Uganda's traditional auditing protocols remain entirely human-centric, focusing on paper trails and static risk registers while ignoring algorithmic code pipelines (Ssekiziyivu, 2023). This regulatory gap shields banks from immediate legal penalties but leaves them highly exposed to hidden operational liabilities. Applying Institutional Theory (DiMaggio & Powell, 1983), the absence of explicit, coercive oversight from the central bank causes institutions to use mimetic behavior. Banks copy international governance models not to comply with local laws, but to project corporate legitimacy to global financial counterparties and credit rating agencies.

12.2. Objective 2: Data Privacy Compliance Frameworks in AI Pipelines

The second objective assessed the structural alignment of AI data pipelines with the mandates of the Data Protection and Privacy Act (2019) within Ugandan commercial banks. The investigation revealed a deep operational conflict: the data-intensive training needs of advanced machine learning models run directly counter to statutory privacy rules such as data minimization and purpose limitation. This friction is compounded by a lack of advanced privacy-preserving tools within local banking architectures. This conflict matches global scholarship highlighting the fundamental tension between data-driven machine learning operations and strict privacy laws like the GDPR (Zetzsche et al., 2020),(Raso et al., 2018). While global financial institutions use advanced techniques like federated learning and synthetic data to protect consumer privacy during model training(Rabbani et al., 2024; Spears et al., 2025) the empirical findings show that Ugandan commercial banks continue to process raw consumer data within traditional, centralized storage systems. Furthermore, this study identifies a critical local complication: banks face contradictory demands from overlapping regulatory bodies. NITA-U enforces a consumer's right to data deletion, while the Bank of Uganda's AML rules mandate that customer data must be stored for at least ten years to support financial intelligence audits. Faced with this regulatory contradiction, banks routinely prioritize algorithmic performance over privacy ideals, using broad, bundled terms of service agreements to secure legal cover. This insight challenges the optimistic view that simply passing data privacy laws guarantees consumer safety in digital-first economies (Ebers, 2025). In reality, because local regulatory bodies lack the technical capacity to audit live corporate data streams, banks continue to repurpose consumer profiles to train their commercial AI engines without explicit user knowledge (Ssekiziyivu, 2023).

From a sociotechnical perspective, this operational compromise reflects a failure to align technological workflows with legal mandates, creating long-term compliance risks that could trigger severe financial and reputational damage as data protection enforcement in Uganda matures.

12.3. Objective 3: Systemic and Operational Risk Mitigation Protocols

The third objective analyzed the systemic and operational risk mitigation protocols deployed by commercial banks in Uganda to manage AI-driven financial vulnerabilities. The empirical findings reveal that while banks have robust disaster recovery protocols for physical infrastructure and legacy banking software, their risk systems are ill-equipped to handle unique algorithmic vulnerabilities like model drift, data poisoning, and systemic market monoculture. This finding supports the warnings of Danielsson et al. (2022), who assert that advanced AI systems can create a false sense of security while introducing hidden risks into financial markets. In Uganda, this vulnerability is heightened by a highly concentrated banking sector where most Tier-1 institutions source their risk analytics tools from the same small group of global vendors. As the cross-case synthesis shows, this concentration creates a dangerous risk of market monoculture: multiple major institutions utilize identical underlying machine learning frameworks. During an unexpected macroeconomic shock, these automated engines could execute highly correlated risk-reduction actions—such as freezing credit to specific informal sectors, amplifying a market downturn across the entire Ugandan economy (Frimpong, 2026). Despite these systemic risks, current regulatory frameworks in Sub-Saharan Africa often focus on traditional methods, failing to adequately address modern protections like independent algorithmic stress-testing or dedicated model validation units (ALAWODE et al., 2026). Consequently, commercial banks continue to treat AI systems merely as standard IT assets in their corporate risk registers, focusing on server uptime while ignoring the deeper hazards of model decay and vendor lock-in (Nwachukwu et al., 2025). By failing to integrate these algorithmic risks into their capital adequacy assessments, banks create a major governance blind spot (ALAWODE et al., 2026). This study directly addresses this gap by showing that true banking compliance in the digital era requires moving past analog checklists to build dynamic, automated auditing structures that safeguard both individual institutions and the wider macroprudential ecosystem.

