



A Cyber-security Governance Framework for Nigerian FinTech Firms to Support Regulatory Compliance and Financial Inclusion

Jennifer Chiamaka Udeh

Department of Cyber Security, Faculty of Computing, Air Force Institute of Technology, Kaduna, Nigeria

Corresponding Author Email: udehjennifer73@gmail.com

Osichinaka Chiedu Ubadike

Department of Aerospace Engineering, Faculty of Air Engineering, Air Force Institute of Technology, Kaduna, Nigeria

Adeniran Kolade Ademuwagun

Department of Cyber Security, Faculty of Computing, Air Force Institute of Technology, Kaduna, Nigeria

Obunike Arinze Ubadike

Department of Computer Science, Faculty of Computing, Air Force Institute of Technology, Kaduna, Nigeria

Samaila Musa Abdullahi

Department of Cyber Security, Faculty of Computing, Air Force Institute of Technology, Kaduna, Nigeria

and

Dr. Suleiman Abu Usman

Department of Cyber Security, Faculty of Computing, Air Force Institute of Technology, Kaduna, Nigeria

Abstract

Nigeria's FinTech sector now functions as the primary channel of financial inclusion for millions of previously unbanked citizens, yet it operates without a unified cyber-security governance instrument. Unregistered schemes such as MMM Nigeria and CBEX have processed the financial data of millions of Nigerians under no

governance obligation whatsoever, while Chinese-backed super-app platforms such as OPay and PalmPay, which together serve more than 30 million accounts, raise unresolved data-sovereignty questions. This study designed the Nigerian FinTech Cyber-security Governance Framework (NFCGF), a six-layer, tiered, and implementable governance architecture grounded in the principles of Transparency, Accountability, and Explainability (TAE). The framework was developed using Design Science Research (DSR) methodology, drawing on quantitative and comparative evidence from Nigeria, Kenya, India, South Africa, and Ghana, and benchmarked against ISO/IEC 27001:2022, NIST CSF 2.0, PCI DSS v4.0, COBIT 2019, and SOC 2 Type II. A structured rubric-based expert review ($n = 3$) across five evaluation criteria produced an aggregate mean score of 4.20 out of 5.0 and yielded three traceable revisions. The NFCGF's mandatory pre-operational registration requirement, its OPay/PalmPay backend audit protocol, and its four-tier cost-proportionate implementation model together provide a governance pathway applicable to Nigerian FinTech operators of every size. The study concludes that institutional will, not framework design, is the harder constraint on implementation, and recommends a multi-round Delphi validation and pilot deployment as the necessary next stage.

Keywords: Cyber-security Governance, Nigerian FinTech, Financial Inclusion, Data Sovereignty, Regulatory Compliance.

Introduction

Nigeria's financial technology sector is among the most consequential digital transformations in sub-Saharan Africa, not simply because of its scale but because of what it has replaced. For many Nigerians, particularly those in semi-urban and rural communities, FinTech platforms are not supplementary to the financial system; they are the financial system [1]. Ogbonna et al. [2], in a primary quantitative study of OPay's services among Nigerian small and medium enterprises ($n = 460$), found that online credit, mobile applications, and point-of-sale terminal deployment jointly explain 67% of the variance in business development ($R^2 = .670$, $F = 417.93$, $p = .001$), establishing that cyber-security failures in FinTech infrastructure carry economic consequences proportionate to that contribution. Ezeocha [3] adds the inclusion dimension, showing that trust and security, rather than cost or connectivity, are the primary barriers to deeper FinTech adoption among low-income and first-time users,

which inverts the common assumption that stronger governance restricts rather than enables access.

By 2024, Nigeria hosted over 200 registered FinTech firms attracting approximately \$1.5 billion in venture capital in 2023 alone [8], spanning payment processors, neo-banks, digital lenders, InsurTech operators, and virtual asset service providers newly brought under the Investment and Securities Act (ISA) 2025. Chinese investors have deployed over \$700 million into OPay and PalmPay alone [9], creating data-sovereignty complications that sit at the centre of this study: both platforms use WeChat-inspired super-app architectures that may be subject to China's Data Security Law and Personal Information Protection Law, which can compel data disclosure to Chinese authorities under national security conditions.

