

Digital Infrastructure and Operational Performance in Nigerian Banks: The Moderating Role of Organisational Digital Readiness

¹Abayomi Jonathan Oloniyo,²Iwuozor Odili Markanthony

^{1,2}Departement of Business Administration, University of Abuja, Abuja, Nigeria

¹abayomioloniyo@gmail.com; ²iwuozor.odili@uniabuja.edu.ng

Phone number:+2348033861800:+2347034245464

Abstract—

This study examines whether organisational digital readiness (ODR) conditions the relationship between digital infrastructure and operational performance in Nigerian deposit money banks. The study distinguishes two digital-capability pathways: ICT infrastructure and service delivery speed, and cybersecurity systems and fraud reduction. The theoretical framework integrates resource-based reasoning, the technology–organization–environment perspective, and dynamic capability theory, with recent empirical research emphasizing that digital value depends not only on technology but also on organisational capabilities, leadership, human resources, change processes, and governance. Survey data from 140 banking professionals across 14 Nigerian deposit money banks were analysed using confirmatory factor analysis, hierarchical moderated regression, and PROCESS Model 1 with 5,000 bootstrap samples. ICT infrastructure was positively associated with service delivery speed ($\beta = .46, p < .001$), while cybersecurity systems were positively associated with fraud reduction ($\beta = .43, p < .001$). ODR significantly strengthened both relationships ($\beta = .21, p < .01$; $\beta = .18, p < .01$). The findings indicate that digital infrastructure should be governed as a complementary technological and organisational investment. The revised study also identifies four empirical gaps in the recent literature: insufficient attention to proximal operational outcomes, limited evidence from Nigerian deposit money banks, inadequate testing of organisational readiness as a post-adoption moderator, and insufficient integration of cybersecurity and readiness in explaining fraud-related outcomes. The study recommends that Bank management should integrate organisational-readiness budgets into digital infrastructure investment plans.

Keywords— digital infrastructure; cybersecurity; fraud reduction; organisational digital readiness; service delivery speed.

I. INTRODUCTION

Digital transformation has become an important strategic issue in banking because digital platforms, payment systems, data infrastructure, automation, and cybersecurity increasingly shape how financial institutions create and deliver services. Recent empirical studies show that digital transformation can improve bank performance, although the direction and magnitude of the effect are not uniform across settings. For example, empirical evidence from Vietnamese commercial banks reports a positive relationship between digital transformation and bank performance, while another Vietnamese study reports negative effects on accounting-based performance measures. More recent evidence from Chinese banks likewise indicates that digital transformation can improve performance and bank soundness. These mixed findings suggest that the question is no longer simply whether banks invest in digital technologies, but how and under what organisational conditions those investments generate operational value (Dao et al., 2022; Hu et al., 2025; Nguyen et al., 2023; Zhang et al., 2025).

The Nigerian banking sector provides an important setting for examining this problem. Recent Nigerian studies report positive relationships between digital financial services and bank financial performance, and between cybersecurity and financial innovation. However, these studies have largely examined broad financial outcomes or innovation rather than specific operational outcomes such as service delivery speed and fraud reduction (Akintoye et al., 2022; Isa-Olatinwo et al., 2022). Consequently, there remains a need to distinguish the operational pathways through which particular digital capabilities affect banking outcomes.

Recent research on organisational readiness, specifically on digital transformation readiness, indicates that technological resources alone are insufficient: organisational capability, human capability, management capability, processes, culture, and coordination are central to transformation success. Empirical research has shown that organisational readiness can influence digital change, while studies of digital maturity demonstrate that strategy- and organisation-related resources become increasingly important as firms progress through digital transformation (Duhan et al., 2021; Röglinger et al., 2022; Homburg & Wielgos, 2022). Yet much of this research focuses on readiness for adoption or transformation rather than on readiness as a moderator of the relationship between deployed digital infrastructure and operational outcomes.

This study therefore conceptualises organisational digital readiness (ODR) as a boundary condition. ODR captures the extent to which employees possess relevant digital capabilities, leadership supports digital initiatives, change processes facilitate adoption and redesign, training develops competence, data governance supports reliable information use, and digital strategy is communicated across operational units. The central proposition is that the same technological infrastructure can produce different operational returns depending on the organisation's capacity to mobilise it.

1.1 Statement of the Problem

The Nigerian banking environment operates a standard digital infrastructure, although digital banking, cybersecurity and financial technology have expanded substantially, digital transformation readiness indicates that technological resources

alone are insufficient: organisational capability, human capability, management capability, processes, culture, and coordination are dwindling which is central to transformation success. There is insufficient empirical evidence explaining how specific dimensions of digital infrastructure influence specific operational outcomes and whether organisational digital readiness strengthens these relationships. The central problem addressed by this study is therefore the insufficient empirical explanation of how digital infrastructure translates into specific operational performance outcomes in Nigerian deposit money banks and whether organisational digital readiness changes the strength of these relationships. Existing Nigerian studies have examined digital financial services in relation to financial performance (Isa-Olatinwo et al., 2022) and cybersecurity in relation to financial innovation (Akintoye et al., 2022), while international banking studies have produced mixed evidence concerning the effect of digital transformation on broad bank performance (Do et al., 2022; Nguyen-Thi-Huong et al., 2023). However, the reviewed literature provides limited evidence that simultaneously examines ICT infrastructure and cybersecurity systems as distinct digital resources, service delivery speed and fraud reduction as proximal operational outcomes, and organisational digital readiness as a moderator in the Nigerian banking context. This constitutes the empirical gap that motivates the present study.