13. Conclusions and Recommendations

13.1. Conclusions

This multiple-case study provides a comprehensive evaluation of artificial intelligence governance and banking regulatory compliance within Tier 1 commercial banks in Uganda. The core conclusion is that while the deployment of machine learning algorithms has driven significant operational efficiencies and expanded digital financial inclusion, it has simultaneously created a critical governance deficit. Ugandan commercial banks are embedding autonomous black-box engines into core decision-making pipelines without establishing the necessary internal accountability structures, explainability protocols, or privacy-preserving architectures. This operational gap leaves institutions highly exposed to hidden liabilities, including algorithmic bias, data privacy violations, and performance decay over time.

Furthermore, this study demonstrates that Uganda's financial regulatory framework is facing a critical structural mismatch. Uganda's current governance structures inadequately address emerging ethical challenges in AI, particularly concerning privacy and digital rights (Okello, 2013). In digital markets, predatory financial applications often abuse informed consent, using bundled user consent agreements to obfuscate privacy disclosures (Pervez et al., 2026).

Ultimately, achieving genuine banking compliance in the digital era cannot be accomplished through passive adherence to outdated monitoring frameworks. As Sociotechnical Systems Theory outlines, it requires an active, integrated approach where advanced technical pipelines are structurally aligned with trained human compliance teams and dynamic regulatory parameters. Without clear, risk-based AI governance mandates, the continued expansion of unmanaged algorithms poses a substantial threat to financial inclusion and consumer welfare, particularly in developing countries (Truby, 2020).

13.2. Recommendations

To address the governance deficits and regulatory friction points identified in this study, the following integrated roadmap is proposed for key stakeholders within Uganda's financial and regulatory sectors:

For Regulatory Authorities (Bank of Uganda and NITA-U)

- Issue Risk-Based AI Governance Guidelines: The Bank of Uganda (BoU) should immediately draft and issue a dedicated financial technology regulatory circular focused specifically on artificial intelligence governance. This framework should move past generic IT asset management to mandate independent algorithmic auditing, explicit model validation protocols, and mandatory explainability standards for all high-risk banking models, such as automated credit scoring and anti-money laundering screening systems.
- Establish a Joint Digital Regulatory Taskforce: The BoU and the Personal Data Protection Office (PDPO) under NITA-U should establish a formal, permanent joint committee to harmonize financial data retention policies with consumer data protection rules. This body should provide clear, unified guidance on data partitioning techniques and compliance frameworks, ensuring banks can fulfill their anti-money laundering duties without violating consumer privacy rights.
- Build Technical SupTech Infrastructure: The central bank must invest in upgrading its supervisory technology (SupTech) capabilities, hiring specialized data scientists and software engineers capable of executing dynamic, live audits of commercial machine learning pipelines during periodic institutional reviews.

For Commercial Banking Institutions

- Form Independent Algorithmic Oversight Committees: Tier 1 commercial banks should move past traditional IT reporting lines to establish a dedicated, cross-functional Algorithmic Governance Committee. This body, comprising risk officers, compliance directors, data scientists, and legal experts, should hold sole authority for approving, monitoring, and deactivating autonomous models, ensuring that all technical deployments align directly with ethical corporate values and statutory laws.
- Deploy Explainable AI (XAI) and Privacy-Preserving Technologies: Banks must actively invest in modern data engineering tools to reduce reliance on third-party vendor assertions. Internal technology teams should integrate explainability layers (such as SHAP or LIME frameworks) into their machine learning pipelines to provide clear, traceable reasons for automated choices, while deploying privacy-preserving techniques like data anonymization and synthetic data generation to minimize consumer privacy risks.
- Incorporate Algorithmic Risks into Stress-Testing Regimes: Risk management departments must explicitly integrate algorithmic vulnerabilities, including model drift, data poisoning, and vendor lock-in hazards, into their corporate risk registers and capital adequacy assessments. Banks should execute regular, automated stress-testing simulations to monitor how their predictive models perform during sudden economic shocks, mitigating the dangers of market monoculture and correlated balance-sheet failures.

