

GOVERNING FINTECH THROUGH BORROWED LICENCES: BOARD ACCOUNTABILITY AND REGULATORY DESIGN IN NIGERIA'S DIGITAL FINANCIAL SECTOR

Misbau Alamu Lateef*

Abstract

Nigeria has no licence designed specifically for digital banks. Firms offering app-based deposit, payment and lending services operate under microfinance, payment service bank or finance company licences, or under no financial licence at all. This article asks what follows for corporate governance. Through doctrinal analysis of the Companies and Allied Matters Act 2020, the Banks and Other Financial Institutions Act 2020, the Nigerian Code of Corporate Governance 2018 and Central Bank of Nigeria instruments, evaluated against five criteria drawn from bank-governance theory and regulated self-governance, it argues that Nigerian fintech governance is licence-contingent: board obligations follow the licence a firm holds rather than the risks its activities create. Board-level technology competence and oversight are required of payment service and commercial banks but not of microfinance banks, the licence most digital banks use, while consumer and data obligations attach to activity but stop below board level. A functional comparison with the United Kingdom, Kenya and Singapore shows how governance can instead attach to activity or regulated status. The article proposes reforms achievable largely under existing powers and introduces licence-contingency as an analytical concept for jurisdictions that have absorbed digital finance into pre-existing licence categories.

* PhD, SFHEA; Senior Lecturer in Law, School of Criminology, Politics, and Law, University of Hull, United Kingdom. Email: m.lateef@hull.ac.uk.

Keywords: corporate governance; fintech; bank governance; licensing; board accountability; Nigeria

1. INTRODUCTION

A customer who opens an account on a Nigerian banking app may be dealing with a microfinance bank, a payment service bank, a commercial bank's digital subsidiary, or a technology company that holds no deposit-taking licence. To that customer the services look alike. To the law they do not. Nigeria has no licence category designed for digital banks, so entities or firms that operate entirely through digital channels must fit themselves into licence categories designed for other kinds of institution.¹ The Banks and Other Financial Institutions Act 2020 (BOFIA) now defines banking business to include business conducted 'digitally, virtually or electronically only'.² Recognition of the activity, however, has not been matched by a governance regime designed for the institutions that carry it on.

This paper examines the consequences of that mismatch for corporate governance. Its central claim is that the governance of Nigerian fintech is *licence-contingent*. The duties of a fintech board, its required composition and committees, and the oversight it must exercise over technology, cyber and data risks follow from the licence the firm holds and from the general company law that applies to it. They do not follow from the risks its activities generate. Two firms running similar digital deposit and payment services can therefore carry materially different governance obligations. That difference reflects regulatory history rather than any assessment of risk.

¹ N Ofo, R Ngwoke and FK Ekwe, 'An Appraisal of the Regulation of Digital Banks in Nigeria' (2024) 18(1) AGORA International Journal of Juridical Sciences 62.

² Banks and Other Financial Institutions Act 2020 (BOFIA 2020), s 131.

Three research questions (RQs) structure the analysis. The first (RQ1) asks what board-level governance obligations Nigerian law currently imposes on digital financial institutions, and how those obligations vary across licence categories. The second (RQ2) asks where, measured against an explicit evaluative framework, those obligations fall short, and whether licence-contingency is their common cause. The third (RQ3) asks what comparable jurisdictions show about attaching governance obligations to activity and risk rather than to licence category, and what limits the transfer of those approaches to Nigeria.

The existing literature approaches these questions from three directions without meeting at the point this paper occupies. The first strand is the international fintech regulation literature. It has concentrated on the design of the regulator's toolkit: sandboxes, innovation hubs and RegTech.³ It has also examined the tension Brummer and Yadav⁴ term the 'innovation trilemma', under which regulators seeking to issue clear rules, maintain market integrity and encourage innovation can achieve at most two of the three. This literature has said comparatively little about the internal governance obligations that licensing regimes impose on fintech firms. The second strand is the bank governance literature. It explains why banks warrant

³ Dirk A Zetsche and others, 'Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation' (2017) 23 *Fordham Journal of Corporate and Financial Law* 31; Hilary J Allen, 'Regulatory Sandboxes' (2019) 87 *George Washington Law Review* 579; Ross P Buckley and others, 'Building Fintech Ecosystems: Regulatory Sandboxes, Innovation Hubs and Beyond' (2020) 61 *Washington University Journal of Law and Policy* 55; Misbau Alamu Lateef and Ammar Abdullah Alhammadi, 'Beyond the Sandbox: Rethinking Fintech Regulatory Innovation in Kuwait through Comparative Analysis' (2025) 16 *Beijing Law Review* 2259.

⁴ Chris Brummer and Yesha Yadav, 'Fintech and the Innovation Trilemma' (2019) 107 *Georgetown Law Journal* 235.

governance arrangements different from those of ordinary companies,⁵ but it predates fintech and takes a licensed, full-service bank as its object. The third strand is Nigerian corporate governance scholarship. It has examined governance in weak institutional settings⁶ and, more recently, the licensing of digital banks.⁷ It has not examined how governance obligations are distributed across the licence categories through which digital finance is actually delivered. This paper supplies that analysis.

Nigeria is a theoretically distinctive case, not merely a large one. Adegbite⁸ characterises Nigeria as a weak institutional setting. Corporate law enforcement and self-regulatory initiatives remain largely aspirational there, and market pressures such as takeovers and shareholder activism are absent or ineffective. On that account, the governance structures firms are required to build internally carry more of the governance burden than they would where external discipline is strong. It follows, and this is the present paper's inference rather than Adegbite's, that the question of which firms are required to build those structures matters more in Nigeria than elsewhere. Three features of the Nigerian framework make that allocation analytically revealing.

The first is the borrowed-licence model already described. The second is a structure in which at least seven federal regulators hold mandates touching fintech activity. The third is a gradient in governance rules

⁵ Jonathan R Macey and Maureen O'Hara, 'The Corporate Governance of Banks' (2003) 9(1) Federal Reserve Bank of New York Economic Policy Review 91; Basel Committee on Banking Supervision, *Corporate Governance Principles for Banks* (Bank for International Settlements 2015) (BCBS).

⁶ Emmanuel Adegbite, 'Good Corporate Governance in Nigeria: Antecedents, Propositions and Peculiarities' (2015) 24 International Business Review 319.

⁷ Ofo, Ngwoke and Ekwe (n 1).

⁸ Adegbite (n 6).

across licence categories. The Central Bank of Nigeria's (CBN) 2023 Corporate Governance Guidelines apply, together with the Nigerian Code of Corporate Governance 2018, to commercial, merchant, non-interest and payment service banks.⁹ They require at least two non-executive directors, one of them independent, with knowledge and experience of innovative financial technology, information and communication technology (ICT) and/or cyber security.¹⁰ They also require the board to develop and implement an IT framework covering data confidentiality, network security, third-party connections and incident response.¹¹ A payment service bank must in addition establish a board committee for ICT and cybersecurity, and a majority of its audit committee must be knowledgeable in those fields.¹² Microfinance banks, by contrast, are deposit-taking institutions that extend credit,¹³ and theirs is the licence most digital banks use.¹⁴ They are governed by a 2018 code that contains none of these requirements and ties board skills only to the general approved-persons regime.¹⁵ Finance companies, whose licence permits consumer lending but not deposit-taking, are governed by 2014 guidelines and a 2018 code that mirrors the microfinance code; neither imposes any technology-

⁹ Central Bank of Nigeria, *Corporate Governance Guidelines for Commercial, Merchant, Non-Interest and Payment Service Banks in Nigeria* (13 July 2023) (CBN Guidelines 2023) Application section; Financial Reporting Council of Nigeria, *Nigerian Code of Corporate Governance 2018* (NCCG).

¹⁰ CBN Guidelines 2023 (n 9) s 1.7.

¹¹ *ibid* s 2.9.

¹² *ibid* ss 6.6, 6.13(c).

¹³ Central Bank of Nigeria, *Microfinance Policy, Regulatory and Supervisory Framework for Nigeria* (December 2005) (Microfinance Policy 2005) paras 11.5, 13.3.