The present study addresses this problem by distinguishing two digital-infrastructure pathways: ICT infrastructure and service delivery speed as well as cybersecurity systems and fraud reduction, while examining organisational digital readiness as a moderator of both relationships. This focus directly addresses the outcome-measurement, Nigerian contextual, post-adoption readiness and integrated cybersecurity-readiness gaps identified in the study.

1.2 Research Questions

- i. What are the levels of relationship between ICT infrastructure and service delivery speed in Nigerian deposit money banks?
- ii. What are the degree of relationship between cybersecurity systems and fraud reduction in Nigerian deposit money banks?
- iii. To what extent does organisational digital readiness moderate the relationship between ICT infrastructure and service delivery speed?
- iv. To what extent does organisational digital readiness moderate the relationship between cybersecurity systems and fraud reduction?

2.0 LITERATURE REVIEW AND THEORETICAL FRAMEWORK

2.1 Conceptual Review

2.1.1 Concept of Digital Infrastructure

Digital infrastructure refers in this study to the technological foundation that enables information processing, connectivity, integration, automation, real-time transactions, digital channels, and protection of financial information. The concept is deliberately separated into ICT infrastructure and

cybersecurity systems. ICT infrastructure is integration-oriented and includes platform reliability, system interoperability, workflow automation, network stability, real-time processing, and updating. Cybersecurity systems are protection-oriented and include intrusion detection, fraud monitoring, access control, encryption, incident response, and cybersecurity governance. This distinction is consistent with recent research showing that different dimensions of digital transformation can have different effects on operational and financial outcomes (Ghosh et al., 2022; Zhang et al., 2025).

2.1.2 ICT Infrastructure and Service Delivery Speed

ICT infrastructure should have a direct operational effect because reliable and integrated systems reduce manual handoffs, support real-time information exchange, and facilitate automated workflows. Empirical banking studies support the broader proposition that digital technologies can improve banking performance, although results vary depending on context and the outcome measured. Dao et al. (2022) found a positive effect of digital transformation on Vietnamese commercial-bank performance, while Nguyen et al. (2023) found a negative effect when performance was measured through return on assets and return on equity. The difference reinforces the need to examine proximal operational outcomes rather than assuming that every form of digital investment should immediately translate into profitability.

H₀₁: ICT infrastructure is not positively associated with service delivery speed in deposit money banks.

2.1.3 Cybersecurity Systems and Fraud Reduction

Cybersecurity systems are expected to reduce fraud because monitoring, access controls, encryption, anomaly detection, incident response, and fraud-management systems improve the capacity to identify and contain suspicious activity. Recent empirical evidence directly supports this relationship. Tariq et al. (2024), studying commercial banks, found that cybersecurity influences fraud prevention. Research on bank anti-fraud systems also shows that advanced analytical techniques can improve fraud detection, although false positives remain an important operational problem (Gomes et al., 2022). In Nigeria, Akintoye et al. (2022) found that cybersecurity, operationalised through risk management and bank monitoring, was positively associated with financial innovation among deposit money banks. These studies establish the importance of cybersecurity but leave room for a more specific test of cybersecurity systems against fraud reduction while considering organisational readiness.

H₀₂: Cybersecurity systems are not positively associated with fraud reduction in deposit money banks.

2.2 Organisational Digital Readiness as a Moderator

Organisational digital readiness represents the organisation's capacity to translate digital resources into effective action. Recent empirical work shows that readiness includes technological, business-process, management, human-capability, and cultural dimensions. Halpern et al. (2021) found that organisational readiness directly affected digital change in an international sample of airports. Silva et al.

(2022) similarly highlighted the importance of assessing organisational readiness from the employee perspective. Homburg and Wielgos (2022) further demonstrated that the value of digital capabilities depends on organisational and environmental contingencies. Together, these findings support the argument that readiness is not merely a prerequisite for adoption; it can also shape the magnitude of performance benefits realised from digital resources.

For ICT infrastructure, high ODR should strengthen the relationship with service delivery speed because digitally capable employees, supportive leadership, effective change processes, and reliable data governance enable banks to exploit integration and automation features. For cybersecurity, high ODR should strengthen the relationship with fraud reduction because skilled employees, management attention, updated training, disciplined data governance, and effective escalation routines enable more effective use of security technologies.

H03: Organisational digital readiness does not positively moderate the relationship between ICT infrastructure and service delivery speed.

H04: Organisational digital readiness does not positively moderate the relationship between cybersecurity systems and fraud reduction.

2.2 Theoretical Review

This study reviews two theories The Resource-Based View (RBV) and Dynamic Capability Theory however, it is underpinned by The Resource-Based View (RBV)

2.2.1 Resource-Based View

The Resource-Based View (RBV), principally associated with Barney (1991), explains firm performance from the perspective of resources and capabilities that are valuable, rare, difficult to imitate and difficult to substitute. The theory assumes that firms possess heterogeneous bundles of resources and that these differences can persist over time. Its basic assumptions are therefore resource heterogeneity, resource immobility or imperfect mobility, and the possibility that strategically valuable resources can produce sustained competitive advantage. In the present study, ICT infrastructure and cybersecurity systems are viewed as technologically important resources, but their value is expected to depend on complementary organisational resources such as employee digital skills, leadership support, training, change capacity and data governance. This makes ODR relevant as a mechanism through which banks can convert technological resources into operational value.

