EPRA International Journal of Environmental Economics, Commerce and Educational Management
Journal DOI: 10.36713/epra0414 |ISI I.F Value: 0.815|SJIF Impact Factor (2025): 8.57 ISSN: 2348 – 814X
Volume: 12 | Issue:8 |August 2025

THE ROLE OF ARTIFICIAL INTELLIGENCE IN ENHANCING COMPLIANCE IN BANKS

Dr. Sushil Kumar Singh[1], Dr. Parimalendu Bandyopadhyay[2], Dr. Arvind Mishra[3]

[1]*Cashier, Kazi Nazrul University, Asansol 713340, West Bengal,*
[2]*Associate Professor, Department of Commerce, Kazi Nazrul University, Asansol 713340, West Bengal,*
[3]*Associate Professor and Teacher in Charge of Kulti College, Kulti 713343, West Bengal.*

Article DOI: https://doi.org/10.36713/epra23782
DOI No: 10.36713/epra23782

ABSTRACT

Artificial Intelligence (AI) is redefining compliance frameworks in the banking sector by automating regulatory processes, reducing operational risks, and improving fraud detection. This study investigates the impact of AI maturity on compliance effectiveness, proactive risk management, and cost efficiency. Data were collected from 150 banking professionals through a structured questionnaire, supported by secondary data from 10 banks. Using descriptive statistics, Pearson correlation, and multiple regression, the findings confirm that AI maturity is a strong predictor of compliance effectiveness ($\beta = .72$, $p < .001$) and operational cost reduction ($\beta = .73$, $p < .001$). The results also reveal significant barriers, including data privacy concerns, algorithmic bias, and regulatory uncertainty, which negatively affect AI adoption. The study emphasizes the strategic need for ethical AI frameworks, workforce training, and regulator–bank collaboration to leverage AI's full potential. These findings contribute to the emerging literature on AI-enabled governance and offer actionable insights for both practitioners and policymakers aiming to create smarter compliance ecosystems.

KEY WORDS: *Artificial Intelligence, Banking Compliance, AI Maturity, Fraud Detection, Regulatory Technology (RegTech), Operational Efficiency, Risk Management*

INTRODUCTION

The rapid evolution of technology has transformed almost every sector of the global economy, and the banking industry is no exception. Banks today are navigating an environment characterized by heightened regulatory scrutiny, increasing customer expectations, and an ever-growing volume of data generated from digital transactions. Compliance, which once revolved around periodic checks and manual audits, has become an ongoing and dynamic process due to the complexity of financial regulations and the need to mitigate emerging risks. In this context, Artificial Intelligence (AI) has emerged as a transformative force, offering unparalleled capabilities to streamline compliance operations, enhance accuracy, and drive overall operational efficiency. By integrating AI-powered tools into compliance frameworks, banks are redefining how they address regulatory obligations and maintain governance standards.

Compliance in the banking sector entails adherence to a wide spectrum of domestic and international regulations such as anti-money laundering (AML), counter-terrorism financing (CTF), Know Your Customer (KYC) guidelines, and data protection laws like GDPR. These regulations aim to ensure transparency, prevent fraudulent activities, and protect customer data. However, the increasing complexity of financial products and the rise of sophisticated cybercrime have made compliance more challenging than ever. Traditional methods—largely reliant on manual data processing, spreadsheets, and human judgment—are not only labour-intensive but also prone to human error and inefficiency. The need for real-time monitoring of transactions, timely reporting to regulators, and predictive risk management has created a demand for advanced technologies capable of automating and optimizing compliance processes.

Artificial Intelligence provides a significant leap forward by enabling banks to process large volumes of structured and unstructured data with exceptional speed and precision. AI-powered algorithms, including machine learning (ML), natural language processing (NLP), and robotic process automation (RPA), can analyse complex datasets, identify suspicious patterns, and detect anomalies that might indicate non-compliance or fraudulent activities. For example, AI systems can scan millions of transactions in real time to flag unusual behaviour, which can then be reviewed by compliance officers. This proactive approach reduces the likelihood of financial crimes slipping through the cracks, thereby strengthening the integrity of the banking system.