¹⁴ Ofo, Ngwoke and Ekwe (n 1).

¹⁵ Central Bank of Nigeria, *Code of Corporate Governance for Microfinance Banks in Nigeria* (24 October 2018) (MFB Code) paras 1.1, 2.1.4, 2.2.3.

governance requirement.¹⁶ Firms holding no CBN licence answer only to general company law. A payment service bank must therefore maintain a board-level ICT and cybersecurity committee, while a microfinance-licensed digital bank taking deposits from the public need not. The most demanding technology-governance rules are therefore not where much of the digital retail activity is. That gap between rule and risk is the subject of this paper, and it matters for any jurisdiction that has absorbed digital finance into pre-existing licence categories.

The paper proceeds as follows. Section 2 explains the method and the choice of comparators. Section 3 builds the evaluative framework. Section 4 sets out the governance obligations Nigerian law imposes across licence categories. Section 5 evaluates those obligations against the framework. Section 6 draws on the United Kingdom, Kenya and Singapore. Section 7 derives reform proposals from the findings, and Section 8 concludes with implications for research, practice and society.

2. METHODOLOGY

The study combines doctrinal analysis, which answers RQ1 and RQ2, with functional comparative analysis, which answers RQ3. The law is stated as of 3rd October 2026.

¹⁶ Central Bank of Nigeria, *Revised Guidelines for Finance Companies in Nigeria* (April 2014) (FC Guidelines 2014) para 9; Central Bank of Nigeria, *Code of Corporate Governance for Finance Companies in Nigeria* (24 October 2018) <https://www.cbn.gov.ng/Out/2018/FPRD/FC.pdf> accessed 3 August 2026 (FC Code) paras 1.1, 2.1.4, 2.2.2.

2.1 Doctrinal analysis: sources and selection

The doctrinal analysis works from primary sources. These are the Companies and Allied Matters Act 2020 (CAMA), BOFIA, the Central Bank of Nigeria Act 2007, the Investments and Securities Act 2025, the Nigeria Data Protection Act 2023, the Nigerian Code of Corporate Governance 2018, and the governance, licensing, cybersecurity and consumer-protection instruments issued by the CBN, the Nigeria Data Protection Commission and the Federal Competition and Consumer Protection Commission.¹⁷ The CBN's power to issue such instruments rests on section 33(1) (b) of the Central Bank of Nigeria Act 2007, which empowers it to issue guidelines to any person or institution under its supervision.¹⁸

Instruments were selected by two criteria. They must be in force at the stated date, and they must impose obligations on the board, senior management or governance structures of firms providing deposit, payment, lending or account services through digital channels. Instruments regulating only transaction-level conduct are considered only where they also allocate governance responsibility. Each instrument was read for what it requires of the board, of identified

¹⁷ Companies and Allied Matters Act 2020 (CAMA 2020); BOFIA 2020; Central Bank of Nigeria Act 2007; Investments and Securities Act 2025; Nigeria Data Protection Act 2023; Federal Competition and Consumer Protection Act 2018; NCCG (n 9); CBN Guidelines 2023 (n 9); Central Bank of Nigeria, *Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Banks* (31 May 2024) (CBN Cybersecurity Framework 2024); MFB Code (n 15); FC Code (n 16); FC Guidelines 2014 (n 16); Microfinance Policy 2005 (n 13); Nigeria Data Protection Commission, *Nigeria Data Protection Act 2023: General Application and Implementation Directive (GAID) 2025* (NDPC/NDP ACT-GAID/01/2025, 20 March 2025) (GAID); Digital, Electronic, Online, or Non-Traditional Consumer Lending Regulations 2025 (made under the Federal Competition and Consumer Protection Act 2018) (Consumer Lending Regulations 2025).

¹⁸ Central Bank of Nigeria Act 2007, s 33(1)(b).

individuals, and of internal structures. The results were then organised by licence category, so that variation across categories becomes visible. That variation is the evidence on which the licence-contingency thesis stands or falls.

In total, sixteen Nigerian instruments were analysed: seven statutes, the national governance code, six CBN instruments, and the data protection and consumer lending instruments of the NDPC and FCCPC. Each was coded against the five criteria developed in Section 3. A provision was recorded where it (i) assigned a responsibility to the board or to a named individual; (ii) specified the competence a board or its members must possess; (iii) required a committee, reporting line or assurance function; (iv) required attention to the interests of customers, depositors, borrowers or data subjects; or (v) cross-referred to, or deferred to, another regulator's regime. The absence of any such provision in an instrument was recorded as a finding in its own right, since the argument concerns gaps as much as content. The resulting matrix is summarised in Table 2, and the coding of each criterion is reported in Section 5.

Public enforcement statements are used as evidence of how obligations operate in supervisory practice, not as proof of governance failure within particular firms. Secondary literature is used to interpret the instruments and situate the analysis, never as authority for propositions of law that can be checked against the primary text.

2.2 Functional comparison: choice of comparators

The comparative analysis is functional.¹⁹ It asks how each comparator solves a shared problem: attaching appropriate governance obligations to firms that deliver financial services digitally. It does not compare institutions that merely share a name. Each comparator was thus chosen because it answers a different element of RQ3.

The United Kingdom is included for its approach to accountability. It's Senior Managers and Certification Regime assigns prescribed responsibilities to identified individuals.²⁰ It is also the historical source of much of Nigerian company law. Kenya is included as an African jurisdiction with extensive experience of mass-market digital financial services. It has also recently brought digital credit providers within a dedicated regime combining licensing with governance requirements.²¹ Singapore is included because it created a dedicated digital bank licence and pairs it with technology-risk guidance that places explicit responsibilities on boards.²² It therefore tests directly the intuitive response to the absence of a Nigerian digital bank licence, which is to create one.²³ South Africa's statutory coordination provisions in the Financial Sector Regulation Act 2017 are considered

¹⁹ Konrad Zweigert and Hein Kötz, *An Introduction to Comparative Law* (Tony Weir tr, 3rd edn, Clarendon Press 1998).

²⁰ Financial Services and Markets Act 2000, pt V, as amended by the Financial Services (Banking Reform) Act 2013 (FSMA 2000).

²¹ Central Bank of Kenya (Digital Credit Providers) Regulations 2022, Legal Notice No 46 of 2022 (Digital Credit Providers Regulations 2022).

²² Monetary Authority of Singapore, 'Digital Full Bank Framework' (Annex A to MAS press release, 28 June 2019) (MAS Digital Full Bank Framework); Monetary Authority of Singapore, *Technology Risk Management Guidelines* (January 2021) (MAS TRM Guidelines).

²³ Ofo, Ngwoke and Ekwe (n 1).

in the discussion of regulatory coherence, but South Africa is not a principal comparator.²⁴

The analysis takes seriously the limits of legal transplantation.²⁵ The comparators differ from Nigeria in supervisory capacity, market structure and regulatory resources. Section 6 therefore treats foreign solutions as evidence of what works under stated conditions, not as models to be copied.

2.3 Limitations

The study has three limitations. It does not measure governance practice within firms, which would require empirical access the study does not claim. It relies on publicly available enforcement information, which is incomplete. And CBN instruments change frequently, so particular findings may be overtaken. The licence-contingency thesis does not depend on any single instrument, however, and should survive incremental change.

3. WHY FINTECH GOVERNANCE IS DIFFERENT, AND HOW TO EVALUATE IT

The framework combines two bodies of theory. Bank-governance exceptionalism explains why digital financial institutions warrant governance obligations beyond those of ordinary companies. Regulated self-governance explains how the law should secure those obligations. Together they yield five evaluative criteria, which Section 5 applies to Nigerian law. Each criterion is derived from the theory

²⁴ Financial Sector Regulation Act 9 of 2017 (South Africa).

²⁵ Otto Kahn-Freund, 'On Uses and Misuses of Comparative Law' (1974) 37 *Modern Law Review* 1; Daniel Berkowitz, Katharina Pistor and Jean-François Richard, 'The Transplant Effect' (2003) 51 *American Journal of Comparative Law* 163.

and then put to the instruments as a question, so that the theory does analytical work rather than serving as background.

