National University of Political Studies and Public Administration
Faculty of Management

Beyond the Direct Effect: Cybersecurity Readiness as a Boundary Condition of the FinTech–Operational Efficiency Relationship in Algerian Commercial Banking

Hassina SAAD BEKHOUCHE[1], Hassiba ALMI[2], Aboubaker KHOUALED[3], Mouloud KHOUALED[4]

[1] Faculty of Economics and Management, University of Abdelhafid Boussouf, Mila, Algeria; h.saadbekhouche@centre-univ-mila.dz

[2] Badji Mokhtar-Annaba University, P.O. Box 12, Annaba 23000, Algeria; hassiba.almi@univ-annaba.dz

[3] Badji Mokhtar-Annaba University, P.O. Box 12, Annaba 23000, Algeria; aboubaker.khoualed@univ-annaba.dz

[4] Faculty of Economics and Management, University of Abdelhafid Boussouf, Mila, Algeria; mouloud.khoualed@centre-univ-mila.dz

Received: July 30, 2026
Revised: August 20, 2026
Accepted: September 1, 2026
Published: September 29, 2026

Abstract: The integration of FinTech is associated with higher operational efficiency in most banks across emerging markets, yet the magnitude of that association varies substantially among institutions. Current research assesses the mean effect and reports contradictory findings, while few studies examine the organisational factors that shape when the benefit emerges. This study investigates cybersecurity readiness as a boundary condition of that relationship. We gathered survey data from 55 employees of Crédit Populaire d'Algérie in Mila province, Algeria, and estimated a moderated model through partial least squares structural equation modelling. FinTech adoption is positively associated with operational efficiency ($\beta = 0.938$, $p < 0.001$), cybersecurity readiness relates to it directly ($\beta = 0.243$, $p = 0.005$), and the interaction between them is positive and significant ($\beta = 0.330$, $p < 0.001$), with the model accounting for 78.0 per cent of the variance in operational efficiency. Simple-slopes analysis indicates that the conditional association increases from 0.608 at low readiness to 1.268 at high readiness, so that a bank with robust security capability is linked to roughly double the efficiency improvement for a given degree of digital adoption. The findings are consistent with a complementarity perspective, in which FinTech investment and cybersecurity capability appear to yield returns jointly rather than independently. Because the design is cross-sectional and the sample is drawn from a single branch network, the results reflect associations within this organisation rather than causal or sector-wide effects. For bank executives, the pattern suggests a sequencing consideration: developing detection, response, and staff proficiency alongside digital platforms rather than afterwards.

Keywords: FinTech adoption; cybersecurity readiness; operational efficiency; digital transformation; bank performance; Algeria.

Introduction

Financial institutions in developing economies have rapidly embraced FinTech, moving transactions to mobile platforms, credit evaluation to algorithms, and administrative procedures to automated workflows. The literature indicates that this transition is associated with lower transaction costs, shorter processing time, and better utilisation of labour and capital (Bartoo et al., 2025; Ristanović et al., 2025; Wang et al., 2021). However, the agreement ends at the mean impact, while individual outcomes vary. Lee et al. (2023) find that FinTech advancement was associated with reduced overall efficiency in Chinese commercial banks, chiefly through higher funding costs; Juma Ally et al. (2025) observe gains in major Tanzanian banks and losses in smaller ones; and Khan et al. (2024) report a U-shaped relationship across 59 developing nations, in which initial adoption relates to

How to cite
Saad Bekhouche, H., Almi, H., Khoualed, A., & Khoualed, M. (2026). Beyond the Direct Effect: Cybersecurity Readiness as a Boundary Condition of the FinTech–Operational Efficiency Relationship in Algerian Commercial Banking. *Management Dynamics in the Knowledge Economy, 14*(3), 344-365. DOI 10.2478/mdke-2026-0019
ISSN: 2392-8042 (online)
www.managementdynamics.ro
https://reference-global.com/journal/MDKE

Vol.14 (2026) no.3, pp.344-365; DOI 10.2478/mdke-2026-0019

lower efficiency before subsequent improvement. These outcomes share a consistent pattern: the return to FinTech is contingent on the bank's existing assets. Iatzaz Ul Hassan et al. (2025) show that stronger economic governance is associated with larger FinTech benefits across 33 developing Asian nations, and Li et al. (2025) report a similar pattern for regional financial development within China. Technology does not generate its own returns; the organisation determines whether those returns become visible.

We contend that cybersecurity readiness belongs to this set of enabling competencies, and the contention rests on a mechanism. FinTech broadens the attack surface, as third-party APIs, cloud reliance, partner access points, and continuous transaction flows introduce more vulnerabilities (Umoga et al., 2024; Waliullah et al., 2025). A bank that digitalises without corresponding detection, response, and recovery mechanisms absorbs the new risk as an operating expense: disruptions hinder service, remediation consumes staff resources, and regulatory requirements increase, so productivity gains from automation are offset by productivity losses from disruption. Al-Shari and Lokhande (2023) identify cyber risk as the most significant adverse factor affecting the performance of FinTech-adopting banks, which corroborates this interpretation. Empirical evidence supports the moderation argument: Hanifan et al. (2026), Al Hammadi et al. (2024), and Murungu et al. (2026) each find that cyber-risk-management maturity or IT-security capability strengthens the performance benefits of digitalisation, and Hasan et al. (2021) show that cyber readiness is associated with greater security effectiveness and, in turn, with financial and non-financial outcomes.

Three voids persist. First, few studies directly assess the interaction term; most cybersecurity literature records threats and controls without testing whether readiness influences the return on digital investment. Second, existing moderation assessments focus on profitability or risk-management efficacy rather than operational efficiency, the primary channel through which FinTech operates, and they treat readiness as a single aggregate, excluding detail about its internal structure. Third, the evidence base rests on banking systems in the Gulf, Southeast Asia, and Southern Africa, while excluding North African public banking, where administrative mandates rather than competitive forces drive digital adoption. That divergence matters: when technology is introduced by regulation rather than market choice, the gap between adoption and organisational readiness widens, making the influence of readiness more apparent. Algeria provides such an environment, as elaborated in the Algerian context section.

This research addresses the three deficiencies by assessing the interaction directly, measuring cybersecurity readiness through its technical and human dimensions, and evaluating the model on one state-owned bank in Algeria. Its contribution is fourfold. Theoretically, it extends the complementarity thesis to the FinTech–efficiency relationship and proposes cybersecurity readiness as the supplementary asset. Empirically, it offers the first direct test of this moderation on operational efficiency and the first such evidence from an Algerian public bank, framed as exploratory findings within a single branch network rather than sector-wide results. Practically, it points to a sequencing consideration for managers, namely developing readiness alongside implementation rather than afterwards, and, for regulators, it suggests that cyber resilience may carry a productivity relevance in addition to a stability one, which would integrate cybersecurity oversight within the digital-transformation agenda rather than treating it as a separate issue. The remainder of the paper presents the literature review, the theoretical framework and hypotheses, the data and methodology, the results, the discussion, and the conclusion.

Literature review

FinTech adoption and bank operational efficiency

The primary conclusion is favourable. Wang et al. (2021) find that FinTech advancement raised total factor productivity in Chinese commercial banks while cutting operating expenses, and Lee et al. (2021) report improvements in cost efficiency and the technology frontier for Chinese banks from 2003 to 2017. Verma et al. (2025), Goel and Kashiramka (2026), Kayed et al. (2025), and Zhu and Guo (2024) report comparable patterns across commercial and emerging-market samples. The mechanism is uniform: digital platforms lower per-transaction cost, automation reduces errors and rework, and scalable systems add volume without a proportional rise in personnel. Sajid et al. (2023) add that operational efficiency mediates the FinTech effect on bank risk-taking, so the efficiency channel matters beyond cost alone.