References

Adanma, U. M., & Ogunbiyi, E. O. (2024). Artificial intelligence in environmental conservation: Evaluating cyber risks and opportunities for sustainable practices. *Computer Science & IT Research Journal, 5*(5), 1178–1209. https://doi.org/10.51594/csitrj.v5i5.1156

Aderibigbe, A. O., Ohenhen, P. E., Nwaobia, N. K., Gidiagba, J. O., & Ani, E. C. (2023). Artificial intelligence in developing countries: Bridging the gap between potential and implementation. *Computer Science & IT Research Journal, 4*(3), 185–199. https://doi.org/10.51594/csitrj.v4i3.629

Adeyelu, O. O., Ugochukwu, C. E., & Shonibare, M. A. (2024). Automating financial regulatory compliance with AI: A review and application scenarios. *Finance & Accounting Research Journal, 6*(4), 580–601. https://doi.org/10.51594/farj.v6i4.1035

Alawode, O., Nwobodo, H., Nwobu, O., Eriabie, S. O., & Arogundade, J. A. (2026). Digital transformation and bank capital adequacy in Sub-Saharan Africa. *Asian Economic and Financial Review, 16*(2), 22–37. https://doi.org/10.55493/5002.v16i2.5903

Alozie, C. E., Umeanozie, C. P., Onyekwuluje, T. P., & Ekine, E. U. (2026). Compliance challenges in AI-driven IT infrastructure: A framework for mitigation and governance. *International Journal of Computer Applications, 187*(78), 63–85. https://doi.org/10.5120/ijca2026926338

Arner, D. W., Buckley, R. P., Zetzsche, D. A., & Veidt, B. (2020). Sustainability, equity, and digital financial inclusion: The evolving role of artificial intelligence in banking. *Journal of Financial Regulation, 6*(2), 245–277. https://doi.org/10.1093/jfr/fjaa006

Awonde, G. (2024). Digital financial services and the informal sector in East Africa: A critical evaluation of machine learning credit scoring models. *African Development Review, 36*(1), 45–59. https://doi.org/10.1111/afrd.12412

Bank of Uganda. (2010). *Risk management guidelines for financial institutions*. Bank of Uganda Financial Sector Supervision Department.

Bank of Uganda. (2023). *Annual integrated report 2022/2023: Navigating the digital frontier in monetary and prudential regulation*. Bank of Uganda.

Birkstedt, T., Minkkinen, M., Tandon, A., & Mäntymäki, M. (2023). AI governance: Themes, knowledge gaps and future agendas. *Internet Research, 33*(7), 133–167. https://doi.org/10.1108/INTR-01-2022-0042

Brummer, C. (2011). *Soft law and the global financial system: Rule making in the 21st century*. Cambridge University Press. https://doi.org/10.1017/CBO9780511792458

Buckley, R. P., Arner, D. W., & Barberis, J. N. (2017). FinTech, RegTech, and the reconceptualization of financial regulation. *Northwestern Journal of International Law & Business, 37*(3), 371–413

Burrell, J. (2016). How the machine "thinks": Understanding opacity in machine learning algorithms. *Big Data & Society, 3*(1). https://doi.org/10.1177/2053951715622512

Essien, I. A., Ajayi, J. O., Erigha, E. D., Obuse, E., & Ayanbode, N. (2025). AI-driven governance systems for proactive regulatory compliance and fraud risk management in financial service environments. *Engineering and Technology Journal, 10*(9). https://doi.org/10.47191/etj/v10i09.26

Chen, L., Xie, Y., Wang, Y., Ge, S., & Wang, F. (2024). Sustainable mining in the era of artificial intelligence. *IEEE/CAA Journal of Automatica Sinica, 11*(1), 1–4. https://doi.org/10.1109/JAS.2023.124182

Chongomweru, H., Nyende, H., Kasauli, R., & Balikuddembe, J. K. (2025). Artificial intelligence in software startups and special challenges in least developed countries: A case study of Uganda. In *Proceedings of the 2025 International Conference on Software Engineering and Information Systems* (pp. 15–20). IEEE. https://doi.org/10.1109/SEIGS66664.2025.00015