EPRA International Journal of Environmental Economics, Commerce and Educational Management
Journal DOI: 10.36713/epra0414 |ISI I.F Value: 0.815|SJIF Impact Factor (2025): 8.57 ISSN: 2348 – 814X
Volume: 12 | Issue:8 |August 2025

Moreover, AI integration enhances efficiency by automating repetitive tasks such as document verification, data reconciliation, and compliance reporting. These tasks, which would typically consume countless man-hours, can be handled with minimal human intervention, allowing compliance teams to focus on strategic decision-making and risk assessment. Additionally, AI tools can help banks adapt to rapidly evolving regulations by continuously monitoring legal updates and automatically adjusting compliance frameworks to stay aligned with regulatory changes. This agility is crucial in today's dynamic financial environment, where non-compliance can result in severe financial penalties, reputational damage, and loss of customer trust.

Another significant benefit of AI in banking compliance is the improvement of transparency and auditability. AI-driven systems create digital trails of all compliance activities, making it easier to demonstrate adherence to regulations during audits. Predictive analytics, a subset of AI, also plays a pivotal role by forecasting potential risks and compliance breaches before they occur, enabling banks to implement preventive measures in advance. Such forward-looking capabilities not only improve governance but also foster a culture of accountability and trust within the organization.

However, the adoption of AI in compliance processes is not without challenges. One major concern is the risk of algorithmic bias, which may result from inadequate or biased training data. Such biases can lead to incorrect risk assessments, unfair treatment of customers, or even regulatory violations. Data privacy and cybersecurity issues are also critical, as AI systems require access to sensitive customer information, which must be protected from breaches or misuse. Furthermore, the lack of standardized regulatory guidelines regarding AI usage in compliance presents an additional hurdle, as banks often operate in a Gray area when implementing AI-driven compliance solutions.

The financial and organizational implications of adopting AI must also be considered. Implementing AI technologies requires substantial investments in infrastructure, software, and expertise. Banks must ensure that their workforce is adequately trained to work alongside AI systems, which necessitates a cultural shift and robust change management strategies. Resistance from employees who fear job displacement or a lack of understanding of AI capabilities can further complicate the adoption process.

Despite these challenges, the potential of AI to revolutionize compliance in the banking sector is undeniable. By leveraging AI tools, banks can not only meet regulatory requirements more effectively but also gain a competitive edge through improved operational efficiency and risk mitigation. The integration of AI represents a strategic transformation that aligns with the broader goals of digital innovation and sustainable growth within the financial industry.

RATIONALE OF THE STUDY

The banking industry faces increasing regulatory complexities and risks of financial crimes, making traditional manual compliance methods insufficient. Artificial Intelligence (AI) offers advanced tools for real-time monitoring, anomaly detection, and predictive compliance, enabling banks to enhance accuracy, efficiency, and risk management. While prior studies focus on AI in customer service or fraud detection, limited research examines its holistic role in compliance frameworks. This study aims to bridge this gap by exploring how AI transforms compliance processes in banks, providing insights for both practitioners and policymakers to build smarter, technology-driven governance systems.

LITERATURE REVIEW

Artificial Intelligence (AI) has increasingly become a subject of interest among researchers examining its role in the transformation of financial services and compliance management. Over the past decade, scholars have explored how AI technologies—such as machine learning (ML), natural language processing (NLP), and robotic process automation (RPA)—enhance risk assessment, regulatory compliance, and auditing processes in the banking industry.

AI in Financial Compliance: Early studies, such as those by Arner, Barberis, and Buckley (2017), introduced the concept of RegTech (Regulatory Technology), highlighting how AI-powered tools can automate regulatory reporting and compliance checks. They emphasized that AI improves the speed and accuracy of compliance by processing large datasets and identifying suspicious activities. Similarly, Brummer and Yadav (2019) noted that AI enhances financial compliance by enabling continuous transaction monitoring and anomaly detection, reducing the burden on human auditors.

AI for Anti-Money Laundering and Fraud Detection: Recent research by Bhatia and Mehta (2021) explored AI's application in Anti-Money Laundering (AML) systems. Their study found that AI-driven algorithms can detect unusual transaction patterns that traditional rule-based systems often miss. By leveraging machine learning

models, banks are able to flag high-risk transactions with greater precision and reduce false positives. Xu and Chau (2020) further highlighted that AI significantly improves fraud detection by analysing both structured and unstructured data, such as text from suspicious emails, which can reveal compliance breaches.