Evidence from developing markets beyond Asia corroborates the trend. Bartoo et al. (2025) find FinTech adoption to be the strongest determinant of technical efficiency in Kenyan banks; Ristanović et al. (2025) report consistent efficiency gains from digital channels across twelve developing nations; and Iatzaz Ul Hassan et al. (2025) find favourable correlations across quantiles in 33 developing Asian nations, with larger relative gains for underperforming banks. In a systematic review, Huang and Said (2025) conclude that FinTech generally improves banking efficiency, while noting that its magnitude varies across contexts in ways the individual studies do not explain. That unexplained variation is precisely what boundary conditions address.

The contradictory evidence

The favourable mean obscures genuine variability, and this dispersion motivates the present research. Lee et al. (2023), examining 74 Chinese banks from 2012 to 2019 with DEA-Malmquist and dynamic GMM, find that FinTech diminished overall efficiency through the liability side, as competition from digital newcomers raised funding costs faster than automation cut operating expenditure. Khan et al. (2024) provide the most relevant result for our context: across 59 developing nations from 2010 to 2022, the FinTech–efficiency correlation is U-shaped, with adoption costs prevailing at low integration and efficiency gains beyond a threshold that larger, better-capitalised banks cross more swiftly. Juma Ally et al. (2025) document the size effect in Tanzania, with beneficial efficiency correlations for large banks and detrimental ones for medium and small banks, and Zhao et al. (2022) report a directional conflict in which FinTech innovation improves management efficiency and capital adequacy but weakens profitability and asset quality.

Cybersecurity as an organisational capability

The literature on cybersecurity in banking has transitioned from enumerating dangers to assessing capabilities, a transition significant for our thesis, since a threat inventory cannot moderate anything whereas a capability can. On the threat side, Waliullah et al. (2025) illustrate the dual nature of FinTech in security, enhancing fraud detection and authentication while creating vulnerable avenues via third-party APIs, cloud infrastructure, and partner access; Umoga et al. (2024) examine emerging financial-technology threats; Oyewole et al. (2024) enumerate online-banking hazards such as credential theft and transactional fraud; AlBenJasim et al. (2024) delineate regulatory and technical obstacles in the Bahraini FinTech industry; and Al-Shari and Lokhande (2023) identify cyber risk as the most detrimental influence on FinTech-adopting banks in Yemen.

On the capability side, Uddin et al. (2020) conclude that the amount spent on cyber technology does not by itself determine stability; Uddin et al. (2023) extend this to operational-risk exposure amid digital transformation; and Türegün (2025) argues that success depends on strategic integration rather than budget size. Governance evidence

Vol.14 (2026) no.3, pp.344-365; DOI 10.2478/mdke-2026-0019

supports this view: Elsayed et al. (2024) find that cybersecurity disclosure elevates performance in MENA listed banks, moderated by the presence of a Chief Risk Officer, and Cheng et al. (2024) link sovereign-level cyber governance to digital-finance outcomes. Crucially for our design, two studies treat readiness as a measurable construct rather than a policy requirement: Hasan et al. (2021) supply a readiness metric spanning awareness, technical controls, and organisational commitment, and Berlilana et al. (2021) correlate cybersecurity readiness with technology readiness. This literature supplies both components of our case: cyber vulnerability rises alongside digital integration, and readiness is an evaluable competency rather than only a compliance cost.

The moderation evidence and the gap

Four studies examine the interaction we assess directly. Hanifan et al. (2026) find, for Indonesian banks, that FinTech financing and cyber-risk-management efficacy each raise return on assets and that their interaction is positive and substantial, so banks with developed cyber risk management capture a greater share of the digitalisation payoff. Al Hammadi et al. (2024) find that IT security measures strengthen the FinTech effect on risk-management efficacy in UAE Islamic banks, and Murungu et al. (2026) show that cybersecurity policies shape digital-transformation results in Zimbabwean banks, positioning cybersecurity as an enabler rather than only a defensive measure. Al-Omoush (2026) reports a mediated path in Jordan, in which AI and cybersecurity drive FinTech advances that then relate to operational efficiency; the specification is enabling rather than moderating, since it asserts that cybersecurity supports digital functionality without testing its impact on the returns to that functionality. A further set of studies shows that broader organisational and institutional conditions shape the FinTech effect: Iatzaz Ul Hassan et al. (2025), Li et al. (2025), and Elmahdy et al. (2025) find that governance quality, regional financial development, and bank size, respectively, condition the relationship, though none identifies cybersecurity readiness as the moderator.

The gap is specific in three respects. First, current moderation assessments target profitability or risk-management efficacy rather than operational efficiency, the primary and most immediate outcome through which FinTech operates. Second, the moderator is generally a single aggregate, referred to as cyber risk management, IT security competence, or cybersecurity strategy, leaving the internal structure of readiness ambiguous. Third, the evidence base spans the Gulf, Southeast Asia, and Southern Africa but excludes North African public banking, where administrative mandates rather than competition drive digital adoption. Jafri et al. (2024) and Cele and Kwenda (2025) both conclude that interaction designs are scarce while the descriptive threat literature is abundant.

The Algerian context

Algerian banking offers circumstances that make the moderation question tractable. State-owned commercial banks dominate the sector and hold the bulk of assets under direct government control. Digital transformation has advanced through national initiatives and central-bank mandates covering electronic-payment frameworks and interbank card networks. Because adoption is driven by administrative choice rather than competitive selection, banks implement digital platforms before building the organisational capability to run them securely, generating discrepancies in readiness among units at comparable adoption levels, which is the variance a moderation test requires. It also raises the stakes, since a public bank that fails to translate adoption into efficiency incurs the investment cost without the return. Ononiwu et al. (2024) describe the operational constraints of digital transformation in emerging economies, namely skills gaps, legacy-system reliance, and infrastructural weakness, which accurately depict the Algerian setting in which organisational readiness shapes whether anticipated returns from digital investment materialise.

Table 1. Summary of the most relevant empirical studies on FinTech adoption, cybersecurity, and bank performance

Authors	Year	Context	Method	Main finding	Relevance to this study
Wang et al.	2021	China	DEA + GMM	FinTech raises productivity and cuts operating costs	Baseline direct effect
Lee et al.	2023	China, 74 banks	DEA-Malmquist + GMM	FinTech reduces overall efficiency through funding costs	Contradictory evidence
Khan et al.	2024	59 developing countries	Non-linear panel	U-shaped FinTech–efficiency relationship	Central motivation for a boundary condition
Juma Ally et al.	2025	Tanzania	Panel	Gains for large banks, losses for small and medium	Heterogeneity by capacity
Huang and Said	2025	Cross-country	Systematic review	FinTech raises efficiency, with unexplained variation in magnitude	Frames the boundary-condition question
Uddin et al.	2020	Cross-country	Panel	Cyber spending volume alone does not determine stability	Separates spending from capability
Hasan et al.	2021	Cross-sector	PLS-SEM	Cyber readiness improves security and organisational performance	Source of the readiness construct
Türegün	2025	International	Regression	Strategic integration matters more than spending volume	Supports the capability framing
Al Hammadi et al.	2024	UAE Islamic banks	Moderation analysis	IT security capability moderates the FinTech effect	Closest moderation test, different outcome
Murungu et al.	2026	Zimbabwe	Survey regression	Cybersecurity strategies enable digital transformation	Cybersecurity as enabler
Hanifan et al.	2026	Indonesia	Panel with interaction	Cyber risk management maturity raises the FinTech payoff	Closest direct moderation test
Al-Omoush	2026	Jordan, 247 respondents	PLS-SEM	AI and cybersecurity drive FinTech innovation and operational excellence	Mediated rather than moderated specification

Source: own processing

Variables and hypotheses

FinTech in banking

Financial technology encompasses digital innovations in financial products, processes, and distribution channels. Candraningrat et al. (2021) describe it as the application of modern digital technology within finance to create products and services that improve

Vol.14 (2026) no.3, pp.344-365; DOI 10.2478/mdke-2026-0019

operational efficacy and stability, while the Financial Stability Board (2017) defines it more expansively as technology-driven innovation that can produce new business models, applications, processes, or products with significant impact on institutions, markets, and service provision. At the bank level, the operational substance matters more than the definition: FinTech in a commercial bank comprises mobile and online banking, digital payment systems, automated credit processes, electronic onboarding, application programming interfaces to external entities, and internal data analytics. We assess adoption across these parameters.