Christensen, S., Lund, A. B., Byrkjeflot, H., & Popp-Madsen, B. A. (2024). Introduction. In *[Book title needs verification]* (pp. 1–20). Routledge. https://doi.org/10.4324/9781003382775-1

I., C. M., Olowonubi, J. A., Fatounde, S. A., & Oyegunwa, O. A. (2023). Artificial intelligence in the era of 4IR: Drivers, challenges and opportunities. *Engineering Science & Technology Journal, 4*(6), 473–488. https://doi.org/10.51594/estj.v4i6.668

Cramarenco, R. E., Burcă-Voicu, M. I., & Dabija, D. (2023). The impact of artificial intelligence (AI) on employees' skills and well-being in global labor markets: A systematic review. *Oeconomia Copernicana, 14*(3), 731–767. https://doi.org/10.24136/OC.2023.022

Dang, A. (2025). AI-driven credit scoring and financial inclusion: Performance, fairness, and transparency in alternative-data lending. *Advanced International Journal for Research, 6*(6). https://doi.org/10.63363/aijfr.2025.v06i06.2229

Daníelsson, J., Macrae, R., & Uthemann, A. (2019). *Artificial intelligence and systemic risk. SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3410948

Daníelsson, J., Macrae, R., & Uthemann, A. (2022). Artificial intelligence and systemic risk. *Journal of Banking & Finance, 140*, 106290. https://doi.org/10.1016/j.jbankfin.2021.106290

Dash, B., Sharma, P., & Ali, A. (2022). Federated learning for privacy-preserving: A review of PII data analysis in fintech. *International Journal of Software Engineering & Applications, 13*(4), 1–13. https://doi.org/10.5121/IJSEA.2022.13401

Rachapalli, S. K. (2022). Building AI pipelines that comply with GDPR, HIPAA, and industry standards. *International Scientific Journal of Engineering and Management, 1*(1), 1–9. https://doi.org/10.55041/ISJEM00141

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review, 48*(2), 147–160. https://doi.org/10.2307/2095101

Durán, G. de J. P. (2021). Systemic model of organizations. *Open Journal of Business and Management, 9*(3), 1230–1245. https://doi.org/10.4236/ojbm.2021.93066

Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J. S., Eirug, A., Galanos, V., Ilavarasan, P. V., Janssen, M., Jones, P., Kar, A. K., Kizgin, H., Kronemann, B., Lal, B., Lucini, B., ... Williams, M. D. (2021). Artificial intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management, 57*, 101994. https://doi.org/10.1016/j.ijinfomgt.2019.08.002

Ebers, M. (2025). Regulating AI in the Global South: Contextual challenges, institutional design, and lessons from African banking transformations. *International Data Privacy Law, 15*(1), 12–31. https://doi.org/10.1093/idpl/ipad022

European Banking Authority. (2023). *Report on the deployment of machine learning models in banking internal ratings-based frameworks*. European Banking Authority.

European Parliament. (2024). *Artificial Intelligence Act: Text adopted by the European Parliament on 13 March 2024*. European Parliament.

U. F., F., & Zh. R., Z. (2026). Compliance of banking AI systems with EU AI Act requirements and their role in risk management. *Zenodo*. https://doi.org/10.5281/zenodo.19246782

Finck, M., & Biega, A. J. (2021). Reviving purpose limitation and data minimisation in data-driven systems. *Technology and Regulation, 2021*, 44–61. https://doi.org/10.71265/z7r0t122

Frimpong, V. (2026). *Model monoculture risk: Systemic AI convergence in banking and financial markets*. *Preprints.org*. https://doi.org/10.20944/preprints202603.0393.v1

García, A. C. B., García, M., & Rigobón, R. (2024). Algorithmic discrimination in the credit domain: What do we know about it? *AI & Society, 39*(4), 2059–2098. https://doi.org/10.1007/s00146-023-01676-3