Recent applications of resource-based reasoning to digital transformation emphasize that technology becomes strategically useful when it is combined with complementary organisational resources and capabilities. Empirical evidence indicates that digital resources and capabilities do not generate uniform performance outcomes across firms; rather, the way organisations orchestrate digital resources affects the value obtained from them. For example, Bhandari et al. (2023) found a non-linear relationship between digitalisation and performance and showed that resource orchestration affects the returns to digitalisation. Similarly, Homburg and Wielgos

(2022) found that digital capabilities contribute to profitability and that organisational and environmental contingencies influence their value. The implication for Nigerian banks is that infrastructure should not be treated as an isolated asset. Its operational value depends on employees, management, processes, governance, and the ability to integrate technology into work routines.

2.2.2 Dynamic Capability Theory

Dynamic Capability Theory is associated particularly with Teece, Pisano and Shuen (1997) and Teece (2007). The theory focuses on the organisational capacity to integrate, build and reconfigure resources in response to changing environments. Its basic assumptions are that environments are dynamic, that existing resource positions are not sufficient by themselves to guarantee continuing performance, and that organisations require capabilities for sensing opportunities and threats, seizing opportunities and transforming or reconfiguring resources and routines. In this study, organisational digital readiness represents an important organisational capacity through which banks mobilise and reconfigure digital resources. Digital skills, leadership commitment, training, change management, data governance and digital strategy can determine whether installed technology is translated into faster service delivery and stronger fraud-control processes.

Dynamic capability theory complements the resource-based perspective by explaining how organisations renew, integrate, and reconfigure resources in changing environments. Recent research identifies sensing, seizing, and reconfiguring routines as important for digital transformation and shows that digital transformation capability depends on organisational structures, strategic processes, culture, and technological integration (Ellström et al., 2022; Ghosh et al., 2022). This perspective is directly relevant to ODR because employees' digital skills, leadership commitment, change-management processes, training, and data governance represent organisational mechanisms through which banks mobilise and reconfigure digital resources.

2.3 Empirical Reviews

Do, Pham, Thalassinou and Le (2022) examined the impact of digital transformation on the performance of Vietnamese commercial banks in Vietnam. The study population comprised Vietnamese commercial banks, and the researchers selected 13 joint-stock commercial banks on the basis of data availability; the selected banks represented about 61% of the total assets of Vietnamese commercial banks. The study used audited annual financial statements covering 2011 to 2019. For data analysis, technical efficiency was examined using Data Envelopment Analysis (DEA), while the impact of digital transformation was estimated with the System Generalized Method of Moments (System GMM), with Bayesian analysis used as a robustness procedure and STATA employed for estimation. The study concluded that digital transformation had a positive effect on bank performance and that larger banks tended to experience greater benefits. A limitation of the study for the present research is that it concentrated on broad bank performance and efficiency rather than proximal operational outcomes such as service delivery

speed and fraud reduction. It was also conducted in Vietnam rather than Nigeria and did not test organisational digital readiness as a moderator. The study therefore supports the general value of digital transformation while leaving a contextual and explanatory gap that the present study addresses.

Nguyen-Thi-Huong, et al. (2023) investigated how digital transformation affected bank performance in Vietnam. The study focused on joint-stock commercial banks listed on the Vietnam Stock Exchange and used financial statements and annual reports covering 2015 to 2021. The retrieved study information does not establish a precise numerical sample size with sufficient certainty, so no exact number is stated here. Digital transformation was measured through text analysis of annual reports, particularly the frequency of technology-related words, while financial performance was examined through accounting indicators including return on assets and return on equity. Panel-data analysis was conducted using STATA 15. The authors found that digital transformation was negatively associated with ROA and ROE, while the COVID-19 period was associated with an unexpected increase in bank profits. A major limitation acknowledged by the authors is the use of technology-word frequency as a proxy for digital transformation, because the measure does not fully capture actual implementation or the quality of digital transformation. For the present study, the research is useful because it demonstrates that digital transformation does not automatically produce the same outcome across measures; however, it focuses on financial performance rather than operational speed or fraud reduction, uses a Vietnamese context, and does not test organisational digital readiness as a moderator.

Isa-Olatinwo, et al. (2022) examined digital financial services and financial performance of commercial banks in Nigeria. The study was conducted in Nigeria and focused on publicly traded commercial banks. It used secondary data from annual reports and Central Bank of Nigeria sources for the period 2012 to 2020. The retrieved study information identifies the population as publicly traded commercial banks but does not provide a sufficiently clear exact numerical sample in the available abstract, so an exact sample number is not inserted. Digital financial services were proxied using ATM and POS transaction volumes, while financial performance was measured using earnings per share. The researchers applied descriptive and inferential statistical techniques. The study concluded that digital financial services had a significant and positive relationship with financial performance and that electronic banking services could improve accessibility and bank performance. The principal limitation for the present research is that the dependent variable was a broad financial-performance indicator rather than a proximal operational outcome. The study also relied on aggregate secondary indicators and did not examine organisational digital readiness as a moderator or fraud reduction as a specific cybersecurity outcome.

Akintoye, et al. (2022) studied cybersecurity and financial innovation among selected deposit money banks in Nigeria. The research was conducted in Nigeria and involved selected deposit money banks; the selected banks accounted for about 93% of total market capitalisation as at 31 December 2021.

The sample consisted of 56 staff purposively selected from senior personnel in key departments affected by cybersecurity and financial innovation. The study used descriptive and inferential statistics to analyse the data. Cybersecurity was operationalised through risk management and bank monitoring, while financial innovation served as the outcome. The study reported a significant positive relationship between the cybersecurity measures and financial innovation, with an adjusted R-squared of 0.447 and an F-statistic of 23.274 at a significance level below 0.05. The authors recommended stronger risk management and improved monitoring of electronic banking channels. Although this study provides direct Nigerian evidence on cybersecurity, it does not examine fraud reduction as the operational outcome and does not test organisational digital readiness as a moderator. Its purposive sample of 56 staff also limits the extent to which its findings can be generalised to the broader banking workforce.