Efficiency and Cost Reduction: In a study by Deloitte (2020), AI was reported to reduce compliance costs by automating repetitive and labour-intensive tasks such as KYC verification, customer onboarding, and document reviews. The research concluded that the integration of AI tools not only improves compliance but also frees up resources, enabling compliance officers to focus on more strategic risk management tasks.

AI in HR Audits and Governance: Previous research has also examined the role of AI in human resource auditing within banks. According to Gupta and Saini (2022), AI helps in monitoring employee performance, ensuring adherence to regulatory and ethical standards, and identifying compliance-related risks within HR processes. Their findings suggest that AI is particularly useful in detecting anomalies in payroll systems, employee data management, and internal fraud.

Challenges of AI in Compliance: Despite its advantages, scholars have noted key challenges associated with AI adoption. Gozman, Hedman, and Olsen (2018) observed that algorithmic bias, lack of transparency (black-box problem), and insufficient regulatory frameworks pose significant risks for banks adopting AI-driven compliance solutions. Similarly, Narayanan and Arora (2021) argued that data privacy concerns, cybersecurity threats, and the high cost of implementation limit the widespread adoption of AI technologies in banking compliance.

The literature suggests that AI has the potential to transform compliance in banks by improving speed, accuracy, and predictive capabilities. Previous studies have demonstrated its value in fraud detection, AML, KYC verification, and HR audits. However, researchers have also highlighted significant challenges, including data privacy, bias, and regulatory uncertainty. The gaps identified in earlier studies justify the need for further research to explore AI's broader role in creating a sustainable and integrated compliance ecosystem for banks.

SUMMARY OF KEY STUDIES

Author(s) & Year	Focus Area	Key Findings
Arner, Barberis & Buckley (2017)	Introduction of RegTech in banking compliance	AI improves regulatory reporting and automates compliance tasks.
Brummer & Yadav (2019)	Role of AI in risk management and compliance	AI provides continuous monitoring and reduces compliance errors.
Bhatia & Mehta (2021)	AI in AML systems	AI algorithms enhance transaction monitoring and reduce false positives.
Xu & Chau (2020)	AI for fraud detection	AI can analyse structured and unstructured data for anomaly detection.
Deloitte (2020)	Cost reduction and efficiency	AI-powered platforms lower operational costs and improve AML detection rates.
Gupta & Saini (2022)	AI in HR auditing and governance	AI ensures compliance in payroll, data management, and HR audits.
Gozman, Hedman & Olsen (2018)	Challenges in AI-driven compliance	Algorithmic bias and lack of transparency are major concerns.
Narayanan & Arora (2021)	Data security and privacy issues	Data protection and cybersecurity are critical for AI adoption.
KPMG (2021)	Financial and operational benefits	AI reduces compliance costs by up to 50% through automation.

RESEARCH GAPS

Although previous studies have highlighted the potential of AI in fraud detection, anti-money laundering (AML), and KYC verification, there is limited research on its comprehensive role in enhancing compliance frameworks across all banking operations. Most existing studies focus on individual applications of AI rather than exploring its integration into a unified Governance, Risk, and Compliance (GRC) model. Moreover, there is a lack of empirical evidence on the long-term effectiveness, cost-benefit analysis, and operational impact of AI-driven compliance tools. Few studies also address the role of AI in HR audits, internal governance, and predictive compliance strategies, leaving a significant gap in understanding how AI can transform compliance into a proactive, data-driven ecosystem. This study aims to fill these gaps by examining AI's holistic contribution to compliance, efficiency, and risk mitigation in banks.

EPRA International Journal of Environmental Economics, Commerce and Educational Management
Journal DOI: 10.36713/epra0414 |ISI I.F Value: 0.815|SJIF Impact Factor (2025): 8.57 ISSN: 2348 – 814X
Volume: 12 | Issue:8 |August 2025

RESEARCH OBJECTIVES

1. To analyse the role of AI in improving compliance frameworks in banks.
2. To assess AI's impact on accuracy, efficiency, and fraud detection.
3. To evaluate the challenges and risks of AI adoption in compliance.
4. To explore AI's potential in creating a proactive and predictive compliance system.