Cybersecurity readiness and its dimensions

Cybersecurity readiness evaluates an organisation's ability to prevent, identify, respond to, and recover from cyber events. Hasan et al. (2021) characterise it as the degree of awareness, preparedness, and commitment an organisation holds in relation to preventing and addressing cyberattacks; Makridis and Smeets (2019) add response and recovery, describing readiness as an overall state of preparedness supported by technical and organisational frameworks; and the NIST framework groups the same content into five functions: identify, protect, detect, respond, and recover (National Institute of Standards and Technology, 2024).

We analyse readiness in two dimensions, aligning with the distinction between technological and human elements in the NIST functions and with the measurement framework of Hasan et al. (2021). Technical readiness encompasses secure information systems, security frameworks, ongoing surveillance and detection, backup and recovery, and the adaptability needed to confront evolving threats (International Organization for Standardization & International Electrotechnical Commission, 2022; National Institute of Standards and Technology, 2018). Human readiness encompasses proficiency in using security technologies, identifying threats, responding to incidents, and maintaining a security-focused culture through training (European Union Agency for Network and Information Security, 2018; Von Solms & Van Niekerk, 2013). The division carries analytical significance: technological readiness without human readiness yields tools personnel cannot use effectively, whereas human readiness without technological readiness leaves vigilant personnel without tools, and neither dimension can substitute for the other. We therefore define readiness as a second-order construct requiring both elements rather than a single cumulative measure.

Operational efficiency

Operational efficiency refers to delivering financial services at the lowest cost, minimising resource waste, and ensuring uninterrupted availability. Bank-level studies assess it in three ways: frontier scores (from data envelopment analysis or stochastic frontier analysis), the cost-to-income ratio as the accounting approach, and survey-derived constructs capturing processing speed, error frequency, and service quality. We use the third because our unit is a branch network rather than a bank population, which precludes frontier estimation, and because survey measurement captures operational elements that accounting data overlook: transaction-processing duration, error incidence, system uptime, and personnel capacity to manage workload. These are the mechanisms through which FinTech operates, and a cost-to-income ratio consolidates them into a single metric that cannot separate them. Al-Omoush (2026) uses the same construct family in Jordanian banking.

We assess operational efficiency via three facets: process acceleration (transaction velocity and service duration), cost minimisation (operating expenses, resource efficiency, and rework), and financial inclusion (accessibility across the client base). The third facet requires justification, since inclusion is often treated as an outcome rather than a component of efficiency. We regard it as operational because it captures the bank's ability to serve more clients without a proportional rise in resources: digital platforms dissociate service quantity from branch and staffing limits, so a network serving a broader clientele

with the same resources exemplifies production efficiency, with reach as its tangible branch-level manifestation. Banna et al. (2023) find FinTech-driven inclusion correlating positively with banking efficiency in dual banking systems, which supports treating the two as interrelated rather than distinct outcomes.

Complementarity and hypotheses

Two frameworks underpin the argument: complementarity theory supplies the mechanism, and the resource-based perspective explains why the supplementary asset is a strategic capability rather than a mere operating cost. Complementarity theory holds that the yield from one investment increases with the magnitude of a corresponding investment, so technology investment produces productivity benefits only when the organisation holds the complementary assets to use it. Here FinTech infrastructure is the technological investment and cybersecurity readiness the supplementary asset; without the complement, digital adoption becomes exposure rather than efficiency. The resource-based perspective explains why readiness is a strategic complement: it develops gradually, embeds in employee skills and organisational procedures, and cannot be bought outright, so it qualifies as a competence yielding durable rather than fleeting advantage, unlike security expenditures any bank can quickly imitate.

The direct association of FinTech adoption follows from the mechanisms outlined earlier: digital platforms lower transaction-processing cost, automation reduces errors and rework, and scalable systems add volume without a proportional rise in personnel.

H1: FinTech adoption has a positive and significant effect on operational efficiency.

The direct association of cybersecurity readiness follows a different route: readiness reduces the operating cost of incidents. Detection shortens the interval between breach and mitigation, response protocols cut cleanup hours, and recovery measures limit disruption, each carrying operational value regardless of how much technology the bank has deployed, since incidents impose costs on manual and digital procedures alike.

H2: Cybersecurity readiness has a positive and significant direct effect on operational efficiency.

The moderation follows from complementarity: as digital integration intensifies, the vulnerability surface widens and the cost of weak readiness rises. A bank with robust readiness absorbs the same adoption with less disruption, converting more of it into realised efficiency, so the interaction should be positive.

H3: Cybersecurity readiness positively moderates the relationship between FinTech adoption and operational efficiency, such that the effect of FinTech adoption is stronger at higher levels of readiness.

Figure 1 illustrates the theoretical framework. FinTech adoption serves as the independent variable. Operational efficiency serves as the dependent variable, assessed via process acceleration, cost minimisation, and financial inclusion. Cybersecurity readiness, assessed via technical and human dimensions, serves as both a direct predictor of operational efficiency and a moderator of the relationship between FinTech adoption and operational efficiency.

Vol.14 (2026) no.3, pp.344-365; DOI 10.2478/mdke-2026-0019

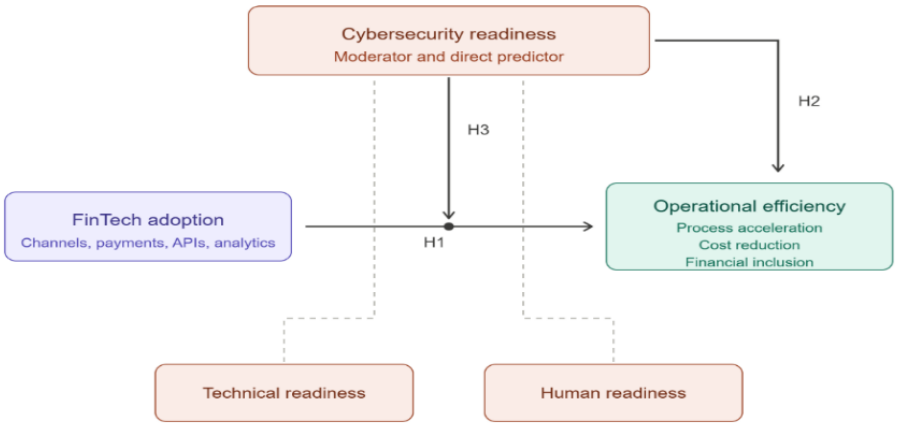


Figure 1. Conceptual model: Cybersecurity readiness as a boundary condition of the FinTech–operational efficiency relationship
Source: own processing

Data and methodology

Research setting

Crédit Populaire d'Algérie (CPA) is one of the six state-owned commercial banks in Algeria. Its branch network in Mila province serves retail and small-business clients through conventional counter services and recently implemented digital platforms, including electronic payment cards, automated transaction processing, and remote banking. The bank exemplifies the model outlined in the Algerian context section: digital capability emerges from national initiatives and institutional mandates rather than competitive forces, producing disparities in organisational readiness among units operating at comparable levels of adoption.