Halpern, et al. (2020) investigated whether organisational readiness, innovation, airport size and ownership affected digital change at airports. The research was conducted in an international airport context rather than banking. The study examined organisational readiness as a factor associated with digital change and used structural modelling techniques to assess the relationships among readiness and digital-change variables. The study concluded that organisational readiness is an important determinant of digital change and that organisational characteristics help explain differences in digital transformation outcomes. The study is relevant because it supports the proposition that technological change is conditioned by organisational preparedness. However, its airport setting means that the findings cannot be transferred directly to Nigerian deposit money banks. More importantly, readiness was considered in relation to digital change itself rather than as a post-adoption moderator of the relationship between deployed digital infrastructure and operational outcomes. This leaves a clear conceptual gap for the present study.

Silva, et al. (2022) assessed organisational readiness for digital transformation in small and medium-sized enterprises. The study focused on the SME context and developed an approach for assessing readiness from the employee perspective, with particular emphasis on non-technological dimensions of readiness. The available study record does not provide a sufficiently reliable exact numerical population and sample for inclusion here, so those figures are not invented. The study's analysis centred on the development and assessment of a readiness model rather than on testing a banking performance equation. The authors concluded that readiness assessment can identify foundational organisational gaps that may undermine digital transformation. The study is useful for conceptualising ODR because it demonstrates that readiness extends beyond technology to organisational and human factors. Its main limitation for the present research is that it does not empirically test organisational digital readiness as a moderator between digital infrastructure and specific operational outcomes in banks.

Tian, et al. (2021) examined enablers of supply-chain integration from a Technology–Organization–Environment perspective. The study used data from the International Manufacturing Strategy Survey and examined how human

resources and digital manufacturing technologies contributed to supply-chain integration. The study found that human resources and digital manufacturing technologies positively affected dimensions of supply-chain integration, while competition moderated some relationships involving human resources but did not significantly moderate the relationships involving digital manufacturing technologies. The study provides empirical support for the TOE proposition that organisational factors and technological resources jointly shape outcomes. Nevertheless, it was conducted in manufacturing and supply-chain management rather than Nigerian banking. Its outcomes were integration related rather than service delivery speed or fraud reduction, and it did not test organisational digital readiness as the specific moderator proposed in the present study. Its contribution is therefore primarily theoretical and contextual rather than a direct replication of the current banking model.

2.3.1 STUDY GAPS

Recent Nigerian evidence has mainly examined digital banking in relation to broad financial outcomes such as earnings per share, return on assets, or overall bank performance. Isa-Olatinwo et al. (2022), for example, found a positive relationship between digital financial services and financial performance, while Origin and Molokwu (2022) reported a positive but statistically insignificant effect of digital banking on commercial-bank performance. These studies are useful but do not isolate proximal operational mechanisms such as service delivery speed. International banking evidence also demonstrates that digital transformation can have inconsistent effects when broad accounting measures are used (Nguyen et al., 2023; Zhang et al., 2025). The present study addresses this gap by matching ICT infrastructure to service delivery speed.

There is growing Nigerian evidence on digital financial services and cybersecurity, but the evidence base remains comparatively small and fragmented. Akintoye et al. (2022) studied cybersecurity and financial innovation in selected Nigerian deposit money banks, while Isa-Olatinwo et al. (2022) studied digital financial services and financial performance. These studies provide country-specific evidence but do not jointly model digital infrastructure, cybersecurity, organisational readiness, and operational outcomes. The present study addresses this gap by integrating both technological pathways within Nigerian deposit money banks. Recent readiness studies have established that organisational readiness matters for digital change, but much of the empirical work examines readiness as an antecedent of transformation or adoption. Halpern et al. (2021) found that organisational readiness directly influenced digital change, and Silva et al. (2022) identified important non-technological readiness dimensions from employees' perspectives. Homburg and Wielgos (2022) demonstrated the importance of organisational contingencies in digital capability value. However, there is limited empirical testing of readiness as a moderator between already-deployed digital infrastructure and specific operational outcomes. This study therefore treats ODR as a boundary condition rather than merely an adoption antecedent.

Recent cybersecurity studies show that security systems and organisational practices matter for fraud prevention and digital banking, but these streams are often examined separately. Tariq et al. (2024) provide empirical evidence linking cybersecurity to fraud prevention, while Akintoye et al. (2022) demonstrate a positive cybersecurity–financial-innovation relationship in Nigeria. Yet limited evidence explains whether organisational readiness changes the strength of the cybersecurity–fraud relationship. The present study addresses this gap by testing the cybersecurity systems × ODR interaction.

2.4 Conceptual Framework

The conceptual model proposes two direct relationships and two moderation effects. ICT infrastructure is expected to improve service delivery speed; cybersecurity systems are expected to improve fraud reduction; and organisational digital readiness is expected to strengthen both relationships.