3.1 Bank-governance exceptionalism

Agency theory begins from the conflict between shareholders as principals and managers as agents, and prescribes mechanisms that reduce agency costs.²⁶ Banks unsettle that starting point. Their creditors are mainly depositors, who are numerous, dispersed and poorly placed to monitor. Their leverage gives shareholders an incentive to take risks whose downside falls on depositors and, through contagion, on the wider system. Macey and O'Hara²⁷ therefore argue that bank directors' fiduciary duties should extend beyond shareholders to creditors, and that directors should take solvency risk explicitly into account or face personal liability. The Basel Committee's corporate governance principles build on similar reasoning. They make the board ultimately responsible for the bank's risk management and compliance obligations, and require board members to be qualified individually and collectively. They also call for an independent risk-management function under a chief risk officer with access to the board.²⁸ Importantly for present purposes, the Committee states that implementation should be commensurate with the bank's size, complexity, and risk profile and business model.²⁹ The principle of proportionality is thus tied to risk and business model, not to legal form.

²⁶ Michael C Jensen and William H Meckling, 'Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure' (1976) 3 *Journal of Financial Economics* 305.

²⁷ Macey and O'Hara (n 5).

²⁸ BCBS (n 5) principles 1, 2 and 6.

²⁹ *ibid.*

The question for this paper is whether exceptionalism extends to fintech. The argument advanced here is that it extends to activity rather than to legal form. A microfinance-licensed digital bank that takes deposits from millions of retail customers raises the depositor problem directly. A payment firm that holds customer funds in transit, or sits at a node in the payment system, raises the contagion and public-confidence problems even if it takes no deposits. A digital lender raises neither in the same form, but it raises acute problems of conduct towards consumers and of data use. Technology dependence adds a dimension that bank-governance theory did not originally anticipate. For an institution with no branches, operational and cyber failure is a failure of the whole business rather than of one channel. If bank-governance exceptionalism is grounded in these risks, governance obligations should track them. Whether they do so in Nigeria is the test Section 5 applies.

On this account stakeholder theory does analytical work rather than serving as background.³⁰ Depositors, payment users and data subjects are stakeholders whose interests the exceptionalist argument says boards must weigh. Nigerian company law recognises them only partially. Section 305(3) of CAMA requires directors to have regard to the impact of the company's operations on the environment in the community where it operates, and section 305(4) to the interests of its employees and members. Neither provision mentions customers or creditors. For a deposit-taking institution that silence is precisely the problem bank-governance exceptionalism identifies, and sector codes rather than the statute have had to address it. The 2018 microfinance code, for example, states that directors owe the bank a duty to act in

³⁰ R Edward Freeman, *Strategic Management: A Stakeholder Approach* (CUP 2010).

the interests of its shareholders ‘and other stakeholders’.³¹ Stewardship theory, which presents managers as aligned with the firm,³² is treated more sceptically. It describes founder-led fintechs plausibly, but alignment with growth does not secure alignment with depositors or regulators.

3.2 Regulated self-governance

The second body of theory concerns regulatory technique. Fintech firms change products faster than regulators can write rules, and their technology risks are often better understood inside the firm than by the supervisor. Ayres and Braithwaite³³ propose enforced self-regulation for such conditions: firms write and operate their own rules within a framework the regulator requires and can enforce, backed by an escalating enforcement pyramid. Principles-based regulation shares this logic but carries known weaknesses. It depends on the regulator’s capacity to supervise judgements, and on firms’ willingness to interpret principles in good faith.³⁴ The fintech literature reaches a compatible conclusion from another direction. It argues that the fragmentation of market participants and the growing use of technology call for a proportionate regime, reached through sequential reform that moves beyond sandboxes towards digitally enabled ‘smart’ regulation.³⁵

³¹ MFB Code (n 15) para 2.1.1; see also FC Code (n 16) para 2.1.1.

³² James H Davis, F David Schoorman and Lex Donaldson, ‘Toward a Stewardship Theory of Management’ (1997) 22 *Academy of Management Review* 20.

³³ Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (OUP 1992).

³⁴ Julia Black, ‘Forms and Paradoxes of Principles-Based Regulation’ (2008) 3 *Capital Markets Law Journal* 425.

³⁵ Zetzsche and others (n 3).

Two implications follow for evaluation. First, governance obligations must be specific enough to allocate responsibility. A general duty to manage risk, owed by no one in particular, is the absence of regulated self-governance, not an instance of it. Second, the regulatory system must be coherent enough that a firm's internal governance answers to a consistent set of expectations. A firm accountable to several regulators with different expectations, or to none for a given risk, cannot meaningfully govern itself against them.

3.3 Five evaluative criteria

The two theories yield the following criteria (Table 1). Each is stated as a question that can be put to the Nigerian instruments and answered from their text.

Table 1. Evaluative criteria

Criterion	Theoretical source	Question put to Nigerian law
C1 Allocation of accountability	Regulated self-governance; bank exceptionalism	Does the law identify a board or individual responsible for technology, cyber and data risk?
C2 Board competence	Bank exceptionalism; BCBS Principle 2	Does the law require the board collectively to possess competence in the firm's core technology risks?
C3 Risk oversight architecture	Bank exceptionalism; BCBS Principles 3 and 6	Does the law require board-level structures, reporting lines and independent assurance for those risks?
C4 Stakeholder protection	Stakeholder theory; bank exceptionalism	Does the law require the board to oversee outcomes for depositors, payment users, borrowers and data subjects?
C5 Regulatory coherence	Regulated self-governance; BCBS proportionality	Do obligations attach consistently to equivalent activities, whatever the licence or regulator?

Source: Developed by the author from the theoretical framework in section 3.

Criteria C1 to C4 ask whether the right obligations exist. Criterion C5 asks whether they attach to the right firms, and is therefore the direct test of licence-contingency. The other criteria are applied separately to each licence category, so that variation in the answers is itself evidence for or against the central claim. Long-term outcomes for consumers and financial inclusion are captured within C4.

4. GOVERNANCE OBLIGATIONS ACROSS LICENCE CATEGORIES

This section answers RQ1. Board-level governance obligations for Nigerian digital financial institutions come from four layers: general company law, the national governance code, sector-specific CBN instruments, and activity-based overlays administered by other regulators. Which layers apply depends first on the licence a firm holds.

4.1 General company law

Every company, whatever its business, is subject to CAMA. Every company that is not a small company must have at least two directors.³⁶ Directors owe fiduciary duties of good faith³⁷ and must act in what they believe to be the best interests of the company as a whole.³⁸ They must also exercise the care, diligence and skill that ‘a reasonably prudent director would exercise in comparable

³⁶ CAMA 2020, s 271(1).

³⁷ *ibid* s 305(1).

³⁸ *ibid* s 305(3).

circumstances'.³⁹ A director may not delegate powers in a manner amounting to 'an abdication of duty'.⁴⁰

Three features of this layer matter for fintech. First, its structural requirements are aimed at public companies. Independent directors are required only in public companies,⁴¹ as is the audit committee to which auditors must report.⁴² Most fintech operators are private companies, so neither applies to them. Second, the duty of care is an ex post standard enforced through litigation. It is not an ex ante requirement to build any particular oversight structure. Third, the section 305 duties are 'enforceable against a director by the company',⁴³ not by customers or depositors. For a fintech with no CBN licence, this layer is the whole of its board-level governance law.

4.2 The national code

The Nigerian Code of Corporate Governance 2018 (NCCG), issued under the authority of the Financial Reporting Council (FRC), contains Nigeria's most explicit general statement on technology governance.⁴⁴ It recommends that the board provide 'oversight over Information Technology governance'.⁴⁵ It also recommends that the risk committee review, at least annually, an IT data governance framework covering cyber threats, third-party IT providers and periodic independent assurance.⁴⁶ The NCCG is principles-based, applied on an 'Apply and

³⁹ *ibid* s 308(1).

⁴⁰ *ibid* s 305(7).

⁴¹ *ibid* s 275, as amended by the Business Facilitation (Miscellaneous Provisions) Act 2022, sch, pt I, para 14.

⁴² *ibid* s 404(2).