Nigeria's FinTech cyber-security governance is fragmented across six regulatory agencies (the Central Bank of Nigeria, the Securities and Exchange Commission, the Nigeria Data Protection Commission, the National Information Technology Development Agency, the Economic and Financial Crimes Commission, and the Nigerian Financial Intelligence Unit), and no single instrument applies to all operators. Two cases illustrate what this study terms the 'operating on the air' problem: fraudulent, unregistered entities that exploit the FinTech identity while bearing none of its governance obligations. MMM Nigeria (2015–2018) attracted roughly three million participants before its collapse wiped out an estimated \$50 million; CBEX, which collapsed in April 2025, attracted an estimated 500,000 participants and caused losses of approximately ₦1.3 trillion. Neither entity was ever licensed, registered, or subjected to a cyber-security audit. The ISA 2025 criminalises Ponzi schemes and brings virtual asset service providers under Securities and Exchange Commission oversight, but it does not specify which cyber-security standards licensed entities must meet, leaving its cyber-security licensing condition legally present but practically unenforceable.

This study designs the Nigerian FinTech Cybersecurity Governance Framework (NFCGF): a structured, six-layer, implementable cyber-security architecture that supports regulatory compliance, advances financial inclusion, and protects Nigerian data sovereignty, grounded in the principles of Transparency, Accountability, and Explainability. The specific objectives are to (i) assess cyber-security governance gaps in Nigeria's FinTech sector; (ii) design the NFCGF, including a supporting Nigerian FinTech Data Classification Matrix; and (iii) recommend targeted legislative reforms and international regulatory provisions for adoption. The remainder of this paper is organized as follows: Section 2 reviews the relevant literature; Section 3 presents the design methodology and framework architecture; Section 4 reports the validation results and discussion; Section 5 sets out limitations and future work; and Section 6 concludes the paper.

Literature Review

The Nigerian FinTech Ecosystem and Its Economic Significance

Lottu et al. [7] trace the sector's development from rudimentary automated teller machine infrastructure in the 1990s, through the Central Bank of Nigeria's Cashless Policy of 2012, to today's multi-product digital financial ecosystem. Ogbonna et al. [2] provide the clearest empirical anchor for the sector's economic weight, while Ikenna [6] identifies the absence of formalised firm-level risk management, rather than inadequate regulation alone, as a root structural cause of cyber-security failure. Oni et al. [1] argue that the optimal governance approach is a tiered, risk-proportionate framework that imposes universal minimum requirements while scaling obligations to firm size, an argument this study adopts directly. Hassan et al. [4] complement this position, showing that the primary constraint is not regulatory design but the absence of enforcement mechanisms and technical governance, risk, and compliance (GRC) capacity within Nigerian regulatory agencies, a finding corroborated quantitatively by Akinsulire and Ohakawa [5], who demonstrate that control deficiencies produce regulatory compliance failures and elevated incident rates.

The 'Operating on the Air' Problem and Data Sovereignty

The MMM Nigeria and CBEX cases illustrate a governance failure type that conventional cyber-security frameworks do not address: not imperfect governance among registered firms, but the complete absence of governance for entities that never entered the regulatory perimeter [1]. Separately, OPay and PalmPay's WeChat-inspired super-app architectures aggregate payment, communication, and behavioural data into unified user profiles [9]; PalmPay's pre-installation on Transsion devices further blurs the boundary between a FinTech application and device-level data collection. Nigeria's Data Protection Act (NDPA) 2023 establishes data sovereignty as a legal principle, but it does not, on its own, provide the technically enforceable controls needed to operationalise that principle against foreign-owned platforms.

Comparative Developing-Economy Governance Evidence

A systematic review of four comparable developing-economy markets, Kenya, India, South Africa, and Ghana, establishes that purpose-built, contextually adapted cyber-security governance instruments consistently outperform the direct transplantation of international standards. Table 1 summarises the design features drawn from each market and their relevance to the NFCGF.