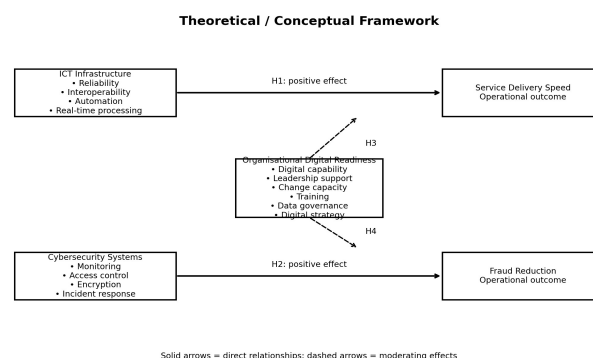


Figure 1: Linking diagram of the conceptual framework

3.0 METHODOLOGY

The study adopted a cross-sectional explanatory survey design among employees of Nigerian deposit money banks. Purposive sampling was applied across three institutional strata: systemically important Tier 1 banks, Tier 2 banks, and regional or smaller banks. Eligible respondents were professionals in IT and digital operations, risk and compliance, and operations and service management because these roles provide direct knowledge of digital infrastructure and operational processes.

Data were collected between February and August 2025 in Lagos, Abuja, Port Harcourt, and Kano. Of 180 questionnaires distributed, 147 were returned. Seven responses were excluded because they were incomplete or exhibited straight-line response patterns, leaving 140 usable questionnaires from 14 banks, representing a usable response rate of 77.8%. Participation was voluntary, informed consent was obtained, and responses were anonymous and confidential.

The unit of analysis was the individual banking professional. Therefore, the constructs represent informed employee assessments of infrastructure, organisational readiness, and operational outcomes within respondents' employing institutions. They are not presented as audited bank-level indicators. Because respondents were nested within 14 institutions and the reported analysis did not estimate a multilevel model, conclusions are restricted to respondent-level associations.

Table 3.1 Demographic Data

Characteristic	Category	N	%
Gender	Male	89	63.6
Gender	Female	51	36.4
Age	25–34 years	62	44.3
Age	35–44 years	54	38.6
Age	45 years and above	24	17.1
Education	HND/Bachelor's degree	78	55.7
Education	Master's degree	55	39.3
Education	Doctorate/professional qualification	7	5.0
Bank tier	Tier 1 (SIFI)	63	45.0
Bank tier	Tier 2	49	35.0
Bank tier	Regional/smaller	28	20.0
Experience	Less than 5 years	34	24.3
Experience	5–10 years	67	47.9
Experience	More than 10 years	39	27.9
Functional role	IT/digital operations	58	41.4
Functional role	Risk/compliance	39	27.9
Functional role	Operations/service	43	30.7

Source: Field Survey Data, 2026.

All constructs were measured reflectively using five-point Likert-type response options ranging from 1 = strongly disagree to 5 = strongly agree. Items were adapted and contextualised from recent digital transformation, digital capability, organisational readiness, banking, and cybersecurity literature. Three banking IT executives and two information-systems academics reviewed the instrument for clarity and content relevance. A pilot involving 20 respondents was used to identify ambiguous wording before the main survey.

Table 3.2 Constructs Measure

Construct	No. of items	Operational dimensions
ICT infrastructure	6	Reliability, integration, real-time processing, workflow automation, network stability, updating
Cybersecurity systems	6	Intrusion detection, fraud monitoring, access control, incident response, encryption, governance
Organisational digital readiness	6	Employee capability, leadership commitment, change processes, data governance, training, strategy communication
Service delivery speed	5	Transaction speed, response times, workflow time, coordination, digital-channel uptime
Fraud reduction	5	Reduced transaction

		fraud, reduced fraud losses, alert action, multilayered protection, security compliance
--	--	---

Source: Field Survey Data, 2026.

The analysis proceeded in four stages. First, confirmatory factor analysis (CFA) was used to assess the measurement model using CFI, TLI, RMSEA, and SRMR. Convergent validity was assessed through standardised factor loadings, composite reliability, and average variance extracted, while discriminant validity was assessed through the Fornell–Larcker procedure. Second, descriptive statistics and bivariate correlations were examined. Third, hierarchical moderated regressions were estimated separately for service delivery speed and fraud reduction. Institutional size, institutional age, and regulatory tier were entered as controls; the focal infrastructure variable was entered next; ODR was then entered; and finally the mean-centred infrastructure $\times$ ODR interaction was entered. Fourth, PROCESS Model 1 with 5,000 bootstrap samples was used to estimate conditional effects at one standard deviation above and below the ODR mean.

Model Specification

$$\text{SDS} = \beta_0 + \beta_1\text{ICTI} + \beta_2\text{ODR} + \beta_3(\text{ICTI} \times \text{ODR}) + \beta_4\text{Controls} + \varepsilon$$

$$\text{FRD} = \beta_0 + \beta_1\text{CSS} + \beta_2\text{ODR} + \beta_3(\text{CSS} \times \text{ODR}) + \beta_4\text{Controls} + \varepsilon$$

Where SDS represents service delivery speed; FRD represents fraud reduction; ICTI represents ICT infrastructure; CSS represents cybersecurity systems; ODR represents organisational digital readiness; and the controls include institutional size, institutional age and regulatory tier.

4.0 DATA ANALYSIS & DISCUSSIONS

4.1 Measurement Model

The CFA indicated acceptable approximate fit: CFI = .961, TLI = .954, RMSEA = .051, 90% CI [.033, .067], and SRMR = .054. Standardised factor loadings ranged from .72 to .84 and were significant at $p < .001$. Composite reliability exceeded .70 and average variance extracted exceeded .50 for every construct. These results support internal consistency and convergent validity. The single-factor diagnostic accounted for 24.3% of variance; however, this diagnostic does not by itself eliminate common-method variance, which remains a limitation of the single-source cross-sectional design.