Sample and data collection

Data were gathered from employees of Crédit Populaire d'Algérie in Mila province during March and April 2026. We used purposive sampling, targeting personnel whose roles provide direct exposure to the bank's digital infrastructure and information-security protocols; this excluded staff whose positions lack exposure to the constructs, whose responses would add measurement error rather than variation. We distributed 60 questionnaires in physical and digital form and obtained 55 valid responses, an effective response rate of 91.7 per cent. The rate reflects the distribution technique, not atypical respondent eagerness: we distributed questionnaires directly at branch offices with in-person follow-up, which reduced the non-return rates associated with postal or open electronic dissemination. The purposive design also contributed, since we engaged personnel for whom the questionnaire was relevant to their routine tasks.

Sample size adequacy

The sample of 55 requires justification, as it falls below standard power calculations. The ten-times rule sets the minimum at ten times the largest number of paths directed at any endogenous construct; with three paths to operational efficiency, the minimum is 30, which the sample meets. The rule neglects statistical power, however: a three-predictor model needs roughly 77 observations to detect a medium effect ($f^2 = 0.15$) at $\alpha = 0.05$ and power = 0.80, so the sample is insufficient for medium effects. Two considerations bound this. First, the effects here are large rather than medium, since the model accounts for 78.0 per cent of the variance in operational efficiency, with the lowest path coefficient at 0.243

(t = 2.808), and a sample of 55 offers adequate power at that magnitude. Second, interaction terms require more power than direct effects, so detecting a significant moderation (β = 0.330, t = 4.922) at this sample size indicates a substantial effect: underpowered designs fail to detect genuine effects rather than manufacturing spurious ones at this level of significance. The residual limitation is generalisation, not estimation: 55 respondents from one branch network support inferences within this organisation, not about the Algerian banking industry, which we treat as a constraint in the discussion.

Respondent profile

Table 2 reports the demographic composition of the sample. Male participants constitute 67.3 per cent and female participants 32.7 per cent. Those aged 26 to 45 represent 92.7 per cent (54.5 per cent in the 26 to 35 group). Educational attainment is high: 90.9 per cent hold university degrees and 52.7 per cent Master's degrees. This matters for measurement validity, since both cybersecurity readiness and FinTech adoption require participants to assess technical frameworks they engage with directly, and a sample of degree-holders in operational roles supports the assumption that respondents understood the concepts evaluated.

Table 2. Respondent profile

Characteristic	Category	Frequency	Percentage
Gender	Male	37	67.3
	Female	18	32.7
	Total	55	100.0
Age	25 years or under	2	3.6
	26 to 35 years	30	54.5
	36 to 45 years	21	38.2
	Over 45 years	2	3.6
	Total	55	100.0
Education	Bachelor's degree	16	29.1
	Master's degree	29	52.7
	Doctorate	5	9.1
	Other qualification	5	9.1
	Total	55	100.0

Source: own processing based on SPSS 27 output

Measurement instrument

All dimensions were assessed using multi-item reflective scales on a five-point Likert scale (1 = strongly disagree, 5 = strongly agree). FinTech adoption has six items: mobile and online banking platforms, digital payment systems, automated transaction management, electronic customer onboarding, third-party application interfaces, and technology-enhanced internal decision-making. Cybersecurity readiness comprises nine items across two dimensions: technical readiness (five items on the up-to-date status of ICT systems, security frameworks, monitoring and detection, backup and recovery, and operational flexibility) and human readiness (four items on staff proficiency in managing security systems, understanding of information-system frameworks, threat identification and escalation, and the cultivation of a security-oriented culture), adapted from Hasan et al. (2021). Operational efficiency comprises ten items across three dimensions: process acceleration (three items on transaction velocity and service duration), cost reduction (four items on operating expenses, resource efficiency, and rework), and financial inclusion (three items on service availability and client accessibility).

Analytical approach

We used partial least squares structural equation modelling in SmartPLS 4 to test the hypotheses and SPSS 27 for descriptive statistics. PLS-SEM suits this study because it accommodates second-order constructs, performs reliably with small samples without

Vol.14 (2026) no.3, pp.344-365; DOI 10.2478/mdke-2026-0019

assuming multivariate normality, and is oriented towards prediction and theory extension rather than confirmation. Cybersecurity readiness and operational efficiency were specified as reflective second-order constructs measured through their first-order dimensions, and the moderation was modelled in two stages, producing latent-variable scores first and computing the interaction term second, a method appropriate for higher-order constructs. We evaluated the measurement model via factor loadings, Cronbach's alpha, rho_A, composite reliability, average variance extracted, the variance inflation factor, the Fornell-Larcker criterion, and HTMT, and the structural model via the coefficient of determination, effect size, the standardised root mean square residual, and path significance from bootstrapping with 5,000 subsamples.

Common method bias

Because respondents rated both predictors and outcomes, we assessed common method bias with the full collinearity method: all variance inflation factors fell below the 3.3 threshold, indicating that method variance did not jeopardise the estimates. We also applied procedural remedies during data collection, guaranteeing confidentiality, defining the construct components in the survey, and avoiding evaluative wording that could prompt socially desirable responses. We return to this concern, and to construct overlap, in the limitations.

Results

Measurement model assessment

Model validation requires evaluating the measurement model before the structural model. This evaluation covers convergent validity, internal-consistency reliability, multicollinearity, and discriminant validity. This sequence confirms that the measurement instruments are of satisfactory quality and that the constructs are distinct, enabling dependable hypothesis testing thereafter.

Convergent validity, reliability, and multicollinearity

The measurement model meets established standards (Table 3).

Table 3. Convergent validity, reliability, and multicollinearity assessment

Variable	Factors	Items	Loadings (FL)	Cronbach's Alpha	RHO-A	Composite Reliability (CR)	Average Variance Extracted (AVE)	Variance Inflation Factor (VIF)
FinTech adoption		**Item 1**	0.916	0.944	0.945	0.955	0.782	4.794
		Item 2	0.902					4.779
		Item 3	0.848					2.823
		Item 4	0.848					2.779
		Item 5	0.896					3.537
		Item 6	0.893					4.165
Cybersecurity readiness	**Technical readiness**	**Item 7**	0.874	0.918	0.920	0.939	0.754	2.910
		Item 8	0.840					2.506
		Item 9	0.900					3.388
		Item 10	0.820					2.208
		Item 11	0.905					3.570
	Human readiness	**Item 12**	0.807	0.907	0.914	0.935	0.783	2.080
		Item 13	0.915					3.893
		Item 14	0.914					3.457
		Item 15	0.898					3.377
Operational efficiency	**Process acceleration**	**Item 16**	0.941	0.918	0.918	0.948	0.859	3.851
		Item 17	0.918					3.042
		Item 18	0.922					3.201
	Cost reduction	**Item 19**	0.889	0.889	0.901	0.924	0.752	2.902
		Item 20	0.882					2.685

		Item 21	0.928				3.846
		Item 22	0.762				1.678
	Financial inclusion	**Item 23**	0.950	0.920	0.922	0.949	0.862	4.677
		Item 24	0.899				2.676
		Item 25	0.935				3.984

Source: own processing based on SmartPLS 4 output

All factor loadings exceed the 0.70 benchmark, from 0.762 (Item 22) to 0.950 (Item 23). Cronbach's alpha (0.889 to 0.944) and composite reliability (0.924 to 0.955) both exceed 0.70, confirming internal consistency, and average variance extracted (0.752 to 0.862) exceeds 0.50, confirming convergent validity. VIF values range from 1.678 to 4.794, below the conservative threshold of 5.0; six values exceed 3.5 and two approach 4.8, indicating some redundancy within the FinTech adoption and financial inclusion blocks, but we retained all indicators, since removing them would narrow the conceptual breadth of the constructs without improving the already satisfactory reliability. Figure 2 illustrates the measurement model with all standardised loadings.