Table 1: Comparative Developing-Economy FinTech Cybersecurity Governance Evidence

Country	Instrument	Key Design Feature	Relevance to NFCGF
Kenya	CBK Cyber-security Guidelines for PSPs (2023)	Three-tier compliance model by transaction volume and risk	Validates tiered implementation; no data-sovereignty provision
India	RBI Master Direction on Digital Payment Security Controls (2021)	Inclusion-sensitive authentication; 47% fraud reduction	Basis for mandatory USSD-OTP in Layer 3
South Africa	SARB-FSCA Joint Standard 2 of 2023	Proportionality; joint inter-agency standard	Validates the proposed FCRCC coordination body
Ghana	BOG Cyber-security Directive for PSPs (2022)	Integrates data protection and cyber-security in one instrument	Informs the integrated design of Layer 4

Kenya's Central Bank Cyber-security Guidelines for Payment Service Providers (2023) confirm that a mandatory, tiered, sector-specific framework is achievable in a comparable African market [12]. India's Reserve Bank of India reported a 47% reduction in digital payment fraud per unit of transaction volume following its Master Direction on Digital Payment Security Controls, attributable to inclusion-sensitive authentication requirements [13], [14]. South Africa's joint SARB-FSCA standard demonstrates that inter-agency coordination in financial cyber-security is achievable, though its two-agency model is structurally simpler than Nigeria's six-agency fragmentation problem [15]. Ghana's integrated cyber-security-and-data-protection directive offers the closest West African design template for treating data sovereignty as intrinsic to cyber-security governance rather than a separate compliance stream [16].

International Standards and the Nigerian Regulatory Landscape

ISO/IEC 27001:2022 [17], NIST Cybersecurity Framework 2.0 [18], PCI DSS v4.0 [19], and COBIT 2019 [20] each provide partial coverage of the FinTech cyber-security governance space but require contextual adaptation for the Nigerian environment, a finding consistent across all four comparator markets reviewed above. Domestically, the CBN's Risk-Based Cyber-security Framework applies only to CBN-

supervised deposit money banks and payment service banks, leaving digital lenders, InsurTech platforms, and newly licensed virtual asset service providers outside its scope. The NDPA 2023 [21] establishes the Nigeria Data Protection Commission's supervisory authority but lacks FinTech-specific provisions, while the ISA 2025 [22] criminalises fraudulent schemes without specifying the cyber-security standard that licensed operators must meet [24]. These gaps, taken together, establish the governance vacuum that the NFCGF is designed to close.

Transparency, Accountability, and Explainability

Transparency, Accountability, and Explainability (TAE) function in this study as design requirements rather than aspirational values. Transparency requires that cyber-security practices and incident histories be publicly verifiable, a standard whose absence allowed MMM Nigeria and CBEX to present fabricated governance credentials unchallenged. Accountability requires that cybersecurity responsibilities be assigned to named individuals with enforceable consequences. Explainability requires that algorithmic decisions affecting financial access, particularly credit scoring and fraud detection, be communicable in plain language to affected users and regulators, a requirement made more urgent by the profiling architecture of WeChat-inspired super-apps.

Methodology

Research Design

This study adopts a qualitative Design Science Research (DSR) methodology [25], the appropriate paradigm when the primary research output is a designed artefact intended to solve an identified sociotechnical problem. DSR quality was assessed on three criteria: utility (does the artefact solve the governance problem?), rigour (is it grounded in scholarly and empirical evidence?), and relevance (is it contextually appropriate for its target environment?), supplemented in this study by a fourth criterion, parsimony, reflecting the need for the framework to remain practically navigable for the smallest operators most dependent on inclusive governance. A survey methodology was considered and rejected because it can measure attitudes but cannot itself produce a governance framework; a case-study approach was considered and rejected because its output is explanatory rather than prescriptive and would not generalise across the more than 200 Nigerian FinTech operators the NFCGF targets.