Construct	Items	Loading range	A	CR	AVE
ICT infrastructure	6	.72–.83	.88	.90	.60
Cybersecurity systems	6	.73–.82	.90	.90	.61
Organisational digital readiness	6	.74–.81	.89	.90	.60
Service	5	.77–.84	.89	.90	.64

delivery speed					
Fraud reduction	5	.77–.83	.91	.90	.64

Source: AMOS Output, 2026

4.2 Descriptive Statistics and Discriminant Validity

Construct means ranged from 3.75 to 3.92. All focal correlations were positive and statistically significant. The square root of AVE for each construct exceeded its correlations with the other constructs, supporting discriminant validity under the adopted criterion. The strongest correlations were between ICT infrastructure and service delivery speed ($r = .70$) and between cybersecurity systems and fraud reduction ($r = .70$).

Variable	M	SD	1	2	3	4	5
1. ICT infrastructure	3.92	.83	.77				
2. Cybersecurity systems	3.75	.91	.61**	.78			
3. ODR	3.79	.84	.63**	.57**	.77		
4. Service delivery speed	3.87	.88	.70**	.61**	.66**	.80	
5. Fraud reduction	3.81	.86	.59**	.70**	.58**	.65**	.80

Source: SPSS output version 28.0

4.3 ICT Infrastructure, Service Delivery Speed, and ODR

The control variables accounted for 8% of the variance in service delivery speed. Adding ICT infrastructure increased explained variance by .39, and ICT infrastructure was positively associated with service delivery speed ($\beta = .46$, $t = 10.18$, $p < .001$), supporting H1. ODR added 5% to explained variance. The ICT infrastructure $\times$ ODR interaction was positive ($\beta = .21$, $t = 3.29$, $p < .01$) and explained an additional 4% of variance, supporting H3. The final model explained 56% of the variance in perceived service delivery speed.

Predictor/statistic	Step 1 β	Step 2 β	Step 3 β	Step 4 β
Institutional size	.18*	.12	.10	.09
Institutional age	.14*	.08	.07	.06
Regulatory tier	.12	.07	.06	.05
ICT infrastructure	—	.46***	.44***	.42***
Organisational digital readiness	—	—	.22***	.20***
ICTI $\times$ ODR	—	—	—	.21**
R ²	.08	.47	.52	.56
Adjusted R ²	.06	.46	.50	.54
ΔR^2	—	.39	.05	.04

Source: SPSS output version 28.0

4.4 Cybersecurity Systems, Fraud Reduction, and ODR

The control variables accounted for 7% of the variance in fraud reduction. Adding cybersecurity systems increased explained variance by .40, and cybersecurity systems were positively associated with fraud reduction ($\beta = .43$, $t = 10.44$, $p < .001$), supporting H2. ODR added 4% to explained variance. The cybersecurity systems $\times$ ODR interaction was positive ($\beta = .18$, $t = 2.87$, $p < .01$) and explained a further 3% of variance, supporting H4. The final model explained 54% of the variance in perceived fraud reduction.

Predictor/statistic	Step 1 β	Step 2 β	Step 3 β	Step 4 β
Institutional size	.15*	.10	.09	.08
Institutional age	.11	.07	.06	.05
Regulatory tier	.14*	.09	.08	.07
Cybersecurity systems	—	.43***	.41***	.39***
Organisational digital readiness	—	—	.19***	.17***
CSS $\times$ ODR	—	—	—	.18**
R ²	.07	.47	.51	.54
Adjusted R ²	.05	.46	.49	.52
ΔR^2	—	.40	.04	.03

Source: SPSS output version 28.0

4.5 Conditional Effects

The conditional-effect estimates clarify both moderation effects. The association between ICT infrastructure and service delivery speed was stronger at high ODR ($b = .61$, 95% CI [.51, .71]) than at low ODR ($b = .31$, 95% CI [.19, .44]). Similarly, the association between cybersecurity systems and fraud reduction was stronger at high ODR ($b = .57$, 95% CI [.46, .68]) than at low ODR ($b = .29$, 95% CI [.16, .42]). In the observed sample, each high-ODR slope was approximately twice the corresponding low-ODR slope.

Path	ODR level	B	SE	t	95% CI
ICT infrastructure $\rightarrow$ service delivery speed	High (+1 SD)	.61***	.052	11.73	[.51, .71]
ICT infrastructure $\rightarrow$ service delivery speed	Low (–1 SD)	.31***	.063	4.92	[.19, .44]
Cybersecurity systems $\rightarrow$ fraud reduction	High (+1 SD)	.57***	.055	10.36	[.46, .68]
Cybersecurity systems $\rightarrow$ fraud	Low (–1 SD)	.29***	.067	4.33	[.16, .42]

reduction					
-----------	--	--	--	--	--

Source: PROCESS Model 1 Output, 2026.

4.6 Tests of Hypotheses

Hypothesis One (H1)

H01: ICT infrastructure is not positively associated with service delivery speed.

The hierarchical moderated regression results show that the control variables accounted for 8% of the variance in service delivery speed. After ICT infrastructure was entered, explained variance increased by 39 percentage points, and ICT infrastructure was positively associated with service delivery speed ($\beta = .46, t = 10.18, p < .001$). Because the coefficient is positive and statistically significant, **H01** is rejected and **H1**: is supported. The result indicates that stronger ICT infrastructure is associated with faster perceived service delivery among the sampled banking professionals.

Hypothesis Two (H2)

H02: Cybersecurity systems are not positively associated with fraud reduction.

The control variables accounted for 7% of the variance in fraud reduction. Adding cybersecurity systems increased explained variance by 40 percentage points, and cybersecurity systems showed a positive and statistically significant association with fraud reduction ($\beta = .43, t = 10.44, p < .001$). Accordingly, **H02** is rejected and **H2**: is supported. The finding indicates that stronger cybersecurity systems are associated with greater perceived fraud reduction in the sampled Nigerian deposit money banks.