⁴³ *ibid* s 305(9).

⁴⁴ NCCG (n 9).

⁴⁵ *ibid* Recommended Practice 1.10.

⁴⁶ *ibid* Recommended Practice 11.5.6.6.

explain' basis, and monitored by the FRC through sectoral regulators.⁴⁷ Its committee recommendations are similarly flexible. The board should establish committees for nomination and governance, remuneration, audit and risk management,⁴⁸ but may combine their responsibilities 'taking into consideration the size, needs and other requirements of the Company'.⁴⁹ Its practical force therefore depends on whether a sectoral instrument adopts it. The 2023 Guidelines do so expressly for banks.⁵⁰ Neither the microfinance code nor the finance company code refers to it.

4.3 Sector-specific CBN instruments

The CBN's instruments rest on its power under section 33(1) (b) of the Central Bank of Nigeria Act 2007 to issue guidelines to institutions under its supervision.⁵¹ They divide into two tiers.

The upper tier covers commercial, merchant, non-interest and payment service banks. The 2023 Guidelines require at least two non-executive directors, one of them independent, with knowledge and experience of innovative financial technology, ICT and/or cyber security.⁵² They require a board-approved IT framework covering data confidentiality, network security, third-party connections and incident response,⁵³ and they prohibit commercial, merchant and non-interest banks from combining the risk and audit committees.⁵⁴ Payment service banks must in addition establish a board committee for ICT and

⁴⁷ *ibid* Introduction, pts C and D.

⁴⁸ *ibid* Recommended Practice 11.1.6.

⁴⁹ *ibid* Recommended Practice 11.1.7.

⁵⁰ CBN Guidelines 2023 (n 9) Application section.

⁵¹ Central Bank of Nigeria Act 2007, s 33(1)(b).

⁵² CBN Guidelines 2023 (n 9) s 1.7.

⁵³ *ibid* s 2.9.

⁵⁴ *ibid* s 6.10.

cybersecurity,⁵⁵ and a majority of their audit committee must be knowledgeable in technology, ICT or cybersecurity.⁵⁶

The 2024 Risk-Based Cybersecurity Framework applies to the same four categories of bank.⁵⁷ It makes the board, acting through its risk or IT committee, responsible for the cybersecurity programme.⁵⁸ It requires the board to ensure the appointment of a chief information security officer and to receive quarterly reports on cyber risk, incidents and remediation.⁵⁹ It also requires a stand-alone cybersecurity budget and a cyber risk appetite within the enterprise risk framework.⁶⁰ Cyber incidents must be reported to the CBN within 24 hours of detection.⁶¹

The lower tier covers microfinance banks and finance companies. The microfinance code itself records why governance matters in this tier: it explains that by 2014 some licensed microfinance banks had become insolvent, 'a development largely attributed to poor governance practices and gross insider abuses'.⁶² Their 2018 codes are near-identical in structure. Board skills are tied to the general Approved Persons Regime.⁶³ At least two non-executive directors must have 'banking or related financial industry experience'.⁶⁴ The codes require risk management, audit, governance and credit committees, but allow risk and audit to be combined in unit and state microfinance banks and

⁵⁵ *ibid* s 6.6.

⁵⁶ *ibid* s 6.13(c).

⁵⁷ CBN Cybersecurity Framework 2024 (n 17) Introduction.

⁵⁸ *ibid* s 1.1.

⁵⁹ *ibid* s 1.1(viii)-(ix).

⁶⁰ *ibid* s 1.1(xi)-(xii).

⁶¹ *ibid* s 5.0(v).

⁶² MFB Code (n 15) para 1.0.

⁶³ *ibid* para 2.1.4; FC Code (n 16) para 2.1.4.

⁶⁴ *ibid* para 2.2.3; FC Code (n 16) para 2.2.2.

‘particularly in small’ finance companies.⁶⁵ Neither code contains any provision on information technology, cybersecurity or digital operations. Nor does the 2014 finance company guidelines’ governance section, which relies on the 2010 Prudential Guidelines and the 2011 Approved Persons Regime circular.⁶⁶

4.4 Activity-based overlays

Two regimes outside the CBN attach to activity rather than to licence. The Nigeria Data Protection Act 2023, implemented through the General Application and Implementation Directive (GAID), applies to any data controller.⁶⁷ In designating controllers ‘of major importance’, the Commission considers ‘data driven financial assets entrusted by data subjects’.⁶⁸ A data privacy impact assessment is mandatory for ‘financial services involving the processing of personal data through digital devices’.⁶⁹ Controllers of major importance must designate a data protection officer.⁷⁰ The GAID allocates these obligations to the controller and its data protection officer. It does not allocate them to the board.

The Digital, Electronic, Online, or Non-Traditional Consumer Lending Regulations 2025, made under the Federal Competition and Consumer Protection Act 2018, apply to unsecured lending by digital or other non-traditional means, whoever the lender is.⁷¹ Registration requires a profile of the board and key management.⁷² Parties must conduct

⁶⁵ *ibid* para 2.5.1; FC Code (n 16) para 2.5.1.

⁶⁶ FC Guidelines 2014 (n 16) para 9.

⁶⁷ NDPA 2023; GAID (n 17).

⁶⁸ GAID (n 17) art 8(3)(d).

⁶⁹ *ibid* art 28(3)(h).

⁷⁰ *ibid* art 7(i).

⁷¹ Consumer Lending Regulations 2025, reg 3.

⁷² *Ibid* reg 12(1)(g).

regular security audits and maintain plans for operational disruption.⁷³ Directors of a defaulting undertaking may be disqualified for up to five years.⁷⁴ Microfinance banks, however, apply for a waiver from registration.⁷⁵ Capital-market fintech activity falls to the Securities and Exchange Commission, whose 2025 statute extends to virtual asset service providers and digital asset operators.⁷⁶ The Commission's statutory objectives include contributing to 'the reduction of systemic risk' and promoting financial stability,⁷⁷ so that capital-market fintech is brought within a prudential as well as a conduct mandate. The governance consequences of that mandate for digital asset operators lie outside the scope of this paper, which concentrates on deposit, payment and lending activity.

A final route is indirect. Banks within the upper tier must not establish API connections with, or grant access to, organisations not licensed by the CBN without prior regulatory approval.⁷⁸ The framework explains the concern: connections through application programming interfaces expose banks to fraud, API compromise, unauthorised access and data breach.⁷⁹ Unlicensed fintechs are thus governed partly through the gatekeeping obligations of the banks they connect to, rather than through obligations on their own boards.

4.5 Summary

Table 2 consolidates the position. The pattern it shows is the subject of Section 5.

⁷³ Ibid reg 20.

⁷⁴ Ibid reg 27(2)(c).

⁷⁵ Ibid sch 5, para 4.

⁷⁶ Investments and Securities Act 2025, s 3(3)(b) and (i), sch 2, para 4.

⁷⁷ Ibid s 3(2)(d).

⁷⁸ CBN Cybersecurity Framework 2024 (n 17) s 4.8(3).

⁷⁹ Ibid s 4.7.

Table 2. Board-level governance obligations by licence category

Licence category	Governing instruments	Board size	Board technology competence	Board technology and cyber structure	Risk and audit committees
Commercial, merchant and non-interest banks	CAMA; NCCG; CBN Guidelines 2023; CBN Cybersecurity Framework 2024	7–15 (s 1.3)	At least two NEDs, one an INED (s 1.7; CBN Cybersecurity Framework 2024, s 1.1(i))	Board IT framework (s 2.9); CISO; quarterly cyber reporting (CBN Cybersecurity Framework 2024, s 1.1)	Must be separate (s 6.10)
Payment service banks	CAMA; NCCG; CBN Guidelines 2023; CBN Cybersecurity Framework 2024	7–13 (s 1.3)	As above; majority of audit committee (s 6.13(c))	Mandatory board ICT and cybersecurity committee (s 6.6); CISO; quarterly reporting	Separation not specified (s 6.10 applies to CMNIBs); risk function headed by a senior management officer (s 12.3)
Microfinance banks	CAMA; MFB Code	5–12 by category (para 2.2.1)	None specified; general banking experience (para 2.2.3)	None	May be combined in unit and state MFBs (para 2.5.1)
Finance companies	CAMA; FC Guidelines 2014; FC Code	5–9 (para 2.2.1)	None specified; general banking experience (para 2.2.2)	None	May be combined, particularly in small FCs (para 2.5.1)

Licence category	Governing instruments	Board size	Board technology competence	Board technology and cyber structure	Risk and audit committees
Fintechs without a CBN licence	CAMA; Consumer Lending Regulations 2025 if lending; NDPA/GAID	2 minimum, unless small (s 271)	None	None at board level; DPO for data controllers of major importance (GAID, art 7(i))	Not required for private companies

Sources: as cited in each cell. Section references in the first two rows are to CBN Guidelines 2023 unless otherwise stated; full citations are given in the footnotes and bibliography. CISO, chief information security officer; CMNIBs, commercial, merchant and non-interest banks; DPO, data protection officer; FCs, finance companies; INED, independent non-executive director; MFBs, microfinance banks; NEDs, non-executive directors.

