Acta Universitatis Danubius
ŒCONOMICA

Third-Party Reliance in the Financial Sector: Opportunities and Challenges in Mitigating Money Laundering Risks

William Gaviyau[1]

Abstract: Background: Modern financial institutions offer integrated banking services than traditional financial institutions. Historically, the banking sector has relied on outsourced third parties' services to offer banking services. Prior studies indicate a growing reliance on third parties to provide banking services in an integrated banking environment. However, contracting third parties brings associated benefits and risks. **Objectives:** This study examined the challenges and opportunities in mitigating money laundering risks by placing reliance on third parties as espoused by FATF recommendation 17. **Approach:** The study adopted a review of secondary sources which enabled deeper understanding of third parties role in financial sector. **Results:** The study identified opportunities which contribute to mitigating money laundering risks and contributing to sector's integrity while challenges promote money laundering. **Contributions:** The results underscore the necessity for a balanced regulatory approach to outsourcing services in a digitally driven environment. Also, policymakers must customize Financial Action Task Force recommendations in support of global efforts of money laundering, thereby ensuring that third parties comply with related regulations. By synthesizing current knowledge, this review provides a foundation for future research and offers insights for regulators, financial institutions, and policymakers seeking to optimise third-party reliance while mitigating money laundering risks.

Keywords: Third-party reliance; AML/CFT; money laundering; financial sector; customer due diligence

[1] Post Doctoral Fellow, Ph.D., Department of Finance, Risk Management and Banking, University of South Africa, Pretoria, South Africa, Address: Preller Street, Muckleneuk Ridge, Pretoria, South Africa, Corresponding author: gaviyw@unisa.ac.za.

JEL Classification: E58, G21, G23, G28

1. Introduction

Financial institutions operate in a highly regulated environment with the overarching goal of maintaining and enhancing financial stability. The dynamic operating environment and integration of services prompted by financial innovations exposes the financial services sector and greater economy to risks. The risks include but are not limited to operational, compliance, transactional, and information security risk (Gandawa, 2026; Rasner, 2021). Moreover, they must comply with sector specific regulations among others such as minimum capital requirements, consumer protection, and anti-money laundering (Kolo, Sunday, Akinde, Valerie & Seun, 2025; Restoy, 2021). Thus, regulators face a regulatory coherence dilemma of encouraging innovation and financial inclusion while promoting competition, maintaining financial integrity and protecting consumers.

Within the regulated environment, financial institutions and fintech compete for the same customers. Importantly, a mismatch between financial institutions and fintech businesses exists. Although financial institutions are required to comply with specified regulations, fintech startups are obliged to follow legislation pertinent to certain activities resulting in regulation arbitrages and blind spots. Consequently, modern financial institutions offer integrated banking services efficiently and at a cheaper cost than traditional financial institutions who are less inclined to innovate due to legacy issues (Nyreröd, Andreadakis & Spagnolo, 2023; Restoy, 2021).

Historically, the banking sector has relied on outsourced third parties' services to offer banking services to banking customers. However, third parties financial regulatory breaches have affected the financial sector negatively. For instance, a data breach was recorded in 2019 by a United States of America (USA) financial services-based company, Capital One which specialized in offering credit cards and related banking services. The breach was due to a misconfigured web application firewall hosted by the third party, Amazon Web Services (AWS) which allowed unauthorized access to personal information from over 100 million accounts (Balogun, Olaniyi & Alao, 2025; Khan, Kabanov, Hua & Madnick, 2022). The incident revealed weak third-party information risk management controls due to cloud infrastructure misconfigurations and associated systematic operational gaps. Another incident, Kabir and Hosen (2024) observed the 2016 Bangladesh Bank heist utilized

fraudulent SWIFT transactions, resulting in a USD81 million theft. The heist exposed weak authentication and internal controls of the bank. This event highlighted the prerequisites for critical third-party infrastructures such as multilayer security with real-time monitoring and oversight.

These two significant cybersecurity breaches involving third-party contractors highlight perennial risk governance issues in financial institutions. Accordingly, these occurrences emphasize the importance of proactive third-party risk management frameworks such as vendor oversight, configuration management, and mitigation measures. In line with Financial Action Task Force (FATF) recommendation 17, extreme caution should be exercised when integrating third parties technologies with banking functions. FATF recommendations are universally acceptable guiding AML/CFT standards in the regulatory design to counter money laundering and the risks of financing terrorism (FATF, 2025).