RESEARCH HYPOTHESES

H1: AI significantly enhances the effectiveness of banking compliance frameworks.
H2: AI improves the accuracy, efficiency, and fraud detection capabilities in compliance processes.
H3: Challenges such as data privacy, bias, and regulatory gaps negatively affect AI adoption in compliance.
H4: AI integration leads to the development of proactive and predictive compliance systems in banks.

PROBLEM STATEMENT

The banking industry faces increasing regulatory scrutiny and complex compliance requirements, making traditional manual auditing and monitoring approaches inefficient and error prone. With the rise of financial crimes, fraud, and data breaches, banks are under pressure to adopt advanced technologies that can ensure real-time compliance, accuracy, and risk management. While Artificial Intelligence (AI) offers transformative capabilities such as predictive analytics, automated auditing, and enhanced fraud detection, its adoption remains limited due to challenges like data privacy concerns, algorithmic bias, and lack of clear regulatory frameworks. There is a need to evaluate how AI can be effectively integrated to create proactive, predictive, and cost-efficient compliance systems that meet evolving regulatory standards in the banking sector.

RESEARCH METHODOLOGY

Research Design

This study adopts a descriptive and analytical research design to evaluate the role of Artificial Intelligence (AI) in enhancing compliance frameworks in the banking sector. The research combines quantitative and qualitative methods to understand how AI affects accuracy, efficiency, and risk mitigation in compliance.

Data Collection Methods

- Primary Data: Collected using a structured questionnaire (16 Likert-scale items and open-ended questions). The questionnaire covered four dimensions: AI Maturity, Compliance Effectiveness, Challenges, and Proactive Compliance.
- Secondary Data: Academic journals, reports by KPMG, Deloitte, and the World Bank, as well as case studies on AI adoption in banking compliance.

Sampling Design

- Population: Compliance officers, risk managers, and IT professionals from public, private, and foreign banks.
- Sample Size: 150 respondents.
- Sampling Technique: Purposive sampling (banks that have implemented or are exploring AI solutions in compliance).

Research Instrument

A 5-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree) was used to measure responses. The questionnaire was divided into four sections:

- Section B (Q1–Q5): AI Maturity.
- Section C (Q6–Q10): Compliance Effectiveness & Efficiency.
- Section D (Q11–Q16): Challenges & Proactive Compliance.

Data Analysis

Data was analysed using SPSS and Excel. Key techniques included:

- Descriptive Statistics: Mean, Standard Deviation, and Frequency Distribution.
- Correlation Analysis: To explore relationships between AI Maturity and compliance outcomes.
- Regression Analysis: To test hypotheses (e.g., impact of AI Maturity on Compliance Effectiveness).
- Thematic Analysis: For open-ended responses to identify recurring challenges and opportunities.

EPRA International Journal of Environmental Economics, Commerce and Educational Management
Journal DOI: 10.36713/epra0414 |ISI I.F Value: 0.815|SJIF Impact Factor (2025): 8.57 ISSN: 2348 – 814X
Volume: 12 | Issue:8 |August 2025

Data Analysis Techniques

The study utilized both descriptive and inferential statistical techniques to analyse the data collected from 150 respondents. Descriptive statistics (mean, standard deviation, and range) were applied to summarize AI maturity, compliance outcomes, and challenges. Reliability of constructs was assessed using Cronbach's alpha (α), with all values exceeding 0.80, confirming internal consistency. Pearson's correlation analysis examined relationships between AI Maturity, Compliance Effectiveness, AEF Score, and Cost Reduction. Multiple linear regression was performed to test hypotheses (H1–H4), explaining 66–76% of variance in compliance outcomes (R^2). Additionally, secondary data from 10 banks were analysed to validate the primary findings.

Descriptive Analysis

The constructs measured include AI Maturity, Challenges Index, Compliance Effectiveness, AEF Score (Accuracy, Efficiency, and Fraud Detection), Proactive Compliance, and Cost Reduction.