García-Llorente, C., & Olmeda, I. (2026). Algorithmic governance in banking: A comparative analysis of risk-based and accountability-oriented oversight. *Journal of Banking Regulation, 27*(2). https://doi.org/10.1057/s41261-026-00320-6

Gentles, S. J., Charles, C., Ploeg, J., & McKibbon, K. A. (2015). Sampling in qualitative research: Insights from an overview of the methods literature. *The Qualitative Report, 20*(11), 1772–1789. https://doi.org/10.46743/2160-3715/2015.2373

Goh, H., & Vinuesa, R. (2021). Regulating artificial intelligence applications to achieve the sustainable development goals. *Discover Sustainability, 2*(1), Article 52. https://doi.org/10.1007/s43621-021-00064-5

Gohr, C., Aboytes, J. G. R., Belomestnykh, S., Berg-Moelleken, D., Chauhan, N., Engler, J., Heydebreck, L. V., Hintz, M. J., Kretschmer, M.-F., Krügermeier, C., Meinberg, J., Rau, A., Schwenck, C., Aoulkadi, I., Poll, S., Frank, E., Creutzig, F., Lemke, O., Maushart, M., ... von Wehrden, H. (2025). Artificial intelligence in sustainable development research. *Nature Sustainability, 8*(8), 970–978. https://doi.org/10.1038/s41893-025-01598-6

Goodhart, C. A. E. (2011). *The Basel Committee on Banking Supervision: A history of the early years, 1974–1997*. Cambridge University Press. https://doi.org/10.1017/CBO9780511996238

Goswami, A. A. V. (2026). The role of artificial intelligence in financial regulation and compliance: Evidence from Indian financial institutions. *Economic Sciences, 22*, 141–151. https://doi.org/10.69889/78bf3q34

Gwagwa, A., Kachidza, P., & Owen, R. (2022). Algorithmic bias, automated lending, and socio-economic exclusion in Sub-Saharan Africa: Tracking the structural gaps. *Journal of African Law, 66*(1), 89–114. https://doi.org/10.1017/S002185532200015X

Isabirye, E., & Bitalo, D. N. (2025). Contextualizing AI ethics in Uganda through adaptive sensitive reweighting (ASR) for equitable microcredit. In *[Book title requires verification]*. Oxford University Press. https://doi.org/10.1093/9780198945215.003.0179

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence, 1*(9), 389–399. https://doi.org/10.1038/s42256-019-0088-2

Kasekende, L. (2022). Capital adequacy architectures and digital operational risks: A regional synthesis of central bank responses within the East African Community. *Journal of Financial Economic Policy, 14*(4), 412–435. https://doi.org/10.1108/JFEP-09-2021-0245

Khazratkulov, O. (2026). Priority of state policy for digitalization of financial services. *Uzbek Journal of Law and Digital Policy, 4*(1), 58–73. https://doi.org/10.59022/ujldp.526

Köbis, N., Rahwan, Z., Rilla, R., Supriyatno, B. I., Bersch, C., Ajaj, T., Bonnefon, J., & Rahwan, I. (2025). Delegation to artificial intelligence can increase dishonest behaviour. *Nature, 646*(8083), 126–134. https://doi.org/10.1038/s41586-025-09505-x

Kour, M. (2023). Challenges and opportunities of machine learning in the financial sector. In *Advances in finance, accounting, and economics* (pp. 61–73). IGI Global. https://doi.org/10.4018/979-8-3693-1746-4.ch004

Kruse, L., Wunderlich, N., & Beck, R. (2019). Artificial intelligence for the financial services industry: What challenges organizations to succeed. In *Proceedings of the 52nd Hawaii International Conference on System Sciences* (pp. 5295–5304). https://doi.org/10.24251/HICSS.2019.770

Kshetri, N. (2021). Evolving uses of artificial intelligence in human resource management in emerging economies in the Global South: Some preliminary evidence. *Management Research Review, 44*(7), 970–990. https://doi.org/10.1108/MRR-03-2020-0168

Kulkov, I., Kulkova, J., Rohrbeck, R., Menvielle, L., Kaartemo, V., & Makkonen, H. (2024). Artificial intelligence-driven sustainable development: Examining organizational, technical, and processing approaches to achieving global goals. *Sustainable Development, 32*(3), 2253–2267. https://doi.org/10.1002/sd.2773

Lawani, A. (2021). Critical realism: What you should know and how to apply it. *Qualitative Research Journal, 21*(3), 320–333. https://doi.org/10.1108/QRJ-08-2020-0101

Van Liebergen, B. (2017). Machine learning: A revolution in risk management and compliance? *Journal of Financial Transformation, 45*, 60–67.