5. EVALUATION: TESTING THE FRAMEWORK AGAINST THE FIVE CRITERIA

This section answers RQ2. Each criterion from Section 3.3 is applied to the instruments set out in Section 4, category by category. The findings are stated at the end of each subsection. Their common cause is then assessed under C5.

5.1 C1: Allocation of accountability

For the upper tier, the answer to C1 is clear. The cybersecurity framework places responsibility for the cybersecurity programme on the board, acting through its risk or IT committee. It also identifies an individual, the chief information security officer, whose appointment

the board must ensure and who must report to it quarterly.⁸⁰ The 2023 Guidelines add a board-approved IT framework.⁸¹ Responsibility for technology risk is thus allocated both collectively and individually.

For microfinance banks and finance companies, responsibility is allocated only in general terms. The board ‘shall approve the risk management policies’ and ensure their implementation.⁸² Nothing identifies technology, cyber or data risk as a board responsibility, or requires any individual to own it. For fintechs without a CBN licence, the only allocation is the collective statutory duty of care in section 308 of CAMA. The data protection regime allocates responsibility to a data protection officer,⁸³ a management-level role whose relationship to the board the GAID does not specify.

Finding 1. Board-level accountability for technology and cyber risk is allocated explicitly only to institutions holding a commercial, merchant, non-interest or payment service bank licence. Elsewhere it is either generic or absent.

5.2 C2: Board competence

The same division as noted above appears here. The 2023 Guidelines and the cybersecurity framework require at least two non-executive directors with knowledge and experience of innovative financial technology, ICT and/or cyber security.⁸⁴ For payment service banks a majority of the audit committee must have such knowledge.⁸⁵ The

⁸⁰ *ibid* s 1.1.

⁸¹ CBN Guidelines 2023 (n 9) s 2.9.

⁸² MFB Code (n 15) para 6.2; FC Code (n 16) para 6.2.

⁸³ GAID (n 17) art 7(i).

⁸⁴ CBN Guidelines 2023 (n 9) s 1.7; CBN Cybersecurity Framework 2024 (n 17) s 1.1(i).

⁸⁵ CBN Guidelines 2023 (n 9) s 6.13(c).

microfinance and finance company codes require instead that two non-executive directors have 'banking or related financial industry experience'.⁸⁶ That is a reasonable requirement for a lender whose principal risk is credit. It is not a requirement directed at an institution whose principal operational risk is technological. CAMA imposes no competence requirement at all. The section 308 standard of the 'reasonably prudent director' in 'comparable circumstances' calibrates the care expected of directors once they are appointed, not the expertise a board must contain.⁸⁷

The gap is not merely formal. The BCBS principles require board members to be qualified 'individually and collectively' in proportion to the 'size, complexity and risk profile' of the institution.⁸⁸ The lower-tier codes calibrate in a different way. Their proportionality runs by geographic authorisation category, unit, state or national, which determines board size, the number of independent directors and whether committees may be combined.⁸⁹ It does not run by customer numbers, deposit volumes or dependence on digital channels.

Finding 2. A requirement for board competence in technology attaches to licence category, and the codes' proportionality is calibrated to geography rather than to digital scale or risk.

5.3 C3: Risk-oversight architecture

The upper tier has a layered architecture. There are separate risk and audit committees for commercial, merchant and non-interest banks,⁹⁰

⁸⁶ MFB Code (n 15) para 2.2.3; FC Code (n 16) para 2.2.2.

⁸⁷ CAMA 2020, s 308(1).

⁸⁸ BCBS (n 5) principle 2.

⁸⁹ MFB Code (n 15) paras 2.2.1, 2.2.5, 2.5.1.

⁹⁰ CBN Guidelines 2023 (n 9) s 6.10.

and a dedicated ICT and cybersecurity committee for payment service banks.⁹¹ Quarterly cyber reporting to the board,⁹² a dedicated cyber budget, and a 24-hour incident reporting duty to the supervisor⁹³ complete it. The NCCG's recommended IT data governance framework, including periodic independent assurance, applies to these banks through the 2023 Guidelines.⁹⁴

The lower tier permits the opposite. Unit and state microfinance banks, and finance companies, may combine risk and audit in a single committee.⁹⁵ No technology committee, cyber reporting line or incident-reporting duty appears in either code. The assurance functions are also thinner. In unit and state microfinance banks the offices of chief compliance officer and internal auditor may be combined,⁹⁶ and the finance company code permits the same combination in any finance company.⁹⁷ The BCBS principles, by contrast, treat an independent compliance function reporting to the board and an internal audit function independent of the activities it audits as distinct elements of sound governance.⁹⁸ A payment service bank is therefore subject to a more demanding technology-oversight architecture than the microfinance bank, which takes deposits and extends credit.⁹⁹

⁹¹ *ibid* s 6.6.

⁹² CBN Cybersecurity Framework 2024 (n 17) s 1.1(viii).

⁹³ *ibid* s 5.0(v).

⁹⁴ NCCG (n 9) Recommended Practice 11.5.6.6; CBN Guidelines 2023 (n 9) Application section.

⁹⁵ MFB Code (n 15) para 2.5.1; FC Code (n 16) para 2.5.1.

⁹⁶ MFB Code (n 15) para 5.2.8.

⁹⁷ FC Code (n 16) para 5.2.8.

⁹⁸ BCBS (n 5) principles 9 and 10.

⁹⁹ Microfinance Policy 2005 (n 13) paras 11.5, 13.3.

This matters because the microfinance licence is reported to be the vehicle for several of Nigeria's largest digital retail operators.¹⁰⁰ Supervisory practice is consistent with a perceived governance gap at this level. Press reports in December 2024, citing unnamed sources, stated that the CBN had fined two large fintech operators ₦1 billion each in the second quarter of 2024 following routine audits. The same reports noted concerns about know-your-customer compliance among fintechs operating under microfinance licences.¹⁰¹ One of the two firms publicly denied having been fined.¹⁰² These reports are therefore treated here as evidence of supervisory concern, not as established findings of governance failure in any particular firm.

Finding 3. The institutions permitted the thinnest board-level oversight architecture include those operating digital deposit-taking businesses at scale. The architecture required by law is inversely related to the digital risk carried.

5.4 C4: Stakeholder protection

Here the picture is more mixed, and this matters for the thesis. Nigerian law does protect digital-finance users through regimes that attach to activity rather than licence. The consumer lending regulations apply to unsecured digital lending by any lender.¹⁰³ They require security audits and operational resilience planning¹⁰⁴ and expose

¹⁰⁰ Ofo, Ngwoke and Ekwe (n 1); TechCabal, 'CBN Fines Moniepoint and OPay ₦1 Billion Each as Nigeria Tightens Fintech Regulation' (*TechCabal*, 10 December 2024) <https://techcabal.com/2024/12/10/cbn-fines-moniepoint-and-opay/> accessed 4 July 2026.

¹⁰¹ TechCabal (n 100).

¹⁰² *ibid.*

¹⁰³ Consumer Lending Regulations 2025, reg 3.