In terms of prior studies on contracting third parties, firstly Sultan, Mohamed, Chisunga and Satar (2025) examined and evaluated the challenges related to rationality and applicability of customer due diligence (FATF recommendation 10), emerging technologies (FATF recommendation 15), and the involvement of third parties (FATF recommendation 17) in the global South, with a particular focus on Pakistan. They revealed that FATF recommendation 17 is rarely discussed and restricts application of fintechs in modern banking. Secondly, Kolo et al. (2025) discovered that third-party software vulnerabilities and vendor credential theft were leading in terms of financial sector breaches. Thirdly, Black (2024) revealed that within the financial sector regulatory system in United Kingdom (UK), third parties play a multifaceted role which can either be beneficial or brings associated risks. Finally, Feng (2021) highlighted that in China, technological innovations have forced the transfer of payment and settlement services from commercial banks to third party payment service providers.

The prior studies indicate a growing reliance on third parties to provide banking services in an integrated banking environment. Country evidence from China, Pakistan and UK gave insights on the subject. Also, most of the studies (Kolo et al., 2025; Black, 2024; Feng, 2021) generalize the subject of third-party service providers apart from Sultan et al. (2025) who incorporated FATF recommendations. Therefore, this study intends to provide an examination of the challenges and opportunities in mitigating money laundering risks by placing reliance on third parties as espoused by FATF recommendation 17. Furthermore, the novel study

contributes to policy and practice on third party issues related to money laundering and financing of terrorism.

2. Methodology

The study aimed to examine the challenges and opportunities in mitigating money laundering risks by placing reliance on third parties as espoused by FATF recommendation 17. Additionally, the study's contribution being to influence policy discussion and practice in the financial service sector, the study adopted a qualitative based study. This approach enabled the gathering of the relevant information from secondary data sources by examining non-numerical data and discover patterns, concepts, and connections between disciplines that arise within established knowledge. Indeed, the approach has generated insights that strengthen evidence-based decision-making and was effectively utilized in others research in banking such as banking sector transformation, digital finance and regulatory innovation, among others (Gaviyau & Godi, 2025; Cele & Kwenda, 2025).

The sources included integration of various sources such as institutional publications, scholarly journals, and policy papers among others which have information pertaining to contracting third parties. This approach enabled deeper understanding of third parties, how and why they are utilized in the various aspects of organisations. Considerably, the concept of third parties is multi-disciplinary as every sector utilizes them.

To ensure reliability and credibility of the approach, specific inclusion and exclusion criteria was applied during the literature sources selection. The study selected peer reviewed journals, policy reports and institutional reports, which focused on AML/CFT frameworks and FATF recommendations. Also, studies in English only were adopted while non-academic sources and blogs not related to the financial sector and related AML/CFT issues were not considered.

3. Literature Review

3.1. Use of Third Parties Services in the Financial Services Sector

In the digital era, innovations to the financial services sector improve service delivery by overcoming technological and physical limitations associated with the analog era (Kim, Kim & Kyung, 2022). Initially, disruptive fintech businesses

threatened financial services sector, nevertheless, they are now widely regarded as partners. For fintech companies, partnering with banks mitigates the necessity to develop the operational processes required for entry into the highly regulated financial services industry (Sampat, Mogaji & Nguyen, 2024; Enriques & Ringe, 2020). Consequently, banking-as-a-platform emerged, allowing banks to provide contractual agreements to fintech firms for operation within the financial services industry.