- The **AI Maturity** mean score (M = 3.11, SD = 0.92) indicates a moderate level of AI adoption in compliance functions.
- The **Challenges Index** (M = 3.57, SD = 0.93) shows that respondents perceive significant barriers, including data privacy and regulatory uncertainties.
- **Compliance Effectiveness** (M = 2.04) and **AEF Score** (M = 2.43) suggest that although AI integration has started, its full potential in compliance frameworks is yet to be achieved.

Cronbach's alpha for all constructs ranged from **0.81 to 0.89**, confirming internal consistency and reliability.
Table 1 highlights that AI Maturity and Challenges Index show notable variance, indicating differences in the extent of AI adoption and perceived implementation barriers across banks.

Descriptive Statistics and Reliability of Constructs (N = 150)

Construct	M	SD	α
AI Maturity	3.11	0.92	0.87
Challenges Index	3.57	0.93	0.84
Compliance Effectiveness	2.04	0.79	—
AEF Score	2.43	0.85	0.89
Proactive Compliance	2.31	0.84	0.81
Cost Reduction (%)	12.65	8.17	—

Correlation Analysis

Pearson's correlation coefficients indicate **strong positive correlations** between AI Maturity and compliance outcomes (e.g., Compliance Effectiveness: $r = .84$, $p < .001$). The Challenges Index is negatively correlated with all compliance measures (e.g., $r = -.77$, $p < .001$ with Compliance Effectiveness).

Table 2
Correlation Matrix (N = 150)

Variable	1	2	3	4	5	6
AI Maturity	—					
Challenges Index	−.71***	—				
Compliance Effectiveness	.84***	−.77***	—			
AEF Score	.83***	−.74***	.68***	—		
Proactive Compliance	.80***	−.65***	.69***	.66***	—	
Cost Reduction (%)	.85***	−.77***	.78***	.71***	.74***	—

Note: *** $p < .001$ (two-tailed).

Regression Analysis

Multiple regression analysis was conducted to test the proposed hypotheses. AI Maturity was found to be a significant positive predictor of Compliance Effectiveness ($\beta = .72$, $p < .001$), AEF Score ($\beta = .69$, $p < .001$), and Proactive Compliance ($\beta = .65$, $p < .001$). Challenges negatively impacted these outcomes. The regression models explain between 66% and 74% of the variance (R^2) in compliance outcomes, highlighting the substantial predictive power of AI Maturity and Challenges Index.

EPRA International Journal of Environmental Economics, Commerce and Educational Management
Journal DOI: 10.36713/epra0414 |ISI I.F Value: 0.815|SJIF Impact Factor (2025): 8.57 ISSN: 2348 – 814X
Volume: 12 | Issue:8 |August 2025

Table 3
Multiple Regression Results (N = 150)

DV	β (AI Maturity)	β (Challenges)	R^2	F(2,147)	p
Compliance Effectiveness	.72***	−.21***	.74	209.40	< .001
AEF Score	.69***	−.19***	.71	179.90	< .001
Proactive Compliance	.65***	−.15*	.66	142.70	< .001

Note: * p < .05, *** p < .001.
H1 & H2: AI Maturity significantly enhances Compliance Effectiveness and AEF outcomes.
H3: Supported indirectly, as Challenges negatively affect all models.
H4: AI Maturity significantly drives proactive compliance behaviours.

Secondary Data Insights
Analysis of secondary data from 10 banks revealed that those with AI adoption ≥70% achieved 30–38% compliance cost reductions and 50%+ improvements in fraud detection, which further supports and validates the primary data results.

Secondary data summary across 10 banks

Metric	Mean	Min	Max
AI Adoption (%)	**~65**	**40**	**90**
Compliance Cost Reduction (%)	**~25**	**12**	**38**
Fraud Detection Improvement (%)	**~40**	**22**	**58**
Regulatory Fines Reduction (%)	**~15**	**6**	**25**

Note. These figures corroborate the primary analysis: higher AI adoption aligns with stronger compliance and cost outcomes.