¹⁰⁴ *ibid* reg 20.

directors to disqualification.¹⁰⁵ The GAID mandates impact assessments for digital financial services.¹⁰⁶ In C4 terms, Nigerian law is partly activity-based.

Three limitations remain. First, these regimes operate on the firm and its conduct, not on board oversight. They require outcomes but do not require the board to receive information about complaints, data incidents or impact assessments, or to be accountable for them. Director disqualification under the lending regulations is an ex post sanction, not an ex ante allocation of oversight. Second, company law gives customers and depositors no standing. CAMA's list of interests directors must consider does not include them,¹⁰⁷ and the duties are enforceable only by the company.¹⁰⁸ The sector codes add only a general reference to 'other stakeholders', a whistleblowing channel and an expectation of corporate social responsibility.¹⁰⁹ Third, the activity-based overlay is itself partly licence-contingent. Microfinance banks may seek a waiver from registration under the lending regulations.¹¹⁰

Finding 4. Consumer and data protection obligations attach largely to activity, but they are not translated into board-level oversight, and stakeholder interests have no standing in directors' statutory duties.

5.5 C5: Regulatory coherence and the licence-contingency thesis

Findings 1 to 3 establish that board-level technology governance in Nigeria varies with licence category. Finding 4 qualifies the picture:

¹⁰⁵ *ibid* reg 27(2)(c).

¹⁰⁶ GAID (n 17) art 28(3)(h).

¹⁰⁷ CAMA 2020, s 305(3)–(4).

¹⁰⁸ *ibid* s 305(9).

¹⁰⁹ MFB Code (n 15) paras 2.1.1, 4.1–4.3.

¹¹⁰ Consumer Lending Regulations 2025, sch 5, para 4.

conduct and data obligations follow activity. The result is a two-track system. One track, board-level prudential and technology governance, is licence-contingent. The other, conduct and data protection, is activity-based but operates below board level. The two tracks are administered by different regulators. The CBN governance codes examined do not refer to the consumer lending regulations or to the GAID. The cybersecurity framework mentions the Nigeria Data Protection Act only as related legislation to be read alongside it.¹¹¹ The lending regulations, for their part, defer to the CBN licence through the microfinance waiver. Nothing in the instruments examined requires a firm's board to see both tracks together.

Armour and others¹¹² explain the predictable consequence. Regulatory arbitrage arises whenever a system provides 'two different regimes' for formally different products or services that perform the same economic function.¹¹³ A digital deposit-and-payments business can be organised under a payment service bank licence or a microfinance licence, and the board-level obligations differ sharply between them, so the arbitrage incentive Armour and others describe is present. Whether firms in fact choose licences for this reason is an empirical question beyond the scope of a doctrinal study. The incentive, however, is a feature of the legal design. The only mechanism reaching unlicensed fintechs' technology risk at all is the indirect gatekeeping duty placed on their bank counterparties.¹¹⁴ That governs the connection, not the fintech's board.

¹¹¹ CBN Cybersecurity Framework 2024 (n 17) Introduction.

¹¹² John Armour and others, 'Principles of Financial Regulation' (2016) European Corporate Governance Institute Law Working Paper No 277/2014 http://ssrn.com/abstract_id=2526740, 13.

¹¹³ Ibid 13.

¹¹⁴ CBN Cybersecurity Framework 2024 (n 17) s 4.8(3).

Early supervisory thinking had already recognised that an internet-only bank faces the same risks as a traditional bank, some of them heightened, including the possibility of ‘virtual bank runs’.¹¹⁵ Nigerian law recognises digital banking as banking¹¹⁶ but has not drawn the governance consequence.

Finding 5. The licence-contingency thesis is confirmed for board-level technology governance and qualified for conduct and data protection. The incoherence lies in the absence of any mechanism connecting the two tracks at board level, and in proportionality calibrated to licence and geography rather than to activity and scale.

5.6 Objections considered

Three objections to the licence-contingency critique deserve an answer.

The first is that the gradient is deliberate proportionality. Microfinance banks were conceived as small institutions serving local markets, and lighter governance requirements spare them costs they could not bear. The objection is sound as to its premise but not its application. Proportionality is a principle of calibration to risk, and the BCBS formulation ties it to size, complexity, risk profile and business model.¹¹⁷ A licence category is a proxy for those things only when the institutions within it resemble one another. Once a single licence category contains both a rural unit microfinance bank and a digital operator serving millions of customers, the proxy fails. The reform

¹¹⁵ Douglas W Arner, János Barberis and Ross P Buckley, ‘The Evolution of FinTech: A New Post-Crisis Paradigm?’ (2015) University of Hong Kong Faculty of Law Research Paper No 2015/047 <https://ssrn.com/abstract=2676553>, 13.

¹¹⁶ BOFIA 2020, s 131.

¹¹⁷ BCBS (n 5).

proposed in Section 7.1 preserves proportionality by replacing the proxy with direct measures of scale.

The second objection draws on the innovation trilemma. Extending upper-tier obligations to more firms might buy market integrity at the cost of innovation.¹¹⁸ The answer lies in what is extended. The obligations at issue concern who on the board understands and answers for technology risk, not which products a firm may offer or how much capital it must hold. Requirements of this kind are closer to the conditions of responsible experimentation than to barriers against it. They are also the internal counterpart of the enforced self-regulation that makes regulatory flexibility defensible in the first place.¹¹⁹ A regulator can more safely relax product rules for a firm whose board is equipped to govern the risks than for one whose board is not.

The third objection is that the CBN already possesses ample discretion. It approves directors, can attach conditions to licences and can intervene through supervision, so the formal content of the codes matters less than supervisory practice. Supervisory discretion is real, and this study does not measure how it is exercised. But discretion exercised case by case does not allocate accountability in advance, does not tell a board what is expected of it, and is not visible to depositors, investors or other regulators. The criteria in Section 3 rest on the premise, drawn from regulated self-governance, that obligations must be specific enough to allocate responsibility (Section 3.2). Discretion supplements that allocation but cannot substitute for it, least of all in a setting where enforcement capacity is itself constrained.¹²⁰

¹¹⁸ Brummer and Yadav (n 4).

¹¹⁹ Ayres and Braithwaite (n 33).

¹²⁰ Adegbite (n 6).

None of these objections displaces the findings. Each, however, sharpens the reform design: thresholds rather than labels, governance rather than product restrictions, and published obligations rather than case-by-case discretion.

6. COMPARATIVE ANALYSIS: ATTACHING GOVERNANCE TO ACTIVITY AND RISK

This section answers RQ3. Each comparator is examined for how it attaches governance obligations to digital financial activity, and for the conditions on which its approach depends.

6.1 United Kingdom: individual accountability across all authorised firms

The United Kingdom's Senior Managers and Certification Regime was introduced for banks following the Financial Services (Banking Reform) Act 2013.¹²¹ From 9 December 2019 it was extended to all firms authorised under the Financial Services and Markets Act 2000.¹²² Under the regime, individuals performing senior management functions require regulatory approval and must hold a statement of responsibilities. Firms must allocate prescribed responsibilities among them, and each senior manager owes a duty of responsibility for their areas.¹²³ The regime applies in three tiers, limited, core and enhanced, according to the size and complexity of the firm.

Two features answer the Nigerian findings. First, accountability attaches to authorisation as such, whatever the type of permission held. The individual responsible for a risk can be identified in every

¹²¹ Financial Services (Banking Reform) Act 2013.

¹²² Financial Conduct Authority, *Extending the Senior Managers & Certification Regime to FCA Firms: Final Rules* (PS18/14, 2018) (FCA PS18/14).

¹²³ *ibid.*

authorised firm, which answers C1. Second, the regime's proportionality runs by firm size and complexity rather than by permission category, which is the calibration Finding 2 shows the Nigerian lower-tier codes lack. The limitation for transfer is supervisory capacity. Pre-approval and ongoing assessment of senior managers across a large population of firms requires sustained regulatory resources.