The DSR process followed three phases: problem identification and motivation, conducted through the literature and comparative governance review summarised in Section 2; design and development, comprising the six-layer NFCGF architecture described below; and evaluation, comprising the structured expert

review reported in Section 4. Data was collected through three channels: a structured rubric-based questionnaire administered to three purposively selected domain experts; systematic review of Nigerian regulatory instruments (the CBN Risk-Based Cyber-security Framework, ISA 2025, NDPA 2023, the Banks and Other Financial Institutions Act 2020, and the Cybercrimes Act 2015); and secondary empirical and regulatory evidence from Nigeria, Kenya, India, South Africa, and Ghana.

The NFCGF Six-Layer Architecture

The NFCGF is organised as six interdependent layers, each addressing a distinct governance dimension, with TAE running as a mandatory cross-cutting requirement through all six. Layer 1 (Governance and Regulatory Architecture) establishes the mandatory pre-operational cybersecurity registration requirement, the framework's principal structural innovation. Any entity presenting itself as a digital financial service provider, whether or not formally licensed, must register a governance baseline and obtain a compliance certificate before commencing operations, closing the vacuum that allowed MMM Nigeria and CBEX to operate unchecked.

Layer 1 also introduces a Designated Cyber-security Accountability Officer role and a proposed FinTech Cyber-security Regulatory Coordination Committee (FCRCC) to harmonise the six fragmented regulatory agencies. Layer 2 (Risk Management) mandates a continuously updated information technology asset inventory, quarterly vulnerability scanning, annual penetration testing, and a dedicated risk-assessment stream for foreign-owned platforms. Layer 3 (Identity and Access Management) mandates tiered Know-Your-Customer verification and a non-negotiable minimum authentication channel, unstructured supplementary service data (USSD)-based one-time passwords, directly modelled on the inclusion-sensitive authentication requirement behind India's 47% fraud-reduction result [14]; because a USSD channel authenticates through the phone number rather than the device, Layer 3 also specifies a SIM-swap countermeasure package comprising carrier-side swap notification integration, a risk-proportionate cooling-off period before USSD transaction authority resumes, and step-up verification triggers.

Layer 4 (Data Protection, Privacy, and Sovereignty) specifies a seven-category backend audit protocol for OPay and PalmPay, covering data-residency certification, application programming interface architecture documentation, encryption key custody, parent-company data-sharing agreements, cloud-vendor SOC 2 Type II assurance, data-controller registration, and foreign-government access protocols; the central technical insight is that data encrypted with keys held offshore by a parent company is not protected against that parent company's access regardless of the encryption algorithm applied. Layer 5 (Incident Response and Resilience) mandates continuous monitoring, a formal incident response plan, and tiered notification

windows to the Central Bank of Nigeria. Layer 6 (Financial Inclusion Integration) requires an inclusion-sensitive security design review, local-language security awareness materials, and an annual inclusion impact assessment, operationalising Ezeocha's [3] finding that security and inclusion are complementary rather than competing objectives.

The architecture is supported by a Nigerian FinTech Data Classification Matrix spanning customer identity data, financial transaction data, card and payment credentials, digital asset holdings, behavioural and profiling data, credit and risk assessment data, and regulatory and audit data, each mapped to a beneficial owner, storage requirement, transfer rule, and regulatory overseer. Implementation is organised into four cost-proportionate tiers, from a minimum baseline applicable to every entity presenting as a digital financial service provider through to full compliance with independent ISO/IEC 27001 certification for large platforms and foreign-owned operators, directly responding to the empirical finding that governance heaviness produces avoidance rather than compliance [1].

Validation Methodology

The completed framework was evaluated through a structured rubric-based expert review consistent with Hevner et al.'s [25] DSR evaluation phase.

Three domain experts, selected for directly relevant professional and academic experience in national security governance, frontline FinTech regulatory compliance, and academic financial technology governance research, independently scored the NFCGF on a 1-to-5 scale across five criteria: Comprehensiveness, Contextual Appropriateness, Regulatory Alignment, Inclusion Sensitivity, and Implementability. Each expert reviewed the complete framework independently and returned a scored rubric with qualitative commentary within an agreed ten-working-day window. This expert review is treated as the study's primary validation instrument and is reported separately from the standards-benchmarking exercise summarised in Section 2, which is a descriptive comparative mapping rather than independent evidence of the framework's quality.