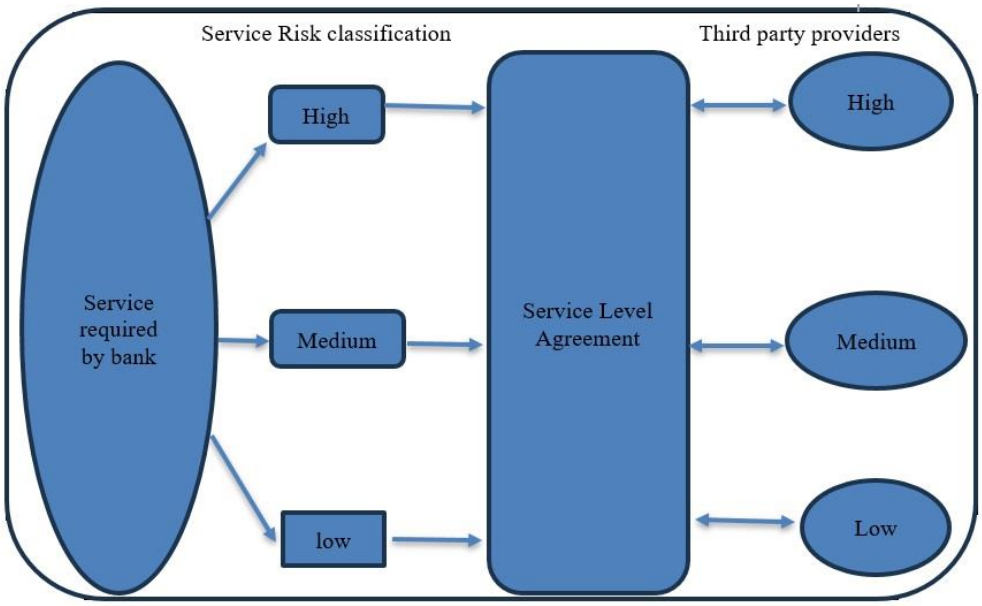

Figure 1. Financial institution third party service identification process

Source: Researcher's Own, 2025

Figure 1 shows the process of outsourcing third party services to operate in a highly regulated financial services sector. Financial institutions outsourcing operations due to variety of reasons such as cost reductions, expertise and skills (Konning et al., 2019). As shown, third party services are integrated into the highly regulated sector through alignment with a service level agreement (SLA). SLA reflects the risk and governance issues to be met in line with the financial sector regulatory obligations. The process involves identifying and risk classifying the required services, drawing up service level agreement and service provision. These are discussed below:

3.1.1. Third Party Services and Risk Management

To optimize efficiency and accelerate digital transformation, financial institutions are increasingly integrating with the third-party service providers. Integration brings risks such as cybersecurity, reputation and compliance among others. Given the privacy and confidentiality associated with the financial services sector, any contractual agreements with third parties should follow specified risk governance framework. Thus, third-party risk governance in financial institutions involves implementing policies, processes, and controls to manage risks from external service providers (Balogun, Olaniyi & Alao, 2025). Pierides and Mulligan (2025) emphasize the importance of this approach to protect institutional data, guaranteeing operational resilience, and addressing regulatory obligations. External outsourcing issues have become an important issue for financial services, requiring management and regulatory attention.

The evolving nature of risk and risk dynamism continues to shape regulations and regulatory structures. For instance, in the USA, the Federal Financial Institutions Examinations Council (FFIEC) issues regularly sector-based guidelines to managing third-party risk across the vendor lifecycle, including planning, selection, contracting, and ongoing monitoring (USAGov, 2024). For the financial services in Singapore the country's financial sector regulator through the Technology Risk Management (TRM) guidelines issued updated cybersecurity procedures in relation to outsourced services (Monetary Authority of Singapore (MAS), 2021). While in European Union (EU) the Digital Operational Resilience Act (DORA) requires financial institutions to implement third-party information and communication technologies (ICT) risk management strategies, including vendor risk classification, contractual safeguards, incident reporting, and continuous monitoring (EIOPA, 2023). This applies especially to third-party risks from information and communication technology (ICT), such as data breaches, access to sensitive information, reputational damage, and intellectual property disclosure.

Effective risk mitigation requires governance frameworks that include due diligence, real-time monitoring, access management, and risk mitigation approaches. Repeated failures in risk mitigation may result in cybersecurity breaches and damage financial institutions' reputations. Also, regulatory blind spots which are areas that fall outside the current regulatory framework which emerge especially in fintech driven environments. They occur when innovation outpaces regulation resulting in assessed risks gaps exploited by launderers (Reddy & Reddy, 2025).

3.1.2. Vendor Classification

An effective third-party risk management strategy requires vendor classification. Financial institutions classify vendors based on factors like risk level, data access, and operational disruption risks. Integration of critical vendors, such as cloud infrastructure and payment processors, remains crucial for business continuity and disaster recovery, while low-risk vendors may pose hidden threats (Bagogun et al., 2025; Cormack & Leverett, 2023). Notably, ICT suppliers with system-level access and non-ICT vendors have been linked to high-profile breaches (Vigren & Eriksson, 2025; Obioha-Val et al., 2025). By illustration, Capital One (Balogun, Olaniyi & Alao, 2025; Khan, Kabanov, Hua & Madnick, 2022) and Bangladesh Bank heist (Kabir & Hosen, 2024).