6.2 Kenya: an activity-based perimeter with person-based controls

Kenya's Digital Credit Providers Regulations 2022 define their perimeter by activity.¹²⁴ No person may carry on digital credit business in Kenya unless licensed by the Central Bank of Kenya, or unless that business is regulated under another written law.¹²⁵ No person may be a significant shareholder, director, chief executive officer or senior officer of a provider unless the Bank has certified them fit and proper.¹²⁶ Directors are also personally bound by the duty to protect the confidentiality of customer information and transactions.¹²⁷ The criteria include 'relevant qualification, knowledge, skills and experience'.¹²⁸ New products and variations require the Bank's prior approval.¹²⁹ The Bank may suspend non-compliant directors or disqualify them from any position in a licensed or financial institution in Kenya.¹³⁰

Kenya thus answers C5 more directly than Nigeria does. The activity of digital lending brings the firm and its directors within prudential

¹²⁴ Digital Credit Providers Regulations 2022.

¹²⁵ *ibid* reg 4(1).

¹²⁶ *ibid* reg 7(2).

¹²⁷ *ibid* reg 13(3).

¹²⁸ *ibid* sch 3, pt A.

¹²⁹ *ibid* reg 17(1).

¹³⁰ *ibid* reg 37.

supervision, whatever corporate form the firm takes. Nigeria's nearest equivalent, the FCCPC lending regulations, likewise defines its perimeter by activity, but it does so through a consumer-protection regulator rather than a prudential one.¹³¹ The Kenyan regulations are, however, thin on governance content. The governance Part requires only that a provider 'practice sound corporate governance' based on ethics, integrity and sound risk management.¹³² It contains no technology-competence or committee requirement comparable to the Nigerian 2023 Guidelines. Kenya therefore offers a model for the perimeter and for person-based controls (C1, C5), but not for oversight architecture (C3).

6.3 Singapore: a digital licence that calibrates entry, not governance

Singapore is an obvious reference point for any proposal to create a dedicated digital bank licence. In 2019 the Monetary Authority of Singapore (MAS) created digital full bank and digital wholesale bank licences. A digital full bank enters in a restricted first stage, subject to caps on deposits and a lower capital requirement. It graduates to full status, with a minimum paid-up capital of S\$1.5 billion, once it has met prescribed milestones.¹³³ The digital licence is thus an instrument for calibrating entry: capital, deposit caps and permitted activities.

Board-level technology governance in Singapore does not depend on that licence. The MAS Technology Risk Management Guidelines apply broadly to financial institutions regulated by MAS.¹³⁴ They expect both the board and senior management to include members

¹³¹ Consumer Lending Regulations 2025, reg 3.

¹³² Digital Credit Providers Regulations 2022, reg 11.

¹³³ MAS Digital Full Bank Framework (n 22).

¹³⁴ MAS TRM Guidelines (n 22).

with the knowledge to understand and manage technology risk, including cyber risk. They also expect the board and senior management to ensure the appointment of a chief information officer and a chief information security officer.¹³⁵ The guidelines are not legally binding, but observance is taken into account in MAS's risk assessment of the institution.¹³⁶

The Singapore lesson is therefore more precise than a simple call for a digital licence would suggest. Ofo, Ngwoke and Ekwe¹³⁷ highlight the absence of a digital bank licence in Nigeria, and creating one is the intuitive response. Singapore shows that such a licence can manage entry risk, but that technology governance is secured by guidance attaching to regulated status across institutions. A Nigerian digital bank licence would not by itself cure licence-contingency. It would add another category unless technology-governance obligations were detached from licence type.

6.4 South Africa: a statutory duty to coordinate

Finding 5 locates part of the Nigerian problem in the absence of any mechanism connecting the prudential and conduct tracks. South Africa's Financial Sector Regulation Act 2017 addresses this by statute.¹³⁸ Financial sector regulators and the Reserve Bank 'must co-operate and collaborate' when performing their functions under financial sector laws, the National Credit Act and the Financial Intelligence Centre Act.¹³⁹ Memoranda of understanding give that duty operational form.¹⁴⁰ The Act also establishes a Financial System

¹³⁵ *ibid.*

¹³⁶ *ibid.*

¹³⁷ Ofo, Ngwoke and Ekwe (n 1).

¹³⁸ Financial Sector Regulation Act 2017.

¹³⁹ *ibid* s 76(1).

¹⁴⁰ *ibid* s 77.

Council of Regulators, whose objective is to facilitate co-operation, collaboration and, where appropriate, ‘consistency of action’ among its members.¹⁴¹ The fintech literature identifies the same need. Brummer and Yadav¹⁴² note that regulators’ creative responses to fintech remain limited by insufficient international and even domestic coordination. Allen¹⁴³ shows that a fragmented regulatory architecture complicates even the design of a sandbox.

6.5 Transferability

The comparators share one feature that Nigeria lacks: in each, the obligation follows the activity or the regulated status, not the licence label. They also share demanding preconditions. Person-based approval regimes and principles-based guidance depend on supervisory capacity and on firms’ willingness to apply principles in good faith.¹⁴⁴ In a setting where enforcement and market discipline are weak,¹⁴⁵ transplanted models may not work as they do at home.¹⁴⁶ Two features of the Nigerian framework reduce this risk. First, an approved-persons regime already exists and is embedded in the lower-tier codes.¹⁴⁷ Second, the substantive technology-governance standards already exist in the 2023 Guidelines and the 2024 cybersecurity framework. The reform task is therefore one of extension and connection rather than invention, which Section 7 takes up.

¹⁴¹ *ibid* s 79(1)-(2).

¹⁴² Brummer and Yadav (n 4) 307.

¹⁴³ Allen (n 3).

¹⁴⁴ Black (n 34).

¹⁴⁵ Adegbite (n 6).

¹⁴⁶ Kahn-Freund (n 25); Berkowitz, Pistor and Richard (n 25).

¹⁴⁷ MFB Code (n 15) para 2.1.4; FC Code (n 16) para 2.1.4; FC Guidelines 2014 (n 16) para 9.1.

7. REFORM: DETACHING GOVERNANCE FROM THE LICENCE

The reforms below follow from the findings. Each is tied to the finding and criterion it addresses, and each is designed to work within existing legal powers where possible. The governing principle is drawn from Section 3 and confirmed by the comparators: board-level technology governance should attach to activity and scale, and the licence should be used to calibrate entry rather than to determine governance.

7.1 An activity-and-scale trigger for technology governance (Findings 1-3; C1-C3)

The CBN should extend the technology-governance core of the upper tier to every CBN-licensed institution that crosses defined thresholds, whatever its licence category. That core comprises board technology competence,¹⁴⁸ a board-approved IT framework,¹⁴⁹ and the board responsibilities, chief information security officer, quarterly reporting and incident-reporting duties of the cybersecurity framework.¹⁵⁰ Thresholds should be expressed in measures of digital risk, such as the number of retail accounts, the value of deposits or transactions processed through digital channels, or the absence of a branch network. They should not be expressed in geographic authorisation category. The CBN can do this by guideline under section 33(1)(b) of the Central Bank of Nigeria Act 2007, without new legislation.¹⁵¹ Proportionality would be preserved: small unit microfinance banks below the thresholds would remain under the existing codes, but scale would bring the upper-tier obligations with it. This mirrors the tiering

¹⁴⁸ CBN Guidelines 2023 (n 9) s 1.7.

¹⁴⁹ *ibid* s 2.9.

¹⁵⁰ CBN Cybersecurity Framework 2024 (n 17) ss 1.1, 5.0.

¹⁵¹ Central Bank of Nigeria Act 2007, s 33(1)(b).

by size and complexity in the United Kingdom’s accountability regime¹⁵² and the BCBS principle that governance should be commensurate with risk profile and business model.¹⁵³

7.2 A prescribed technology responsibility (Finding 1; C1)

Every CBN-licensed institution should be required to allocate responsibility for technology, cyber and data risk to an identified individual whose appointment is subject to the Approved Persons Regime. In the upper tier this already occurs through the chief information security officer.¹⁵⁴ In the lower tier it would close the gap identified in Section 5.1. The model is the UK prescribed-responsibilities approach,¹⁵⁵ scaled down. It requires one designated person and a written statement of what that person is responsible for, not the full UK apparatus. Because the Approved Persons Regime already applies to microfinance banks and finance companies,¹⁵⁶ this is an extension of an existing instrument rather than a new one.