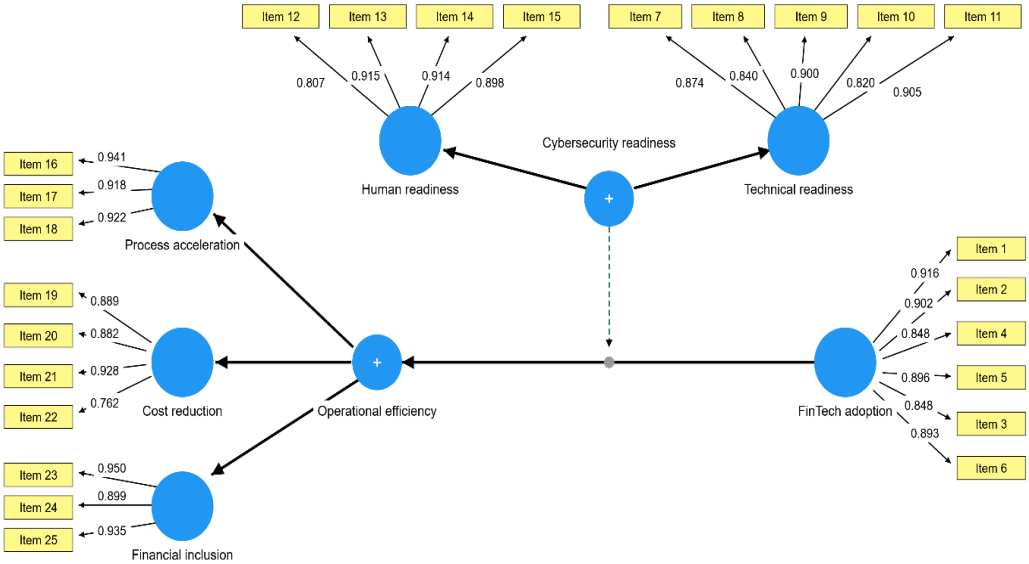


Figure 2. Measurement model with standardised factor loadings
Source: own processing based on SmartPLS 4 output

Discriminant validity

Discriminant validity requires that each construct share more variance with its own indicators than with any other construct. Table 4 presents the Fornell-Larcker results, with the square root of AVE on the diagonal and inter-construct correlations below it.

Table 4. Discriminant validity, Fornell-Larcker criterion

Variables	**Human readiness**	**Technical readiness**	**Financial inclusion**	**Cost reduction**	**Process acceleration**
Human readiness	**0.917**				
Technical readiness	0.885	**0.868**			
Financial inclusion	0.080	0.164	**0.971**		
Cost reduction	0.003	0.049	0.891	**0.883**	
Process acceleration	0.080	0.166	0.928	0.867	**0.927**

Notes: Diagonal values in bold are square roots of AVE. Off-diagonal values are construct correlations.
Source: own processing based on SmartPLS 4 output

Three of the five first-order constructs meet the criterion unconditionally: human readiness (0.917), financial inclusion (0.971), and process acceleration (0.927) each

Vol.14 (2026) no.3, pp.344-365; DOI 10.2478/mdke-2026-0019

exceed their correlations with other constructs. Two constructs record minor exceedances that require disclosure. Technical readiness (0.868) sits just below its 0.885 correlation with human readiness, a difference of 0.017, and cost reduction (0.883) below its 0.891 correlation with financial inclusion, a difference of 0.008. These exceedances stem from the model specification rather than measurement inaccuracy: technical and human readiness load at 0.983 and 0.975 on cybersecurity readiness, and the efficiency dimensions load at 0.977, 0.956, and 0.980 on operational efficiency (all $p < 0.001$), so two dimensions above 0.97 on a shared second-order construct are inherently correlated because they express the same underlying capability. The Fornell-Larcker criterion evaluates the distinctiveness of separate constructs; when applied to dimensions of a single second-order construct, it tests a hypothesis the model does not make. Because these exceedances involve dimensions of the same second-order construct, and because Fornell-Larcker is less sensitive than more recent tests, we also report the heterotrait-monotrait ratio (HTMT), which Henseler et al. (2015) recommend as the primary discriminant-validity criterion. Table 5 presents the HTMT matrix.

Table 5. Discriminant validity, Heterotrait-Monotrait ratio (HTMT)

Variables	Human readiness	Technical readiness	Financial inclusion	Cost reduction	Process acceleration
Human readiness	–				
Technical readiness	0.725	–			
Financial inclusion	0.123	0.181	–		
Cost reduction	0.137	0.143	0.779	–	
Process acceleration	0.116	0.188	0.557	0.771	–

Note: Values below 0.85 indicate discriminant validity.

Source: own processing based on SmartPLS 4 output

The HTMT results confirm discriminant validity across the model's dimensions. All values fall below the accepted 0.85 threshold, ranging from 0.116 to 0.779, consistent with Hair et al.'s (2017) recommendation that HTMT values below this level indicate clear conceptual and statistical distinction between latent constructs, with no substantial overlap. The highest value, 0.779, appears between financial inclusion and cost reduction, followed by 0.771 between cost reduction and process acceleration; both remain within acceptable limits and reflect the shared membership of these dimensions in the same latent construct, operational efficiency, without compromising each dimension's distinctiveness. The HTMT value between human readiness and technical readiness is 0.725, which reflects a logical link between the two as components of cybersecurity readiness. At the same time, each retains its conceptual and statistical distinction. Overall, the HTMT results support the discriminant validity of the measurement model and reinforce the Fornell-Larcker findings, strengthening confidence in the measurement model and its adequacy for proceeding to the structural model and the hypothesis tests.

Structural model assessment

Coefficient of determination

The model accounts for 78.0 per cent of the variance in operational efficiency, with an adjusted figure of 76.7 per cent (Table 6).

Table 6. Coefficient of determination

Endogenous construct	R^2	Adjusted R^2
Operational efficiency	0.780	0.767

Source: own processing based on SmartPLS 4 output

Under the Hair et al. (2019) classification, an R^2 above 0.75 is considered substantial. The 1.3 percentage-point difference between the two figures indicates that the explanatory power does not result from the number of predictors included.

Effect size

Effect size quantifies the change in the coefficient of determination when an exogenous construct is removed from the model. Interpretation thresholds are 0.02 for a small effect, 0.15 for a medium effect, and 0.35 for a large effect; values below 0.02 indicate no substantive effect (Table 7).

Table 7. Effect size for structural paths

Path	f^2
FinTech adoption → Operational efficiency	3.430
Cybersecurity readiness → Operational efficiency	0.220
Cybersecurity readiness × FinTech adoption → Operational efficiency	0.467

Source: own processing based on SmartPLS 4 output

Effect estimates for the paths between second-order constructs and their first-order dimensions are excluded, since those represent measurement rather than structural relationships and their f^2 values are inflated by construction. FinTech adoption shows an effect size of 3.430, far above the large-effect benchmark; we present it as approximate and note that magnitudes above 1.0 lie beyond the range the Cohen thresholds were meant to interpret, so the figure signals the dominant status of FinTech within a model of few variables rather than a precise measure of relative importance. Cybersecurity readiness records 0.220, a medium effect, consistent with its smaller path coefficient in Table 9. The interaction term records 0.467, above the 0.35 large-effect benchmark. This is the figure of analytical significance: moderation effects in behavioural research generally yield small effect sizes, and values above 0.35 are rare, so the difference in FinTech returns between low- and high-readiness scenarios carries considerable practical importance beyond statistical significance.

Model fit

We assessed model fit through two indices. The standardised root mean square residual measures the discrepancy between observed and model-implied correlations (Table 8).