Hypothesis Three (H3)

H03: Organisational digital readiness does not positively moderates the relationship between ICT infrastructure and service delivery speed.

Organisational digital readiness added 5% to explained variance in the service-delivery model. The interaction between ICT infrastructure and ODR was positive and statistically significant ($\beta = .21, t = 3.29, p < .01$) and contributed an additional 4% of explained variance. The final model explained 56% of the variance in perceived service delivery speed. Conditional effects further showed that the association between ICT infrastructure and service delivery speed was stronger at high ODR ($b = .61, 95\% \text{ CI } [.51, .71]$) than at low ODR ($b = .31, 95\% \text{ CI } [.19, .44]$). **H03** is rejected and **H3**: is therefore supported. The result means that organisational readiness strengthens the operational value realised from ICT infrastructure.

Hypothesis Four (H4)

H04: organisational digital readiness does not positively moderates the relationship between cybersecurity systems and fraud reduction.

ODR added 4% to explained variance in the fraud-reduction model. The interaction between cybersecurity systems and ODR was positive and statistically significant ($\beta = .18, t = 2.87, p < .01$), and it explained a further 3% of variance. The final model explained 54% of the variance in perceived fraud reduction. The conditional effects showed that the

cybersecurity–fraud-reduction relationship was stronger at high ODR ($b = .57, 95\% \text{ CI } [.46, .68]$) than at low ODR ($b = .29, 95\% \text{ CI } [.16, .42]$). **H04** is rejected and **H4**: is therefore supported.

4.7 Discussion of Findings

The findings support all four hypotheses. ICT infrastructure was positively associated with service delivery speed, while cybersecurity systems were positively associated with fraud reduction. The results therefore support a functionally differentiated view of digital infrastructure. Integration-oriented infrastructure is most closely connected to process acceleration, whereas protection-oriented infrastructure is most closely connected to risk containment. This interpretation is consistent with recent banking evidence showing that digital transformation affects performance through multiple and sometimes divergent mechanisms (Dao et al., 2022; Nguyen et al., 2023; Zhang et al., 2025).

The stronger moderation effects at high ODR are consistent with recent empirical work showing that organisational and human capabilities condition the value of digital resources. Homburg and Wielgos (2022) show that digital capabilities create value in interaction with organisational and environmental contingencies. Halpern et al. (2021) and Silva et al. (2022) demonstrate that readiness involves capabilities extending beyond technology. Ellström et al. (2022) and Ghosh et al. (2022) further show that digital transformation requires organisational routines for sensing, seizing, and reconfiguring resources. The present results extend this logic to Nigerian banking by treating readiness as a moderator of operational value rather than only as an antecedent of adoption.

The cybersecurity findings are also consistent with recent evidence that cybersecurity practices influence fraud prevention and financial innovation. Tariq et al. (2024) identify a relationship between cybersecurity and fraud prevention, while Akintoye et al. (2022) report a positive cybersecurity effect on financial innovation among Nigerian deposit money banks. The present study adds that the strength of the cybersecurity–fraud relationship depends on organisational readiness. In practical terms, a security system is more likely to produce operational value when employees can interpret alerts, management supports response processes, data are governed effectively, and training is updated.

5.0 CONCLUSION AND RECOMMENDATION

5.1 Conclusion

This study examined the relationships between digital infrastructure and operational performance in Nigerian deposit money banks and tested organisational digital readiness as a moderating condition. The reported evidence indicates that ICT infrastructure is positively associated with service delivery speed and that cybersecurity systems are positively associated with fraud reduction. More importantly, both relationships are stronger when organisational digital readiness is high.

The findings reinforce a central conclusion from recent digital transformation research: technology investment does not

automatically translate into equivalent organisational value. Digital resources must be combined with human capability, leadership support, effective processes, governance, and the organisational capacity to reconfigure routines. The Nigerian banking context is particularly relevant because digital banking has expanded rapidly while banks continue to face operational, cybersecurity, and capability challenges.

5.2 Recommendations

- i. Bank management should integrate organisational-readiness budgets into digital infrastructure investment plans. Each major technology project should specify associated training, process redesign, data-governance responsibilities, and change-management activities.
- ii. Banks should strengthen digital skills development for IT, operations, risk, compliance, and service personnel. Training should be continuous rather than limited to system implementation.
- iii. Management should establish post-implementation performance reviews that assess whether digital infrastructure has actually improved transaction-cycle times, workflow completion, service responsiveness, system uptime, and other operational indicators.
- iv. Cybersecurity investments should be linked to measurable fraud-management processes, including alert response time, incident escalation, rule updating, access-control effectiveness, and verified fraud-loss indicators.

5.3 Implications

The findings have implications for bank management. Digital infrastructure and organisational readiness should be treated as complementary investments. Business cases for core banking systems, automation, integration platforms, and cybersecurity tools should include explicit provisions for employee capability, training, process redesign, leadership sponsorship, data ownership, and change accountability. Technical implementation should therefore be followed by post-implementation evaluation of actual organisational use and operational outcomes.

For ICT and operations managers, programs aimed at service speed should emphasise integration, workflow redesign, user competence, uptime, and cross-functional coordination. Cybersecurity programs aimed at fraud reduction should emphasise alert governance, data quality, analytical capability, escalation routines, incident-response exercises, and continuous updating of monitoring rules.