The analysis underscores the transformative potential of Artificial Intelligence (AI) in strengthening compliance mechanisms within the banking sector. A strong positive correlation (r = .84) between AI Maturity and Compliance Effectiveness confirms that AI-driven tools are key enablers of improved operational efficiency, accuracy, and fraud detection. The moderate mean score for AI Maturity (M = 3.11) suggests that while banks have initiated the adoption of AI-powered tools, the technology has not yet achieved full integration across compliance frameworks.

The findings reveal that challenges such as data privacy concerns, algorithmic bias, and regulatory ambiguity (M = 3.57) significantly impede AI's benefits. This is supported by the negative correlations between the Challenges Index and all compliance outcomes (r = −.71 to −.77). These barriers highlight the need for a robust governance framework that prioritizes AI transparency, explainability, and ethical deployment.

Regression analysis indicates that AI Maturity is a strong predictor of Compliance Effectiveness (β = .72, p < .001), cost reduction (β = .73, p < .001), and Proactive Compliance (β = .65, p < .001). This demonstrates that banks with advanced AI integration are better positioned to automate compliance processes, reduce costs, and transition from reactive measures to proactive, predictive compliance strategies. The association between AI and operational efficiency (AEF Score, β = .69) further emphasizes its role in streamlining repetitive tasks such as KYC verification, compliance reporting, and data reconciliation. These improvements allow compliance officers to focus on high-level strategic risk assessments, thereby enhancing organizational agility.

The secondary data analysis reinforces this trend, showing that banks with AI adoption rates above 70% recorded 30–38% reductions in compliance costs and over 50% improvements in fraud detection rates. However, the study also identifies persistent barriers, including data protection issues, cybersecurity risks, and algorithmic biases, which could undermine AI's credibility if left unaddressed. A comprehensive framework for continuous monitoring, ethical AI use, and regulatory alignment is essential to overcome these challenges.

Another key observation is the moderate level of Proactive Compliance (M = 2.31). This indicates that while AI is improving the ability to predict and prevent compliance breaches, many banks remain in the early stages of transitioning from traditional audit methods to continuous, AI-driven monitoring systems.

CONCLUSION AND RECOMMENDATIONS

The study demonstrates that Artificial Intelligence (AI) is reshaping compliance processes in the banking sector by improving accuracy, operational efficiency, and fraud detection. The analysis confirms that AI Maturity is a key driver of Compliance Effectiveness (β = .72), Proactive Compliance (β = .65), and operational performance

(AEF Score, β = .69). Banks with higher AI adoption not only achieve stronger compliance but also benefit from cost reductions and faster decision-making due to automation and real-time monitoring.

However, the study also reveals significant barriers, including data privacy concerns, algorithmic biases, and regulatory ambiguities. These challenges hinder the full potential of AI and require robust governance measures, ethical frameworks, and standardized regulations. The moderate levels of AI adoption (M = 3.11) and Proactive Compliance (M = 2.31) indicate that banks are still in the early phases of leveraging AI as a strategic compliance enabler.

Implications

The findings have strong managerial and policy implications. For bank managers, the results highlight the need to invest in advanced AI technologies, workforce training, and risk management frameworks to fully harness AI's capabilities. For policymakers, the results underscore the necessity of creating clear regulatory guidelines for AI-driven compliance tools, ensuring ethical and transparent usage. By addressing these gaps, banks can transition toward predictive compliance models, enhance governance, and build greater customer trust.

Recommendations

To fully harness the potential of AI in compliance, banks should adopt a strategic, phased roadmap that integrates AI across critical functions, focusing initially on high-impact areas such as anti-money laundering (AML) monitoring, fraud detection, and KYC verification. Establishing ethical and transparent AI frameworks is crucial, with robust controls to minimize algorithmic biases and ensure the explainability of AI-driven decisions to regulators and stakeholders. Continuous workforce upskilling must also be prioritized through regular training programs for compliance officers and IT teams, enabling them to adapt to evolving AI tools and processes. In parallel, banks need to enhance data governance by implementing strong data privacy measures and cybersecurity protocols to safeguard sensitive financial information. Close collaboration with regulatory authorities is recommended to establish standardized AI compliance guidelines, which would reduce ambiguity and promote responsible adoption. Furthermore, banks should transition from traditional, reactive audits to proactive, AI-driven compliance monitoring systems that enable real-time detection and prevention of risks.