Table 8. Model fit indices

Model	SRMR
Saturated model	0.088
Estimated model	0.091

Source: own processing based on SmartPLS 4 output

The SRMR reaches 0.088 for the saturated model and 0.091 for the estimated model, both above the conventional 0.08 threshold of Hu and Bentler (1999). We do not treat the criterion as satisfied. Contemporary methodological guidance cautions against relying on global fit indices in PLS-SEM: Hair et al. (2019) note that PLS-SEM does not optimise a covariance-based fit function, that SRMR was imported from covariance-based SEM, and that its thresholds have not been validated for the variance-based estimator, so an exceeding SRMR does not by itself indicate misspecification, nor does a passing value confirm fit. Rather than interpret the value optimistically, we base our assessment of the model on the measurement-model criteria (all loadings, reliabilities, AVE, and HTMT within thresholds) and the structural-model criteria (R^2, f^2, and the significance and sign of the path estimates), which are the evaluation standards current PLS-SEM practice prioritises. We report the SRMR for transparency and comparability rather than as evidence of adequate fit, and we frame the study as exploratory partly because it exceeds the threshold. For comparability with earlier studies in the field, we also computed the goodness-of-fit index (GoF) as the geometric mean of the average AVE and the average

Vol.14 (2026) no.3, pp.344-365; DOI 10.2478/mdke-2026-0019

$\boldsymbol{GOF} = \sqrt{(\overline{\boldsymbol{R^2}} \times \overline{\boldsymbol{AVE}})}$which yields 0.789. We attach little weight to this value: the current PLS-SEM literature has largely abandoned GoF because, as Henseler and Sarstedt (2013) show, it does not reliably separate valid from misspecified models and lacks a meaningful threshold for rejecting a model. We report it only so readers can compare our results with prior work that used the index, and we do not treat it as evidence of model validity.

Hypothesis testing

Table 9 and Figure 3 present the structural model with path coefficients and significance levels.

Table 9. Path coefficients and hypothesis testing results

Path	O	M	STDEV	T	P	Decision
H1: FinTech adoption → Operational efficiency	0.938	0.942	0.060	15.512	0.000	Supported
H2: Cybersecurity readiness → Operational efficiency	0.243	0.240	0.086	2.808	0.005	Supported
H3: Cybersecurity readiness × FinTech adoption → Operational efficiency	0.330	0.330	0.067	4.922	0.000	Supported

Source: own processing based on SmartPLS 4 output

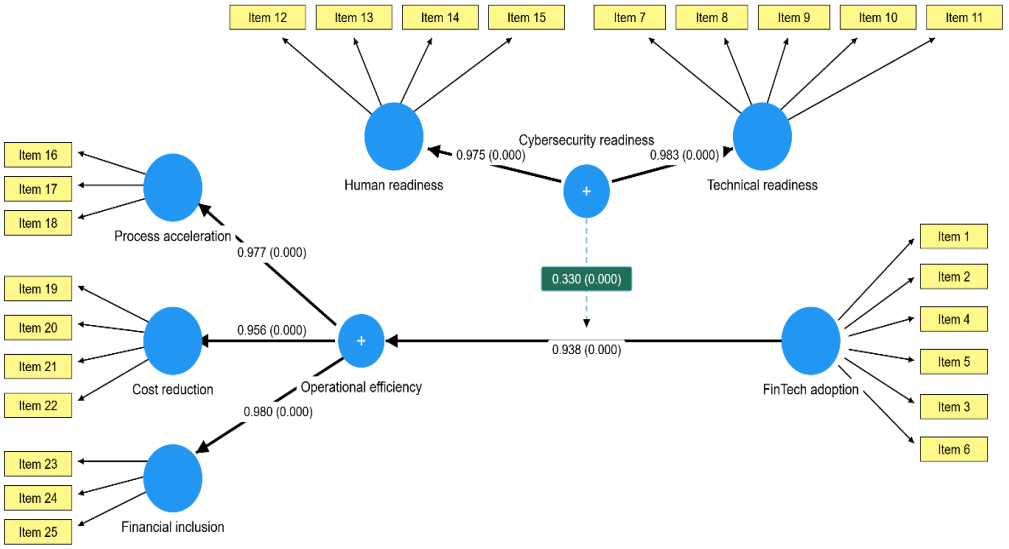


Figure 3. Structural model with path coefficients and p-values
Source: own processing based on SmartPLS 4 output

H1. The direct path from FinTech adoption to operational efficiency (β = 0.938, t = 15.512, p < 0.001) is positive, strong, and significant. Greater use of digital channels, automated processing, and electronic-payment infrastructure is associated with higher branch-level efficiency, consistent with faster transaction handling, fewer errors, and broader reach. H1 is supported.

H2. Cybersecurity readiness has a positive, significant direct association with operational efficiency (β = 0.243, t = 2.808, p = 0.005), smaller than the FinTech path. Higher security infrastructure and staff capability are associated with greater service continuity and less disruption, which relates to efficiency independently of the digital tools deployed. H2 is supported.

H3. The interaction term (β = 0.330, t = 4.922, p < 0.001) is positive and significant: the association between FinTech adoption and operational efficiency is stronger at higher levels of cybersecurity readiness. H3 is supported.

The moderation result carries the study's analytical weight. The pattern is consistent with FinTech adoption and cybersecurity readiness operating as complementary capabilities rather than independent investments: higher adoption is associated with the largest efficiency differences in units that also exhibit the technical and human capacity to operate digital systems securely.

Simple slopes analysis

To quantify moderation, we investigated the conditional effect of FinTech adoption on operational efficiency across three levels of compliance with cybersecurity standards (Table 10).

Table 10. Conditional effects of FinTech adoption at three levels of cybersecurity readiness

Level of cybersecurity readiness	O	M	STDEV	T	P
High (+1 SD)	1.268	1.272	0.112	11.285	0.000
Mean	0.938	0.942	0.060	15.512	0.000
Low (−1 SD)	0.608	0.612	0.061	10.004	0.000

Source: own processing based on SmartPLS 4 output

The conditional association increases steadily with readiness. At one standard deviation below the mean, the association between FinTech adoption and operational efficiency is 0.608; at the mean, it is 0.938; and at one standard deviation above the mean, it reaches 1.268, all significant at p < 0.001. The gap of 0.660 between the low- and high-readiness states indicates that, for a given rise in adoption, a bank with strong readiness is associated with roughly double the efficiency difference observed in a low-readiness bank. The association remains positive and significant even at low readiness, so inadequate security capacity is not linked to the absence of a digital return; it is associated with roughly half the return. The moderation is thus reinforcing rather than restricting: readiness is associated with the share of the potential difference a bank exhibits, not with whether any positive association exists. Figure 4 illustrates the simple-slope plot.

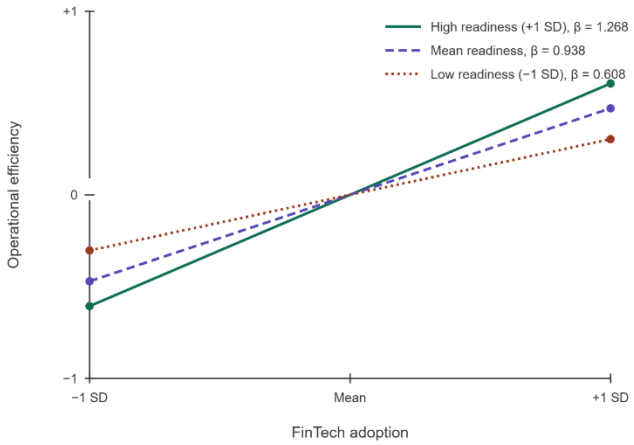


Figure 4. Simple slope plot of the moderating effect of cybersecurity readiness
Source: own processing based on SmartPLS 4 output

Vol.14 (2026) no.3, pp.344-365; DOI 10.2478/mdke-2026-0019

Discussion

Summary of findings

This research asked whether a bank's cybersecurity readiness is associated with the operational efficiency observed alongside FinTech integration, and the findings answer affirmatively on three counts. FinTech adoption is strongly and positively associated with operational efficiency ($\beta = 0.938$, $p < 0.001$), cybersecurity readiness relates to it independently ($\beta = 0.243$, $p = 0.005$), and their interaction is positive and significant ($\beta = 0.330$, $p < 0.001$), with the model accounting for 78.0 per cent of the variance. The moderation bears the analytical weight: the association rises from 0.608 at low readiness to 1.268 at high readiness, so a comparable degree of adoption is linked to roughly double the efficiency difference where security capability is greater. Because the data come from one branch network and the design is cross-sectional, these results describe associations within this organisation rather than causal or generalisable effects.