Lieberman, M. B., & Asaba, S. (2006). Why do firms imitate each other? *Academy of Management Review, 31*(2), 366–385. https://doi.org/10.5465/AMR.2006.20208686

Lund, E., Johansson, J., & Lööw, J. (2024). The designers' perspective on autonomous mining systems and sociotechnology. *Mining, Metallurgy & Exploration, 41*(2), 647–657. https://doi.org/10.1007/s42461-024-00952-0

Magnuson, W. (2020). Financial regulation in the age of artificial intelligence. *Vanderbilt Law Review, 73*(4), 1159–1204.

Malterud, K., Siersma, V. D., & Guassora, A. D. (2016). Sample size in qualitative interview studies: Guided by information power. *Qualitative Health Research, 26*(13), 1753–1760. https://doi.org/10.1177/1049732315617444

Mazzini, G., & Bagni, F. (2023). Considerations on the regulation of AI systems in the financial sector by the AI Act. *Frontiers in Artificial Intelligence, 6*, Article 1277544. https://doi.org/10.3389/frai.2023.1277544

Nanziri, E. L. (2022). Financial inclusion, digital footprints, and macroprudential stress-testing post-COVID-19: Empirical insights from Ugandan commercial banks. *Journal of Development Economics, 158*, Article 102912. https://doi.org/10.1016/j.jdeveco.2022.102912

Nwachukwu, P. S., Chima, O. K., & Okolo, C. H. (2025). The artificial intelligence governance framework for finance: A control-by-design approach to algorithmic decision-making in accounting. *Finance & Accounting Research Journal, 7*(8), 350–379. https://doi.org/10.51594/farj.v7i8.2016

Nzeako, G., Akinsanya, M. O., Popoola, O. A., Chukwurah, E. G., Okeke, C. D., & Akpukorji, I. S. (2024). Theoretical insights into IT governance and compliance in banking: Perspectives from African and U.S. regulatory environments. *International Journal of Management & Entrepreneurship Research, 6*(5), 1457–1466. https://doi.org/10.51594/ijmer.v6i5.1094

Okello, J. (2025). *Ethics and governance in African AI: A comparative study in Uganda*. Zenodo. https://doi.org/10.5281/zenodo.18993512

Olabanji, S. O., Oladoyinbo, O. B., Asonze, C. U., Oladoyinbo, T. O., Ajayi, S. A., & Olaniyi, O. O. (2024). Effect of adopting AI to explore big data on personally identifiable information (PII) for financial and economic data transformation. *Asian Journal of Economics, Business and Accounting, 24*(4), 106–125. https://doi.org/10.9734/ajeba/2024/v24i41268

O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown.

Oosthuizen, R. M. (2022). The Fourth Industrial Revolution—Smart technology, artificial intelligence, robotics and algorithms: Industrial psychologists in future workplaces. *Frontiers in Artificial Intelligence, 5*, Article 913168. https://doi.org/10.3389/frai.2022.913168

Opesemowo, O. A. G., & Adekomaya, V. (2024). Harnessing artificial intelligence for advancing sustainable development goals in South Africa's higher education system: A qualitative study. *International Journal of Learning, Teaching and Educational Research, 23*(3), 67–86. https://doi.org/10.26803/ijlter.23.3.4

Oriji, O., Shonibare, M. A., Daraojimba, R. E., Abitoye, O., & Daraojimba, C. (2023). Financial technology evolution in Africa: A comprehensive review of legal frameworks and implications for AI-driven financial services. *International Journal of Management & Entrepreneurship Research, 5*(12), 929–951. https://doi.org/10.51594/ijmer.v5i12.627