3.1.3. Service Level Agreements

Prior to onboarding, due diligence of service providers is conducted first. Service Level Agreements (SLAs) is an agreement between two parties, outsourcer and outsourcee, which details the expectations and responsibilities of parties. From a regulatory perspective, the financial institution serves as the outsourcer, while the fintech business or any related third-party business acts as the outsourcee. This indicates that the financial institution must verify that the outsourcee complies and operates within the regulatory confines. The due diligence process checks issues such as business history, business referrals, tax compliance, and registration certificates among others.

Compliance can be guaranteed through SLA, which is comprehensive contract management between the outsourcer and the outsourcee. Sissodia et al. (2024) posits that contract management is deemed to be a mediating factor, ensuring financial stability and addressing other regulatory mandates. Consequently, financial institutions are being encouraged to exercise greater oversight over their outsourcing partnerships. The absence of enforcement and adequate oversight may result in financial instability (Enriques & Ringe, 2020).

Regular audits monitor risk and specify exit strategies assuring continuity during vendor disengagement (Sissodia et al., 2024; Olutimehin et al., 2025). Although these frameworks provide a foundation, their effectiveness relies on customized application and adaptability to contextual realities. Strategic, proactive, and adaptive regulation of third- and fourth-party risks is needed due to regulatory divergence,

complex worldwide vendor networks, and a continuously changing risk environment.

4. Challenges and Opportunities for Third Parties in Mitigating Money Laundering Risk

4.1. Challenges

Financial institutions face problems in implementing strategic third-party risk governance due to structural, operational, and cultural factors among others (Sissodia, Rauthan & Barthwal, 2024). Though, third parties provide efficiency, they also bring regulatory, operational, and risk management concerns that may undermine AML/CFT procedures if not resolved. The following are some of the challenges associated with incorporating third parties into the financial services sector:

4.1.1. Data Protection and Confidentiality

Using third party services can include exchanging sensitive consumer data across businesses and countries. This presents data privacy and security, legal and ethical challenges. Different data protection laws may restrict information sharing, complicating AML/CFT and privacy compliance. For instance, most countries have implemented data protection legislations such as General Data Protection Regulation (GDPR) of Europe and Personal Information Protection Law (PIPL) of China (Sungjin & Junhyoung, 2025).

4.1.2. Reduced Control and Oversight

Financial institutions can lose control over the quality and integrity of AML/CFT elements. In the digital era, most customer onboarding is conducted virtually using third party platforms, this can entail losing control on information quality generated. This generates dependency risk, especially if the third party operates in a foreign country with different regulations. According to the Basel Committee on Banking Supervision (2020), inadequate management of third-party arrangements can lead to risk identification gaps, exposing institutions to regulatory breaches and reputational risks.

4.1.3. Structural Restrictions

Financial institutions might employ "check-the-box" compliance technique for third-party processes without sufficient due diligence or supervision. Instead, institutions may prioritize compliance with regulatory requirements above risk-informed approaches, leading to a false sense of security (Hochrainer-Stigler et al., 2021). Superficial compliance doesn't adapt to changing threats. Thus, the process of continual due diligence, business continuity planning, and vendor reaction to emerging threats should be adhered to (BIS, 2025). When engaging third parties, defined security processes should be followed and in place to secure sensitive data and information.

4.1.4. Accountability and Legal Ambiguity

When institutions outsource important activities to third-party providers, they struggle to map interdependence and assign accountability across several service partnerships. Although regulatory frameworks specify that the relying institution is ultimately responsible, assigning responsibility can be complicated, especially in cases of compliance lapses. If contractual provisions are unclear or inadequate, this may lead to legal disputes and increased regulatory attention.

Also, the lack of insight into fourth-party vendors, firms subcontracted by principal third parties over whom financial institutions typically have no contractual power, is a major issue (Olutimehin et al., 2025; Panorays, 2024). This obscurity might conceal systemic weaknesses and compromise risk mitigation methods for the institution. George et al. (2024) argued that the interdependent structure that exists in modern financial systems exposes vulnerabilities in external vendors' infrastructure to spread and pose systemic threats to essential institutional activities.