Theoretical implications

The findings are consistent with extending complementarity theory to the FinTech–efficiency relationship. Complementarity holds that the return to one investment rises with the magnitude of a corresponding one, and our results are compatible with cybersecurity readiness serving as that supplementary resource, such that in its absence digital adoption may amount to exposure rather than realised efficiency. The framework also offers a possible account of the conflicting evidence that motivated the study: the U-shape of Khan et al. (2024), the size effect of Juma Ally et al. (2025), and the negative aggregate of Lee et al. (2023) become more interpretable if readiness conditions the magnitude of the digital return, since analyses averaging across banks of varying readiness would yield divergent outcomes. We advance this as an interpretation consistent with our cross-sectional associations, not a demonstrated causal mechanism, which would require longitudinal or multi-bank evidence.

The result also speaks to how the literature treats cybersecurity. Most research frames it as a protective expenditure that guards against loss. Türegün (2025) advanced a capability perspective by showing that strategic integration matters more than spending, and Murungu et al. (2026) framed cybersecurity measures as enablers of digital transformation. Our results align with that view: readiness appears associated with more than loss avoidance, since higher readiness is linked to a stronger positive association between adoption and efficiency. The finding aligns directionally with Hanifan et al. (2026) despite a different institutional context and outcome metric, and this convergence lends tentative support to treating readiness as a boundary condition worth testing across settings rather than a purely context-specific one.

Practical implications

Read with appropriate caution, the associations suggest a sequencing consideration for bank management: cybersecurity allocation may be more effective when incorporated into the digitalisation budget than when treated as a separate, risk-justified line item. Where a bank builds digital platforms faster than it develops its detection, response, and staff competencies, our pattern is consistent with digital channel uptake being accompanied by a smaller realised efficiency benefit. We frame this as a plausible managerial implication of an association rather than a proven causal prescription.

Because both dimensions load above 0.97 on the readiness construct, they express a single capability rather than two interchangeable ones, so financing the technical dimension while postponing the human one builds a diminished capability, not a partial one. For Algerian banking, the pattern suggests integrating two agendas that now run separately—digital transition through legislative and institutional mandates, and cybersecurity

through prudential channels—since the productivity relevance of digital investment appears tied to the accompanying security capability.

Policy implications

The result also situates cybersecurity oversight within the productivity agenda rather than alongside it. Supervisory attention to incident documentation, resilience assessment, and personnel accreditation is usually justified by stability; our findings suggest a possible efficiency justification as well, since units with superior readiness are associated with greater operational benefit from digital investment, so strengthening supervisory capacity may relate to returns in both sector productivity and safety. The International Monetary Fund (2024) observes that cybersecurity structures in emerging and developing nations remain deficient in oversight practices, incident-reporting protocols, and testing frameworks, and our findings are consistent with treating the reduction of those gaps as part of the productivity agenda rather than a separate concern. This consideration may matter most where regulatory mandates drive adoption rather than competitive choice, since required adoption does not automatically confer the capacity to absorb new technology, and a digitalisation initiative that funds channels without confirming readiness risks producing adoption metrics without commensurate productivity improvements. We advance these as policy-relevant implications of an association observed in one bank, to be tested on broader samples before informing regulation.

Limitations

Several limitations bound these conclusions and shape how they should be read. First and most important, the sample comprises 55 employees of a single branch network of one Algerian public bank. The results therefore describe associations within this organisation and cannot be generalised to Crédit Populaire d'Algérie as a whole, to Algerian public banking, or to emerging-market banking; throughout the revised manuscript we have restricted the wording of the findings to this scope. The sample is also below the level a conventional power analysis suggests for medium effects, though adequate for the large effects observed, so the study is best regarded as exploratory. Second, because all constructs are self-reported by the same respondents, common method bias and construct overlap are genuine concerns. We applied procedural remedies (confidentiality, defined constructs, non-evaluative item wording) and a statistical check (full collinearity VIF < 3.3), and we now report HTMT alongside Fornell-Larcker to address discriminant validity; nevertheless, single-source data cannot fully rule out inflation of the observed relationships, and the exceptionally strong FinTech–efficiency path ($\beta = 0.938$) and high R^2 (0.780) should be read with this caveat. Third, the design is cross-sectional, so the estimates are associations, not causal effects: a bank that already operates efficiently might invest more in readiness, producing a similar pattern through the reverse path. Fourth, operational efficiency is measured perceptually rather than from audited cost or transaction data, and perceived and accounting efficiency may diverge. Fifth, global fit in PLS-SEM is limited: the estimated SRMR (0.091) exceeds the 0.08 threshold, and GoF is not a reliable model-selection criterion, so our assessment rests on the measurement- and structural-model criteria rather than a single fit index. Finally, the moderator combines human and technical readiness into one second-order variable, so the analysis shows that readiness conditions the association without establishing which dimension drives it.

Directions for future research

Several directions follow. Replication across Algerian public and private banks would show how ownership affects the moderation and establishes generalisability. Combining the survey with branch-level cost-to-income data would test whether perceived and accounting efficiency converge. Decomposing the moderator would reveal which facet of readiness drives the interaction, guiding investment priorities that our aggregate results leave open. Disaggregating FinTech adoption would help, since payment channels, credit

Vol.14 (2026) no.3, pp.344-365; DOI 10.2478/mdke-2026-0019

algorithms, and open APIs carry different exposure profiles. Finally, a longitudinal design would permit tests of causality and of whether the cross-country U-shape reflects the capability accumulation our results suggest.

Conclusions

Within this single Algerian public bank, the degree to which units are equipped to confront cybersecurity threats is associated with the operational efficiency observed alongside FinTech adoption. The association between adoption and efficiency is 0.608 under low readiness and 1.268 under high readiness, so that, for a comparable degree of digital adoption, greater security capability is linked to roughly double the efficiency difference. Read cautiously, this pattern invites a reconsideration of what cybersecurity does. Most studies characterise it as a protective expenditure that mitigates losses; our results are additionally consistent with its acting as a complementary capability associated with larger efficiency differences. This distinction shifts the managerial question from how much to allocate to security to when to develop it, and the study points—tentatively, given its design—toward building readiness alongside digital adoption rather than after it. On this evidence, readiness may not only limit the exposure digitalisation creates but also be part of what is associated with translating digitalisation into efficiency. These readings remain associational and specific to the studied organisation; establishing causation and generalisability requires longitudinal and multi-bank research.

The study's contribution lies in testing cybersecurity readiness as a boundary condition of the FinTech–efficiency relationship, doing so with operational efficiency as the outcome, and providing early evidence from an Algerian public bank. Its tentative practical implication is a sequencing consideration that would integrate security capability into the digital-transformation agenda for both managers and regulators, subject to confirmation on larger and longitudinal samples.