Osasona, F., Amoo, O. O., Atadoga, A., Abrahams, T. O., Farayola, O. A., & Ayinla, B. S. (2024). Reviewing the ethical implications of AI in decision making processes. *International Journal of Management & Entrepreneurship Research, 6*(2), 322–335. https://doi.org/10.51594/ijmer.v6i2.773

Oyeyemi, A. (2025). *Bridging AI governance and financial regulation*. Zenodo. https://doi.org/10.5281/zenodo.17836814

Pantserev, K. (2022). Malicious use of artificial intelligence in Sub-Saharan Africa: Challenges for Pan-African cybersecurity. *Vestnik RUDN. International Relations, 22*(2), 288–302. https://doi.org/10.22363/2313-0660-2022-22-2-288-302

Papagiannidis, E., Enholm, I. M., Dremel, C., Mikalef, P., & Krogstie, J. (2023). Toward AI governance: Identifying best practices and potential barriers and outcomes. *Information Systems Frontiers, 25*(1), 123–141. https://doi.org/10.1007/s10796-022-10251-y

Papagiannidis, E., Mikalef, P., & Conboy, K. (2025). Responsible artificial intelligence governance: A review and research framework. *The Journal of Strategic Information Systems, 34*(2), Article 101885. https://doi.org/10.1016/j.jsis.2024.101885

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

Pervez, M. M., Ullah, M. Q. A., Khan, I. A., Rahat, R., Zaffar, M. F., Tahir, R., Rahwan, T., & Zaki, Y. (2026). *(Mis-)Informed consent: Predatory apps and the exploitation of populations with limited literacy*. *arXiv*. https://doi.org/10.48550/arXiv.2601.17025

Rabbani, H., Shahid, M. F., Khanzada, T. J. S., Siddiqui, S., Jamjoom, M., Ashari, R. B., Ullah, Z., Mukati, M. U., & Nooruddin, M. (2024). Enhancing security in financial transactions: A novel blockchain-based federated learning framework for detecting counterfeit data in fintech. *PeerJ Computer Science, 10*, e2280. https://doi.org/10.7717/peerj-cs.2280

Raso, F., Hilligoss, H., Krishnamurthy, V., Bavitz, C., & Kim, L. (2018). *Artificial intelligence and human rights: Opportunities and risks*. Berkman Klein Center for Internet & Society Research Publication. https://doi.org/10.2139/ssrn.3256343

Board of Governors of the Federal Reserve System. (2011). *Supervisory guidance on model risk management (SR Letter 11-7)*. Board of Governors of the Federal Reserve System.

Ridzuan, N. N., Masri, M., Anshari, M., Fitriyani, N. L., & Syafrudin, M. (2024). AI in the financial sector: The line between innovation, regulation and ethical responsibility. *Information, 15*(8), Article 432. https://doi.org/10.3390/info15080432

Roche, C., Wall, P. J., & Lewis, D. (2023). Ethics and diversity in artificial intelligence policies, strategies and initiatives. *AI and Ethics, 3*(4), 1095–1115. https://doi.org/10.1007/s43681-022-00218-9

Sætra, H. S. (2021). AI in context and the Sustainable Development Goals: Factoring in the unsustainability of the sociotechnical system. *Sustainability, 13*(4), Article 1738. https://doi.org/10.3390/su13041738

Shajek, A., & Hartmann, E. (2023). *New digital work*. Springer. https://doi.org/10.1007/978-3-031-26490-0

Sharma, M., Luthra, S., Joshi, S. K., & Kumar, A. (2022). Implementing challenges of artificial intelligence: Evidence from the public manufacturing sector of an emerging economy. *Government Information Quarterly, 39*(4), Article 101624. https://doi.org/10.1016/j.giq.2021.101624

Shetty, M. D., & Bhat, S. (2024). Basel norms compliance in Indian banks. *International Journal of Management, Technology, and Social Sciences, 9*(1), 238–249. https://doi.org/10.47992/IJMTS.2581.6012.0354