Results and Discussion

Expert Validation Results

Table 2 reports the complete rubric scores. The framework scored consistently in the Good-to-Excellent range on four of five criteria, each returning a mean of 4.33 out of 5.0. Implementability was rated lowest, at a mean of 3.67, on every reviewer's independent assessment, and the aggregate mean across all fifteen individual scores was 4.20 out of 5.0.

Table 2: Expert Review Rubric Scores (1–5 Scale)

Criterion	Expert 1	Expert 2	Expert 3	Mean	Assessment
Comprehensiveness	4	4	5	4.33	Good-Excellent
Contextual Appropriateness	5	4	4	4.33	Good-Excellent
Regulatory Alignment	4	5	4	4.33	Good-Excellent
Inclusion Sensitivity	4	4	5	4.33	Good-Excellent
Implementability	4	3	4	3.67	Lowest-rated
Aggregate Mean				4.20	Good

The uniform 4.33 clustering across four criteria warrants caution rather than uncritical acceptance. Because the review was conducted in a single, non-anonymous round, the pattern is at least as consistent with response anchoring or deference among reviewers who were known to one another as it is with genuinely independent convergence. Applying the logic of the Delphi method to this result, in which anonymity and iteration are specifically designed to surface latent disagreement, suggests the 4.20 aggregate is better read as an upper-bound first-round impression than as a stable estimate of the framework's fitness for purpose. This reading does not diminish the value of the three specific, traceable revisions the review produced, which are reported below and would plausibly survive a more rigorous multi-round process intact.

Traceable Revisions

Three substantive revisions followed directly from expert feedback. First, the original Tier 1 registration process required a full cyber-security risk assessment before registration, which a reviewer with direct operational experience of small FinTech operators judged disproportionate and likely to produce the registration avoidance that Oni et al. [1] identify as a critical design risk; the requirement was reduced to a minimum governance-baseline document, with the full risk assessment deferred to a 90-day post-registration obligation. Second, an open banking application programming interface governance control was added to Layer 3 in response to the growing, previously ungoverned attack surface created by the CBN's Open Banking initiative. Third, provisions addressing non-fungible token platforms were added to Layer 1's regulatory compliance component, and the Layer 6 inclusion

impact assessment was revised to require user-level accessibility surveys conducted in at least four Nigerian languages.

Gap-Resolution and Comparative Synthesis

Mapping each of the six governance failures identified in Section 1 to its NFCGF architectural response confirms the framework's utility, the first DSR quality criterion. The governance vacuum is addressed by Layer 1's mandatory pre-operational registration; data-sovereignty risk from foreign-owned platforms is addressed by the Layer 4 backend audit protocol; regulatory fragmentation is addressed by the proposed FCRCC, modelled on the South African SARB-FSCA precedent but scaled to a more complex six-agency environment; financial inclusion exclusion risk is addressed by Layer 6's inclusion-sensitive design review; cyber-security maturity deficits are addressed by Layers 2, 3, and 5; and the ISA 2025 cyber-security specificity gap is addressed by Layer 1's designation of NFCGF compliance or ISO/IEC 27001:2022 certification as the applicable standard pending formal Securities and Exchange Commission subsidiary regulation. Each response, however, carries an implementation constraint, most consistently the absence of a statutory basis for the FCRCC and the dependence of the Layer 4 audit protocol on the CBN's willingness to exercise existing examination authority against commercially significant, foreign-owned platforms.

Unresolved Design Tensions

Beyond the validation exercise itself, six design tensions remain open rather than fully resolved. The FCRCC's budgetary placement, funding mechanism, and inter-agency dispute-resolution procedure are not yet specified. The Layer 5 two-hour critical-incident notification window, faster than the 72-hour standard common internationally, has not been benchmarked against the operational capacity of Tier 1 and 2 operators without dedicated security staff, and a tier-differentiated notification timeline is a more defensible design. The mandatory USSD-based one-time password channel, while essential for financial inclusion, remains vulnerable to SIM-swap fraud unless paired with the carrier-level countermeasures specified in Layer 3, a genuine security-inclusion trade-off rather than a solved problem. The four-language floor for security disclosures (English, Hausa, Yoruba, and Igbo) should be read as a minimum rather than a ceiling given Nigeria's linguistic diversity. The origin of the ISA 2025's unspecified cyber-security standard, whether a drafting oversight or a deliberate deferral to subsidiary regulation, remains unexamined. Finally, the Layer 4 audit protocol assumes a degree of operator cooperation that regulatory forbearance against systemically significant platforms could undermine in practice; framing the audit as a routine periodic examination, comparable to a standard bank examination, rather than a punitive investigation, is offered as a practical mitigation.