4.1.5. Resources Scarcity

Another issue is a scarcity of resources and finance for robust third-party risk management (TPRM) initiatives. Goktas and Grzybowski (2025) argue that successful governance requires ongoing investment in specialized personnel, monitoring technologies, and policy modification, which small and medium-sized financial institutions often struggle to achieve. Over 60% of financial businesses view TPRM as undervalued, with many lacking internal capacities for thorough monitoring (KPMG, 2020). Insufficient qualified knowledge leads to fragmented institutional accountability, resulting in third-party monitoring across departments like cybersecurity, legal, procurement, and operations. The lack of standardized risk

evaluation frameworks hinders the integration of TPRM into enterprise governance (Neotas, 2023).

4.1.6. Failure to Integrate TPRM Frameworks

Non-technical reform challenges include organizational inertia and cultural resistance. According to Cormack and Leverett (2023), many institutions neglect to update and integrate TPRM frameworks into their strategic operations. Successfully addressing these difficulties requires a coordinated, institution-wide approach that prioritizes dynamic governance, stakeholder alignment, and proactive risk culture.

4.2. Opportunities

Due to balancing difficulties associated with integrated financial structures and cyber laundering, innovative compliance procedures, such as utilizing third-party services remains paramount. Under Financial Action Task Force (FATF) Recommendation 17, financial institutions can rely on third parties to perform some AML/CFT functions, but they are still responsible for compliance. This recommendation presents various opportunities to mitigate money laundering risks, which are highlighted below:

4.2.1. Cost Reduction and Operational Efficiency

Third parties assist financial institutions minimize CDD duplication, especially in correspondent banking and cross-border financial relationships. A client of Bank A, which operates in multiple countries, can utilize the same onboarding information when conducting business in another country. According to World Bank (2022), shared reliance mechanisms may reduce compliance costs, speed up and standardize client onboarding process. This supports banking in jurisdictions with insufficient compliance infrastructure, where duplication of due diligence requirements could hinder business.

4.2.2. Access to Technology Innovation and Specialized Services

Third-party providers, such as fintech and regtech service providers, typically deploy specialized analytics, artificial intelligence, and machine learning technologies for transaction monitoring and risk assessment. The International Monetary Fund (2023) emphasizes that these technical abilities facilitate the identification of suspicious transactions as well as promote adaptable, risk-based methodologies for AML oversight. Smaller financial institutions, possibly lacking the resources to invest in

such technologies, can thus utilize third-party arrangements to enhance their compliance procedures. Risk assessment and transaction monitoring are other elements which contribute to minimize money laundering risks.

4.2.3. Risk Sharing

By sharing due diligence obligations across various regulated entities, financial services institutions can achieve enhanced monitoring while reducing concentration risk. This collaborative strategy strengthens the financial system's resilience, since various stakeholders participate in recognizing and mitigating money laundering issues. Levi and Reuter (2019) noted that multi-actor compliance systems enhance the identification of illicit payments through added monitoring approaches.

4.2.4. Cross Border Information Sharing

Third-party agreements, especially in correspondent banking relationships, allow financial institutions to obtain consumer information and risk assessments across multiple countries. The Basel Committee on Banking Supervision (2020) underscores that such collaboration improves transparency and facilitates the effective implementation of risk-based AML/CFT controls, particularly in complex international transactions.

5. Study Implications

5.1. Policy implications

The findings underscore the necessity for more regulatory clarity and harmonization in overseeing third-party reliance. Policymakers must coordinate national AML/CFT regulations with Financial Action Task Force standards, thereby ensuring that third parties comply with related regulations. Accordingly, it is essential to enhance cross-border regulatory collaboration to resolve gaps in AML/CFT regulatory framework.

Furthermore, policymakers ought to allocate resources towards capacity-building efforts to augment the technical and institutional competencies of third-party providers. Policies must handle the nexus of AML/CFT compliance and data protection, ensuring that regulatory frameworks promote information sharing while maintaining privacy.

5.2. Practice

The study underscores the necessity for financial institutions to have a robust risk-based framework regarding third-party reliance. This involves conducting due diligence on third parties, formulating explicit contractual agreements, and instituting periodic monitoring systems. Also, financial institutions must ensure timely access to CDD information and uphold robust internal supervision mechanisms.

The implementation of regtech can augment the success of reliance agreements through real-time monitoring and data analytics. Institutions must thoroughly evaluate the capability and dependability of third-party suppliers to reduce structural issues.