Singh, A., Kanaujia, A., Singh, V. K., & Vinuesa, R. (2024). Artificial intelligence for Sustainable Development Goals: Bibliometric patterns and concept evolution trajectories. *Sustainable Development, 32*(1), 724–754. https://doi.org/10.1002/sd.2706

Singh, S. K., Bandyopadhyay, P., & Mishra, A. (2025). The role of artificial intelligence in enhancing compliance in banks. *EPRA International Journal of Environmental Economics, Commerce and Educational Management*, 141–148. https://doi.org/10.36713/EPRA23782

Somu, B. (2025). Balancing innovation with compliance: Governance, risk management, and security in artificial intelligence-augmented banking infrastructure. In *[Book title requires verification]* (pp. 80–92). https://doi.org/10.70593/978-93-49910-62-1_7

Spears, T., Hansen, K. B., Xu, R., & Millo, Y. (2025). Governing synthetic data in the financial sector. *Finance and Society*, 1–17. https://doi.org/10.1017/fas.2025.10017

Srinadi, N. L. P. (2023). Advancement of banking and financial services employing artificial intelligence and the Internet of Things. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 14*(1), 106–117. https://doi.org/10.58346/JOWUA.2023.I1.009

Ssekiziyivu, B. (2023). Regulatory cross-currents in Uganda's financial sector: Intersecting Bank of Uganda prudential guidelines and the NITA-U data privacy framework. *Uganda Journal of Management and Compliance, 9*(2), 112–134.

Stahl, B. C., Schroeder, D., & Rodrigues, R. (2022). *Ethics of artificial intelligence*. Springer. https://doi.org/10.1007/978-3-031-17040-9

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

Thoom, S. R. (2025). Lessons from AI in finance: Governance and compliance in practice. *International Journal of Science and Research Archive, 14*(1), 1387–1395. https://doi.org/10.30574/ijsra.2025.14.1.0235

Timmons, A. C., Duong, J. B., Fiallo, N. S., Lee, T., Vo, H. P. Q., Ahle, M. W., Comer, J. S., Brewer, L. C., Frazier, S. L., & Chaspari, T. (2023). A call to action on assessing and mitigating bias in artificial intelligence applications for mental health. *Perspectives on Psychological Science, 18*(5), 1062–1096. https://doi.org/10.1177/17456916221134490

Torrance, H. (2012). Triangulation, respondent validation, and democratic participation in mixed methods research. *Journal of Mixed Methods Research, 6*(2), 111–123. https://doi.org/10.1177/1558689812437185

Trist, E. L., & Bamforth, K. W. (1951). Some social and psychological consequences of the longwall method of coal-getting. *Human Relations, 4*(1), 3–38. https://doi.org/10.1177/001872675100400101

Truby, J. (2020). Governing artificial intelligence to benefit the UN Sustainable Development Goals. *Sustainable Development, 28*(4), 946–959. https://doi.org/10.1002/sd.2048

Truby, J., Brown, R. D., & Dahdal, A. (2020). Banking on AI: Mandating a proactive approach to AI regulation in the financial sector. *Law and Financial Markets Review, 14*(2), 110–120. https://doi.org/10.1080/17521440.2020.1760454

European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L 119*, 1–88.

Vinuesa, R., Azizpour, H., Leite, I., Balaam, M., Dignum, V., Domisch, S., Felländer, A., Langhans, S. D., Tegmark, M., & Nerini, F. F. (2020). The role of artificial intelligence in achieving the Sustainable Development Goals. *Nature Communications, 11*(1), Article 233. https://doi.org/10.1038/s41467-019-14108-y

Yaramolu, L. S. K. G. (2025). Architecting AI-driven microfinance platforms: Reimagining credit access for global financial inclusion. *European Journal of Computer Science and Information Technology, 13*(13), 23–38. https://doi.org/10.37745/ejcsit.2013/vol13n132338

Zetzsche, D. A., Buckley, R. P., & Arner, D. W. (2021). Regulating AI and machine learning in finance: The frontiers of data protection, systemic risk, and accountability. *European Business Organization Law Review, 22*(1), 5–42. https://doi.org/10.1007/s40821-020-00152-x