For regulators, the results suggest that digital-resilience supervision can consider organisational capability and governance alongside technical infrastructure. However, the cross-sectional respondent-level evidence does not by itself justify a specific regulatory mandate. Sector-wide prescriptions would require longitudinal, multi-source, and institution-level evidence.

References

[1] R. Akintoye, O. Ogunode, M. Ajayi, and A. A. Joshua, "Cyber security and financial innovation of selected deposit money banks in Nigeria," *Universal Journal of Accounting and Finance*, vol. 10, no. 3, pp. 643–652, 2022. doi: 10.13189/ujaf.2022.100302.

[2] J. Baker, "The technology–organization–environment framework," in *Information Systems Theory: Explaining and Predicting Our Digital Society*, Y. K. Dwivedi et al., Eds. Springer, 2012.

[3] J. Barney, "Firm resources and sustained competitive advantage," *Journal of Management*, vol. 17, no. 1, pp. 99–120, 1991.

[4] K. R. Bhandari, P. Zamborsky, M. Ranta, and J. Salo, "Digitalization, internationalization, and firm performance: A resource-orchestration perspective on new OLI advantages," *International Business Review*, vol. 32, no. 4, p. 102135, 2023. doi: 10.1016/j.ibusrev.2023.102135.

[5] T. D. Do, H. A. T. Pham, E. I. Thalassinou, and H. A. Le, "The impact of digital transformation on performance: Evidence from Vietnamese commercial banks," *Journal of Risk and Financial Management*, vol. 15, no. 1, p. 21, 2022. doi: 10.3390/jrfm15010021.

[6] D. Ellström, J. Holtström, E. Berg, and C. Josefsson, "Dynamic capabilities for digital transformation," *Journal of Strategy and Management*, vol. 15, no. 2, pp. 272–286, 2022. doi: 10.1108/JSMA-04-2021-0089.

[7] S. Ghosh, M. Hughes, I. Hodgkinson, and P. Hughes, "Digital transformation of industrial businesses: A dynamic capability approach," *Technovation*, vol. 113, p. 102414, 2022. doi: 10.1016/j.technovation.2021.102414.

[8] N. Halpern, D. Mwesummo, P. Suau-Sanchez, T. Budd, and S. Bråthen, "Ready for digital transformation? The effect of organisational readiness, innovation, airport size and ownership on digital change at airports," *Journal of Air Transport Management*, vol. 90, p. 101949, 2021. doi: 10.1016/j.jairtraman.2020.101949.

[9] N. Halpern, D. Mwesummo, P. Suau-Sanchez, T. Budd, and S. Bråthen, "Ready for digital transformation? The effect of organisational readiness, innovation, airport size and ownership on digital change at airports," *Journal of Air Transport Management*, vol. 90, p. 101949, 2020.

[10] C. Homburg and D. M. Wielgos, "The value relevance of digital marketing capabilities to firm performance," *Journal of the Academy of Marketing Science*, vol. 50, pp. 666–688, 2022. doi: 10.1007/s11747-022-00858-7.

[11] H. Hu, T. Wei, and A. Wang, "Does digital transformation enhance bank soundness? Evidence from Chinese commercial banks," *Journal of Financial Stability*, p. 101374, 2025. doi: 10.1016/j.jfs.2025.101374.

[12] A. Isa-Olatinwo, U. Uwaleke, and U. A. Ibrahim, "Digital financial services on financial performance of commercial banks in Nigeria," *WSEAS Transactions on Business and Economics*, vol. 19, pp. 1121–1129, 2022. doi: 10.37394/23207.2022.19.98.

[13] L. N. T. H. Nguyen, H. V. Nguyen, A. N. P. Nguyen, and D. V. Nguyen, "How does digital transformation impact bank performance?" *Cogent Economics & Finance*, vol. 11, no. 1, p. 2217582, 2023. doi: 10.1080/23322039.2023.2217582.

[14] R. P. Silva, C. Saraiva, and H. S. Mamede, "Assessment of organizational readiness for digital transformation in SMEs," *Procedia Computer Science*, vol. 204, pp. 362–369, 2022. doi: 10.1016/j.procs.2022.08.044.

[15] E. Tariq, I. Akour, N. Al-Shanableh, E. K. Alquqa, N. Alzboun, S. I. S. Al-Hawary, and M. T. Alshurideh, "How cybersecurity influences fraud prevention: An empirical study on Jordanian commercial banks," *International Journal of Data and Network Science*, vol. 8, no. 1, pp. 69–76, 2024. doi: 10.5267/j.ijdns.2023.10.016.

[16] D. J. Teece, "Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance," *Strategic Management Journal*, vol. 28, no. 13, pp. 1319–1350, 2007.

[17] M. Tian, B. Huo, Y. Park, and M. Kang, "Enablers of supply chain integration: A technology-organization-environment view," *Industrial Management & Data Systems*, vol. 121, no. 8, pp. 1871–1895, 2021. doi: 10.1108/IMDS-09-2020-0564.

- [18] L. G. Tornatzky and M. Fleischer, *The Processes of Technological Innovation*. Lexington Books, 1990.
- [19] I. A. Vorobyev and A. D. Krivitskaya, "Reducing false positives in bank anti-fraud systems based on rule induction in distributed tree-based models," *Computers & Security*, vol. 120, p. 102786, 2022. doi: 10.1016/j.cose.2022.102786.
- [20] C. Zhang, Y. Wang, and Y. Zhang, "Can digital transformation improve commercial banks' performance?" *The Journal of Technology Transfer*, vol. 50, pp. 1341–1362, 2025. doi: 10.1007/s10961-024-10139-w.