6. Conclusion

Dependence on third parties in accordance with Financial Action Task Force Recommendation 17 is a pragmatic solution to the growing complexity of AML/CFT compliance within a globalized financial framework. Although it provides significant benefits regarding efficiency, innovation, and financial inclusion, it also presents significant risks about oversight, regulatory ambiguity, and accountability.

The effectiveness of third-party reliance ultimately depends on the capacity of financial institutions and regulators to strike a balance between harnessing external resources and enforcing stringent internal controls. Strengthening regulatory frameworks, augmenting supervisory capacity, and promoting coordination among stakeholders will be essential in maximizing the advantages of reliance while minimizing its risks. This paper enhances both policy and scholarly discussions by offering a detailed insight of the challenges and opportunities linked to third-party reliance in AML/CFT regulatory frameworks. Future research should focus on the empirically grounded successes and failures of utilizing third parties within the financial services sector. Also, the role of fintech in aiding AML/CFT regulatory compliance.

References

Balogun, A. Y., Olaniyi, O. O., & Alao, A. I. (2025). Shaping trust and tension: Strategic leaks and their impact on global cybersecurity norms. *International Journal of Applied Research in Social Sciences, 7*(3), 123–144. https://doi.org/10.51594/ijarss.v7i3.1823

Barnum, P. (2014). *Target Data Breach (2014) - Technical, Financial, and Legal Analysis*. Inedo.com. https://security.inedo.com/library/incidents/Target-2014

Black, J. (2024). The role of third parties in regulatory systems: Examples from financial services regulation. In *The Regulator–Regulatee Relationship in High-Hazard Industry Sectors: New Actors and New Viewpoints in a Conservative Landscape* (pp. 23-31). Springer Nature Switzerland.

Cele, N. N., & Kwenda, S. (2025): Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. *Journal of Financial Crime*, 32, 31–48.

Cormack, A., & Leverett, É. (2023). Patchy incentives: using law to encourage effective vulnerability response. *Journal of Cyber Policy, 8*(1), 88–113. https://doi.org/10.1080/23738871.2023.2284233

EIOPA. (2023). *Digital Operational Resilience Act (DORA)*. https://www.eiopa.europa.eu/digitaloperational-resilience-act-dora_en

Enriques, L., & Ringe, W.-G. (2020). Bank–fintech partnerships, outsourcing arrangements and the case for a mentorship regime. *Capital Markets Law Journal, 15*(4), 374–397.

European Commission. (2020). *Digital Operational Resilience Act (Regulation (EU) 2022/2554.* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0595

FATF. (2025): *FATF Country Mutual Evaluations Assessment Reports*. https://www.fatf-gafi.org/en/publications/Mutualevaluations/Assessment-ratings.html

Feng, G. (2021). The influence of third-party payment on the intermediary business of commercial banks and countermeasures analysis. *International Journal of Humanities and Social Science, 1*(22), 43-50. http://www.acadpubl.com/Papers/Volume%201,%20IJHSS%202021.pdf#page=47

Gandawa, G. (2026): Regulating Digital Banking, FinTech, and Consumer Protection in African Financial Markets. *Interdisciplinary Journal of Arts, Politics and Law (IJAPL), 1*(2), 2002–2010.

Gaviyau, W., & Godi, J. (2025). Banking Sector Transformation: Disruptions, Challenges and Opportunities. *FinTech, 4*(3), 48. https://doi.org/10.3390/fintech4030048

George, A. S., Baskar, T., & Srikaanth, P. B. (2024). Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors. *Partners Universal International Innovation Journal, 2*(1), 51–75.

Kabir, M., & Hosen, M. M. (2024). A Study of Financial Crimes in the Banking Sector of Bangladesh. *International Journal of Law and Public Policy (IJLAPP), 6*(2), 49-57.

Khan, S., Kabanov, I., Hua, Y., & Madnick, S. (2022). A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned. *ACM Transactions on Privacy and Security, 26*(1), 1–29. https://doi.org/10.1145/3546068

Kim, E., Kim, M., & Kyung, Y. (2022). A case study of digital transformation: focusing on the financial sector in South Korea and overseas. *Asia Pacific Journal of Information Systems, 32*(3), 537-563.