Limitations and Future Work

This study has four principal limitations, each pointing to a specific direction for future research. The validation sample ($n = 3$) is appropriate for an undergraduate Design Science Research exercise but falls short of a full Delphi panel or a live pilot deployment; a structured pilot with three to five volunteer FinTech operators across Tiers 1 to 3, measuring registration compliance, DCAO appointment rates, and USSD authentication uptake over twelve months, together with a formally constituted, anonymous, multi-round Delphi panel, is recommended as the immediate next stage. The analysis of OPay and PalmPay's data-governance practices relies on publicly available ownership information and documented industry analysis rather than independent technical audit access; primary interviews with regulatory officers at the CBN Financial Policy and Regulation Department, the Securities and Exchange Commission FinTech Division, and the Nigeria Data Protection Commission Enforcement Unit would strengthen this analysis. Cost estimates for the four-tier implementation model are stated without derivation from vendor procurement data, and a benchmarking study using comparable data from Kenya and Ghana is recommended.

Finally, the NFCGF's registration mechanism assumes an identifiable legal entity capable of registering, a premise that decentralised finance protocols challenge. A dedicated research agenda on the governance of identity-less financial protocols is proposed as future work, alongside longitudinal research tracking the relationship between NFCGF-aligned control adoption and financial inclusion outcomes, in order to generate a Nigerian equivalent of India's documented fraud-reduction evidence [14].

Conclusion

This paper presented the Nigerian FinTech Cybersecurity Governance Framework (NFCGF), a six-layer, tiered, and TAE-grounded cyber-security governance architecture designed to close the governance vacuum that has allowed fraudulent entities to defraud millions of Nigerians, to address the unresolved data-sovereignty exposure created by Chinese-backed super-app platforms, and to advance financial inclusion through security design rather than at its expense. Structured expert review across five criteria produced an aggregate mean score of 4.20 out of 5.0 and generated three substantive, traceable revisions, though the study is explicit that this figure represents a first-round impression rather than a fully validated measure of fitness for purpose. The framework's core contribution, the mandatory pre-operational registration requirement, the OPay/PalmPay backend audit protocol, and the tiered implementation model, is grounded throughout in Nigerian and comparative developing-economy evidence. The harder half of implementation is institutional rather than technical: it depends on the Central Bank

of Nigeria's willingness to exercise existing examination authority against commercially powerful platforms, the Securities and Exchange Commission's issuance of subsidiary regulations under the ISA 2025, and six historically independent regulatory agencies agreeing to coordinate through the proposed FCRCC. A multi-round Delphi validation and a controlled pilot deployment are recommended as the necessary next stages before the NFCGF can be considered a policy-ready regulatory instrument.