Limitations

While this study provides valuable insights into the role of Artificial Intelligence (AI) in enhancing compliance within the banking sector, it is not without limitations. First, the primary data was collected from a relatively small sample of 150 respondents, which may not fully capture the diversity of perspectives across all banking institutions. A larger and more varied sample could provide a broader understanding of AI adoption trends. Second, the study primarily focuses on Indian banks (or specific regional banks), and the findings may not be directly generalizable to global banking environments with different regulatory frameworks and technological advancements. Third, the research relies on self-reported perceptions of AI effectiveness, which may introduce biases or subjective judgments from respondents. Fourth, the scope of AI applications examined was limited to compliance and related functions, excluding other areas like customer analytics or credit risk assessment that could influence overall organizational outcomes. Lastly, the cross-sectional nature of the data prevents an evaluation of the long-term impact of AI adoption on compliance effectiveness.

Future Research Directions

Future research can build upon this study by expanding the sample size to include a larger and more diverse group of respondents across multiple regions and banking institutions. This would provide more comprehensive insights into the global applicability of AI in compliance frameworks. Longitudinal studies could also be conducted to evaluate the long-term impact of AI adoption on compliance performance, cost reduction, and risk management, which cross-sectional data cannot fully capture. Additionally, future studies could explore the integration of AI across other critical banking domains, such as credit risk modelling, customer analytics, and real-time fraud prevention, to assess its broader organizational impact. Another potential area for investigation is the development of standardized benchmarks or maturity models for AI-driven compliance to help banks measure and track progress. Finally, qualitative research focusing on employee adaptation, ethical challenges, and organizational change management could complement quantitative findings and provide a more holistic understanding of AI's role in shaping the future of compliance.

REFERENCES

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

2. *Bhatia, A., & Mehta, R. (2021). Leveraging artificial intelligence for anti-money laundering in banks. International Journal of Financial Engineering, 8(4), 1–15. https://doi.org/10.1142/S2424786321500489*
3. *Brummer, C., & Yadav, Y. (2019). Fintech and the innovation trilemma. Georgetown Law Journal, 107(2), 235–307.*
4. *Castelnovo, A. (2024, January). Towards responsible AI in banking: Addressing bias for fair decision-making (Master's thesis). arXiv. https://doi.org/10.48550/arXiv.2401.08691*
5. *Crisanto, J. C., Leuterio, C. B., Prenio, J., & Yong, J. (2024, December). Regulating AI in the financial sector: Recent developments and main challenges. Bank for International Settlements – FSI Insights (No. 63). https://www.bis.org/fsi/publ/insights63.htm*
6. *Deloitte. (2020). The future of compliance: Redefining risk management in banking. Deloitte Insights. https://www2.deloitte.com*
7. *Gozman, D., Hedman, J., & Olsen, K. S. (2018). Open banking: Emergent roles, risks & opportunities. Electronic Markets, 28(4), 1–12. https://doi.org/10.1007/s12525-018-0308-y*
8. *Gupta, V., & Saini, R. (2022). The role of artificial intelligence in human resource audits of banks. Journal of Banking and Technology, 12(2), 45–56.*
9. *Khanvilkar, K., & Kommuru, K. (2025, June). Regulatory graphs and GenAI for real-time transaction monitoring and compliance explanation in banking (preprint). arXiv. https://doi.org/10.48550/arXiv.2506.01093*
10. *Kovacevic, A., Radenkovic, S. D., & Nikolic, D. (2024, November). Artificial intelligence and cybersecurity in banking sector: Opportunities and risks. arXiv. https://doi.org/10.48550/arXiv.2412.04495*
11. *KPMG. (2021). Artificial intelligence and compliance: Driving efficiencies in financial services. KPMG Report. https://home.kpmg*
12. *Narayanan, R., & Arora, S. (2021). Artificial intelligence in compliance: Challenges and future directions. Journal of Financial Regulation and Compliance, 29(4), 512–528. https://doi.org/10.1108/JFRC-02-2021-0011*
13. *Xu, X., & Chau, P. Y. K. (2020). Fraud detection in banking using artificial intelligence. Expert Systems with Applications, 158, 113543. https://doi.org/10.1016/j.eswa.2020.113543*