Kolo, F. H. O., Joseph, S. A., Ogunmolu, A. M., Ejiofor, V. O., & Oyekunle, S. M. (2025). Mitigating Cybersecurity Risks in Financial Institutions through Strategic Third- Party Risk Governance Frameworks. *Journal of Engineering Research and Reports, 27*(5), 173-93. https://doi.org/10.9734/jerr/2025/v27i51501

Konning, M., Westner, M., & Strahringer, S. (2019). A Systematic Review of Recent Developments in IT Outsourcing Research. *Information Systems Management, 36*(1), 78–96. https://doi.org/10.1080/10580530.2018.1553650

Marjosola, H. (2021): The problem of regulatory arbitrage: A transaction cost economics perspective. *Regulations and Governance, 15*(2), 388–407. https://doi.org/10.1111/rego.12287

Monetary Authority of Singapore. (2021). *Technology Risk Management Guidelines 2021*. GRC Library. https://grclibrary.com/item_display.php?id=ca69632b-4229-491d-9231-7220b118d9a3

Nyreröd, T., Andreadakis, S., & Spagnolo, G. (2023). Money laundering and sanctions enforcement: large rewards, leniency and witness protection for whistleblowers. *Journal of Money Laundering Control, 26*(5), 912-925.

Obioha-Val, O. A., Lawal, T. I., Olaniyi, O. O., Gbadebo, M. O., & Olisa, A. O. (2025). Investigating the Feasibility and Risks of Leveraging Artificial Intelligence and Open-Source Intelligence to Manage Predictive Cyber Threat Models. *Journal of Engineering Research and Reports, 27*(2), 10–28.

Olutimehin, A. T., Ajayi, A. J., Metibemu, O. C., Balogun, A. Y., Oladoyinbo, T. O., & Olaniyi, O. O. (2025). Adversarial Threats to AI-Driven Systems: Exploring the Attack Surface of Machine Learning Models and Countermeasures. *Journal of Engineering Research and Reports, 27*(2), 341–362. https://doi.org/10.9734/jerr/2025/v27i21413

Pierides, M., & Mulligan, J. (2025). Key themes of resiliency, outsourcing and third-party risk management regimes. *Journal of Securities Operations & Custody, 17*(2), 102. https://doi.org/10.69554/auiq5402

Reddy, B. J., & Reddy, B. S. (2025, December). The Silent Risks of Fin-Tech: Unveiling India's Regulatory Blind Spots. In *International Conference on Law and Technology (ICLT 2025)* (pp. 309-324). Atlantis Press.

Restoy, F. (2021). Fintech regulation: How to achieve a level playing field. *Financial Stability Institute Occasional Papers*, 17, 1-27 https://www.bis.org/fsi/fsipapers17.htm

Rodrigues Pessoa, G. H. (2025): *Parallel Banking Through Fintechs: Regulatory Blind Spots, Tax Evasion and Money Laundering in Emerging Markets*. Preprints 2025, 2025120420. https://doi.org/10.20944/preprints202512.0420.v1

Sampat, B., Mogaji, E., & Nguyen, N. P. (2024). The dark side of FinTech in financial services: a qualitative enquiry into FinTech developers' perspective. *International Journal of Bank Marketing, 42*(1), 38-65.

Sissodia, R., Rauthan, M. S., & Barthwal, V. (2024). *Service Level Agreements (SLAs) and Their Role in Establishing Trust*. IGI Global. https://www.igi-global.com/chapter/service-level-agreements-slas-and-their-role-in-establishing-trust/340597

Sultan, N., Mohamed, N., Chisunga, D., & Satar, A. (2025). The correlation of Financial Action Task Force recommendations: the perception of compliance officers concerning the deployment of third parties and Fintech for customer due diligence. *Journal of Money Laundering Control, 28*(2), 292–314. https://doi.org/10.1108/JMLC-08-2024-0135

Sungjin, L., & Junhyoung, O. (2025). *Navigating Privacy: A Global Comparative Analysis of Data Protection Laws*. IET Information Security. https://doi.org/10.1049/ise2/5536763

USAGov. (2024). *Federal Financial Institutions Examination Council (FFIEC).* https://www.ffiec.gov/sites/default/files/media/press-releases/2024/cat-sunset-statement-ffiec-letterhead.pdf

Vigren, O., & Eriksson, K. (2025). A multilayer network model for studying business ecosystems: insights from enterprise architectures in the real estate sector. *Journal of European Real Estate Research*. https://doi.org/10.1108/jerer-04-2024-0027