References

- [1] O. Oni, A. Japinye, G. Ifarajimi, and O. Olubowale, "Regulating fintech for financial stability in Nigeria: Balancing cybersecurity risks and financial inclusion," *African Journal of Economics and Business Research*, vol. 4, no. 2, 2025. <https://doi.org/10.4314/ajebr.v4i2.4>
- [2] K. A. Ogbonna et al., "FinTech and business growth in South West Nigeria: Empirical evidence from OPay users," *Journal of Management and Science*, vol. 14, no. 1, pp. 87–91, 2024.
- [3] C. Ezeocha, "Financial technology as a tool for promoting financial inclusion in Nigeria," *African Journal of Management and Business Research*, 2024. <https://doi.org/10.62154/qqr2sy50>
- [4] A. Hassan, S. Ewuga, A. Abdul, T. Abrahams, M. Oladeinde, and S. Dawodu, "Cybersecurity in banking: A global perspective with a focus on Nigerian practices," *Computer Science & IT Research Journal*, vol. 5, no. 1, 2024. <https://doi.org/10.51594/csitrj.v5i1.701>
- [5] A. Akinsulire and T. Ohakawa, "Enhancing cybersecurity governance in financial institutions: A quantitative study on control deficiencies and regulatory compliance," *International Journal of Advanced Multidisciplinary Research and Studies*, vol. 4, no. 6, 2024. <https://doi.org/10.62225/2583049x.2024.4.6.4264>
- [6] M. Ikenna, "Operational risks faced by financial institutions in the digital age: A case of Nigeria," *International Journal of Modern Risk Management*, 2024. <https://doi.org/10.47604/ijmrm.2642>
- [7] O. Lottu, A. Abiola, D. Daraojimba, A. Alabi, A. John-Ladega, and C. Daraojimba, "Digital transformation in banking: A review of Nigeria's journey to economic prosperity," *International Journal of Advanced Economics*, vol. 5, no. 8, 2023. <https://doi.org/10.51594/ijae.v5i8.572>
- [8] KPMG, "Africa's fintech landscape 2024," KPMG, 2024. <https://home.kpmg/africa>
- [9] Semafor, "China-owned fintechs OPay and PalmPay win big after Nigeria cash crisis," Semafor, 2023. <https://www.semafor.com>
- [10] BusinessDay Nigeria, "How two Chinese fintechs clinched Nigeria's POS market," BusinessDay, 2023. <https://businessday.ng>

-
- [11] Ecofin Agency, "In Nigeria, bank technology failures pushed OPay and PalmPay to leadership in daily payments," Ecofin Agency, 2024. <https://www.ecofinagency.com>
- [12] Central Bank of Kenya, "Cybersecurity guidelines for payment service providers," CBK, 2023. <https://www.centralbank.go.ke>
- [13] Reserve Bank of India, "Master direction on digital payment security controls," RBI, 2021. <https://www.rbi.org.in>
- [14] Reserve Bank of India, "Annual report on digital payment fraud statistics 2022-23," RBI, 2023. <https://www.rbi.org.in>
- [15] South African Reserve Bank and Financial Sector Conduct Authority, "Joint Standard 2 of 2023: Cybersecurity and cyber resilience requirements," SARB, 2023. <https://www.resbank.co.za>
- [16] Bank of Ghana, "Cybersecurity directive for payment service providers," Bank of Ghana, 2022.
- [17] International Organization for Standardization, "ISO/IEC 27001:2022 Information security management systems Requirements," ISO, 2022. <https://www.iso.org/standard/27001>
- [18] National Institute of Standards and Technology, "NIST Cybersecurity Framework 2.0 (CSWP 29)," NIST, 2024. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>
- [19] Payment Card Industry Security Standards Council, "PCI DSS v4.0," PCI SSC, 2022. <https://www.pcisecuritystandards.org>
- [20] ISACA, "COBIT 2019 framework: Governance and management objectives," ISACA, 2019. <https://www.isaca.org/resources/cobit>
- [21] The Federal Republic of Nigeria, "Nigeria Data Protection Act 2023," 2023.
- [22] The Federal Republic of Nigeria, "Investment and Securities Act 2025," 2025.
- [23] The Federal Republic of Nigeria, "Cybercrimes (Prohibition, Prevention, etc.) Act 2015," 2015.
- [24] FinTech Association of Nigeria, "Nigeria's ISA 2025: Key takeaways from stakeholder engagement with the SEC," FinTechNGR, 2025. <https://fintechng.org>
- [25] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS Quarterly*, vol. 28, no. 1, pp. 75–105, 2004.
- [26] R. Akintoye, O. Ogunode, M. Ajayi, and A. Joshua, "Cyber security and financial innovation of selected deposit money banks in Nigeria," *Universal Journal of Accounting and Finance*, 2022. <https://doi.org/10.13189/ujaf.2022.100302>
- [27] GSMA, "State of the industry report on mobile money 2023," GSMA, 2023. <https://www.gsma.com>
-