7.3 Technology competence in fit-and-proper criteria (Finding 2; C2)

The competence criteria applied to directors of digital-first institutions should expressly include knowledge of technology and cyber risk. The lower-tier codes’ requirement of ‘banking or related financial industry experience’ should be supplemented accordingly.¹⁵⁷ Kenya’s fit-and-proper criteria, which assess ‘relevant qualification, knowledge, skills and experience’ at the point of approval,¹⁵⁸ and Singapore’s

¹⁵² FCA PS18/14 (n 122).

¹⁵³ BCBS (n 5).

¹⁵⁴ CBN Cybersecurity Framework 2024 (n 17) s 1.1(ix).

¹⁵⁵ FCA PS18/14 (n 122).

¹⁵⁶ MFB Code (n 15) para 2.1.4; FC Code (n 16) para 2.1.4.

¹⁵⁷ MFB Code (n 15) para 2.2.3; FC Code (n 16) para 2.2.2.

¹⁵⁸ Digital Credit Providers Regulations 2022, sch 3, pt A.

expectation that boards include members able to understand technology risk,¹⁵⁹ show that this can be done through approval criteria rather than rigid board-composition quotas.

7.4 Board oversight of conduct and data outcomes (Finding 4; C4)

The activity-based conduct and data regimes should be connected to the board. The CBN codes should require the boards of institutions above the threshold to receive, at least annually, reports on consumer complaints and their resolution, on data incidents, and on the outcomes of data privacy impact assessments mandated by the GAID for digital financial services.¹⁶⁰ The FCCPC and NDPC could make a parallel requirement for firms within their own perimeters. In addition, the sector codes' reference to 'other stakeholders'¹⁶¹ should name depositors and customers expressly. This would give the bank-governance exceptionalist argument¹⁶² concrete expression in Nigerian regulatory text, without amending CAMA's general duties.

7.5 A coordination duty and forum (Finding 5; C5)

The CBN, the SEC, the FCCPC and the NDPC should be placed under a duty to coordinate on fintech governance. That duty should be supported by memoranda of understanding and a standing council with a mandate for consistency of action, on the model of sections 76, 77 and 79 of South Africa's Financial Sector Regulation Act 2017.¹⁶³ A statutory duty would be the most durable form. An inter-agency memorandum is the realistic first step. Its first tasks should include reconciling the microfinance waiver under the consumer lending

¹⁵⁹ MAS TRM Guidelines (n 22).

¹⁶⁰ GAID (n 17) art 28(3)(h).

¹⁶¹ MFB Code (n 15) para 2.1.1; FC Code (n 16) para 2.1.1.

¹⁶² Macey and O'Hara (n 5).

¹⁶³ Financial Sector Regulation Act 2017, ss 76, 77 and 79.

regulations¹⁶⁴ with the CBN's own conduct expectations, and agreeing common board-level reporting requirements under Section 7.4.

7.6 Reconsidering the digital bank licence

A dedicated digital bank licence is not proposed as the primary reform. Section 6.3 shows that Singapore's digital licence calibrates entry, while its technology governance attaches to regulated status. A Nigerian digital licence would be useful for staged entry, with deposit caps and capital that rise as a firm graduate.¹⁶⁵ It should follow, not replace, the reforms in Sections 7.1 to 7.5. Otherwise, it would add one more licence category to a system whose problem is that governance depends on licence category.

7.7 Sequencing and capacity

The reforms are ordered by feasibility. Reforms 7.1 to 7.4 can be made by guideline and code amendment under existing powers. Reform 7.5 requires agreement among agencies and, ultimately, legislation. Given the capacity constraints identified in Section 6.5, the thresholds in Section 7.1 should initially be set so as to capture the small number of institutions with the largest digital retail footprints, where supervisory attention yields the greatest reduction in risk.

¹⁶⁴ Consumer Lending Regulations 2025, sch 5, para 4.

¹⁶⁵ MAS Digital Full Bank Framework (n 22).

Table 3. Findings, criteria and reforms

Finding	Criterion	Reform	Legal basis
1. Accountability allocated only in upper tier	C1	7.1; 7.2	CBN Act 2007, s 33(1)(b); Approved Persons Regime
2. Competence tied to licence; proportionality by geography	C2	7.1; 7.3	CBN Act 2007, s 33(1)(b)
3. Oversight architecture inverse to digital risk	C3	7.1	CBN Act 2007, s 33(1)(b)
4. Conduct and data obligations not translated to board	C4	7.4	CBN codes; FCCPC and NDPC instruments
5. Two disconnected tracks	C5	7.5; 7.6	Inter-agency MoU; legislation in the longer term

Source: Developed by the author from the findings in section 5 and the reforms in section 7.

8. CONCLUSION

This paper asked how Nigerian law allocates board-level governance obligations to digital financial institutions, and whether that allocation matches the risks they generate. The answer to *RQ1* is that obligations come in four layers and that the licence determines which layers apply. Commercial, merchant, non-interest and payment service banks are subject to explicit board-level technology governance under the 2023 Guidelines and the 2024 cybersecurity framework. Microfinance banks and finance companies are governed by 2018 codes containing no technology provision at all. Fintechs without a CBN licence answer only to general company law at board level.

The answer to *RQ2* is that licence-contingency is confirmed for board-level technology governance and qualified for conduct and data

protection. Accountability, competence and oversight architecture for technology risk all vary by licence category. The proportionality built into the lower-tier codes runs by geography rather than by digital scale. Consumer-lending and data-protection obligations do attach to activity, but they operate below board level and are administered separately from the prudential codes. The result is two tracks with no point at which a board must see both.

The answer to *RQ3* is that the comparators attach governance to activity or regulated status rather than to the licence label. The United Kingdom does so through individual accountability across all authorised firms, Kenya through an activity-defined perimeter with person-based approval, and Singapore through technology-risk guidance applying across regulated institutions, with its digital licence used to calibrate entry. South Africa adds a statutory duty to coordinate. Each depends on supervisory capacity, so transfer must be selective and sequenced.

The paper contributes to three literatures. To the fintech regulation literature, which has concentrated on the regulator's toolkit,¹⁶⁶ it adds attention to the internal governance obligations that licensing regimes allocate. To the bank governance literature,¹⁶⁷ it adds the argument that exceptionalism should attach to activity rather than legal form, and it identifies licence-contingency as the way that principle fails in practice. To Nigerian corporate governance scholarship,¹⁶⁸ it adds a map of how governance obligations are distributed across the licence categories through which digital finance is actually delivered.

¹⁶⁶ Zetzsche and others (n 3); Allen (n 3); Brummer and Yadav (n 4).

¹⁶⁷ Macey and O'Hara (n 5); BCBS (n 5).

¹⁶⁸ Adegbite (n 6).

The thesis is doctrinal and generates testable propositions. Future empirical work could examine whether board composition and committee structures in microfinance-licensed digital banks differ from those of payment service banks of comparable scale. It could also examine whether licence choice responds to governance burden, as the regulatory-arbitrage analysis predicts,¹⁶⁹ and whether the governance gap is associated with supervisory outcomes.

Boards of lower-tier digital institutions need not wait for regulatory reform. They can adopt the upper-tier technology-governance standards voluntarily, consistently with their directors' statutory duty of care, which is judged by what a reasonably prudent director would do in comparable circumstances.¹⁷⁰ Regulators can implement Reforms 7.1 to 7.4 under existing powers. Furthermore, many users of Nigerian digital financial services are recent entrants to formal finance. Aligning board-level governance with the risks these institutions carry strengthens the protection of their deposits and data, and so the durability of the financial inclusion that digital finance has made possible.

Although the foregoing analysis concerns Nigeria, the concept of licence-contingency travels beyond Nigeria. Wherever digital financial services are delivered through licence categories designed before them, the same question can be asked: do governance obligations follow the licence or the risk? The five criteria developed here offer a portable instrument for asking it, and comparative application to other African and emerging-market jurisdictions would test how general the Nigerian pattern is.

¹⁶⁹ Armour and others (n 112).

¹⁷⁰ CAMA 2020, s 308(1).