References

Al Hammadi, M., Jimber-Del Río, J. A., Ochoa-Rico, M. S., Montero, O. A., & Vergara-Romero, A. (2024). Risk management in Islamic banking: The impact of financial technologies through empirical insights from the UAE. *Risks, 12*(2), Article 17. https://doi.org/10.3390/risks12020017

AlBenJasim, S., Dargahi, T., Takruri, H., & Al-Zaidi, R. (2024). FinTech cybersecurity challenges and regulations: Bahrain case study. *Journal of Computer Information Systems, 64*(6), 835–851. https://doi.org/10.1080/08874417.2023.2251455

Ally, O. J., Kulindwa, Y., & Mataba, L. (2025). Bank efficiency in the digital age: The role of financial technology in Tanzanian banks. *Modern Finance, 3*(1), 1–24. https://doi.org/10.61351/mf.v3i1.218

Al-Omoush, K. S. (2026). AI-driven cybersecurity as an enabler of fintech innovation: Evidence from Jordanian banks. *Journal of Financial Services Marketing, 31*(1), Article 20. https://doi.org/10.1057/s41264-026-00345-y

Al-Shari, H. A., & Lokhande, M. A. (2023). The relationship between the risks of adopting FinTech in banks and their impact on performance. *Cogent Business & Management, 10*(1), Article 2174242. https://doi.org/10.1080/23311975.2023.2174242

Banna, H., Hassan, M. K., & Bataineh, H. (2023). Bank efficiency and fintech-based inclusive finance: Evidence from dual banking system. *Journal of Islamic Monetary Economics and Finance, 9*(1), 1–16. https://doi.org/10.21098/jimf.v9i1.1621

Bartoo, H., Warui, S., & Kasisi, R. (2025). Financial technology adoption and technical efficiency of commercial banks in Kenya. *Journal of Finance and Accounting, 13*(2), 64–70. https://doi.org/10.11648/j.jfa.20251302.11

Berlilana, Noparumpa, T., Ruangkanjanases, A., Hariguna, T., & Sarmini. (2021). Organization benefit as an outcome of organizational security adoption: The role of

cyber security readiness and technology readiness. *Sustainability, 13*(24), Article 13761. https://doi.org/10.3390/su132413761

Candraningrat, I. R., Abundanti, N., Mujiati, N. W., Erlangga, R., & Jhuniantara, I. M. G. (2021). The role of financial technology on development of MSMEs. *Accounting, 7*(1), 225–230. https://doi.org/10.5267/j.ac.2020.9.014

Cele, N. N., & Kwenda, S. (2025). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. *Journal of Financial Crime, 32*(1), 31–48. https://doi.org/10.1108/JFC-10-2023-0263

Cheng, S., Li, J., Luo, L., & Zhu, Y. (2024). Cybersecurity governance and digital finance: Evidence from sovereign states. *Finance Research Letters, 65*, Article 105533. https://doi.org/10.1016/j.frl.2024.105533

Elmahdy, A. H. A. M., Abdelkader, M. T. K. M., & Shaker, M. A. M. (2025). Bridging the nexus between Fintech, operational efficiency and banks profitability: The moderating role of bank size. *Future Business Journal, 11*(1), Article 62. https://doi.org/10.1186/s43093-025-00478-x

Elsayed, D. H., Ismail, T. H., & Ahmed, E. A. (2024). The impact of cybersecurity disclosure on banks' performance: The moderating role of corporate governance in the MENA region. *Future Business Journal, 10*(1), Article 115. https://doi.org/10.1186/s43093-024-00402-9

European Union Agency for Network and Information Security. (2018). *Cybersecurity culture guidelines: Behavioural aspects of cybersecurity*. https://doi.org/10.2824/324042

Financial Stability Board. (2017). *Financial stability implications from FinTech: Supervisory and regulatory issues that merit authorities' attention*. https://www.fsb.org/uploads/R270617.pdf

Goel, R., & Kashiramka, S. (2026). FinTech advancement in the banking industry: Is it driving efficiency? *International Journal of Finance & Economics, 31*(1), 842–868. https://doi.org/10.1002/ijfe.3170

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM)* (2nd ed.). SAGE Publications.

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review, 31*(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203

Hanifan, M. Z., Wahyuni, N. A. S., Agung, S., & Adeoye, M. A. (2026). Digitalization and bank financial performance: The role of fintech lending and cyber risk management in Indonesia. *Indonesian Journal of Social Research, 8*(1), 101–116. https://doi.org/10.30997/ijsr.v8i1.970

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications, 58*, Article 102726. https://doi.org/10.1016/j.jisa.2020.102726

Henseler, J., & Sarstedt, M. (2013). Goodness-of-fit indices for partial least squares path modeling. *Computational Statistics, 28*(2), 565–580. https://doi.org/10.1007/s00180-012-0317-1

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science, 43*(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8

Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal, 6*(1), 1–55. https://doi.org/10.1080/10705519909540118

Huang, X., & Said, F. F. (2025). Assessing the impact of financial technology on the efficiency of banks: A systematic literature review approach. *Risk Governance and Control: Financial Markets & Institutions, 15*(4), 85–96. https://doi.org/10.22495/rgcv15i4p8

Iatzaz Ul Hassan, M., Wu, M., Lu, J., Sohu, J. M., Ali, S., Anjum, H. N., & Bilal, M. (2025). Financial technology and banking performance in developing countries: Evidence from an

advanced quantile regression approach. *Humanities and Social Sciences Communications, 12*(1), Article 1455. https://doi.org/10.1057/s41599-025-05571-8

International Monetary Fund. (2024). Cyber risk: A growing concern for macrofinancial stability. In *Global financial stability report: The last mile: Financial vulnerabilities and risks* (pp. 77–100). https://doi.org/10.5089/9798400257704.082

International Organization for Standardization, & International Electrotechnical Commission. (2022). *Information security, cybersecurity and privacy protection—Information security management systems—Requirements* (ISO/IEC Standard No. 27001:2022). https://www.iso.org/standard/27001

Jafri, J. A., Amin, S. I. M., Rahman, A. A., & Nor, S. M. (2024). A systematic literature review of the role of trust and security on Fintech adoption in banking. *Heliyon, 10*(1), Article e22980. https://doi.org/10.1016/j.heliyon.2023.e22980

Kayed, S., Alta'any, M., Meqbel, R., Khatatbeh, I. N., & Mahafzah, A. (2025). Bank FinTech and bank performance: Evidence from an emerging market. *Journal of Financial Reporting and Accounting, 23*(2), 518–535. https://doi.org/10.1108/JFRA-09-2023-0526

Khan, H. H., Kutan, A. M., & Qureshi, F. (2024). Fintech integration: Driving efficiency in banking institutions across the developing nations. *Finance Research Letters, 67*, Article 105772. https://doi.org/10.1016/j.frl.2024.105772

Lee, C.-C., Li, X., Yu, C.-H., & Zhao, J. (2021). Does fintech innovation improve bank efficiency? Evidence from China's banking industry. *International Review of Economics & Finance, 74*, 468–483. https://doi.org/10.1016/j.iref.2021.03.009

Lee, C.-C., Ni, W., & Zhang, X. (2023). FinTech development and commercial bank efficiency in China. *Global Finance Journal, 57*, Article 100850. https://doi.org/10.1016/j.gfj.2023.100850

Li, Y., Stasinakis, C., Yeo, W. M., & Fernandes, F. D. S. (2025). Fintech, financial development and banking efficiency: Evidence from Chinese commercial banks. *The European Journal of Finance, 31*(10), 1245–1295. https://doi.org/10.1080/1351847X.2025.2468481

Makridis, C. A., & Smeets, M. (2019). Determinants of cyber readiness. *Journal of Cyber Policy, 4*(1), 72–89. https://doi.org/10.1080/23738871.2019.1604781

Murungu, C. N., Kupfuwa, M., & Nyazema, M. (2026). Cybersecurity strategies as enablers of digital transformation in commercial banks: Evidence from Zimbabwe. *International Journal of Research and Innovation in Social Science, 10*(2), 4386–4396. https://doi.org/10.47772/ijriss.2026.10200321

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

Ononiwu, M. I., Onwuzulike, O. C., Shitu, K., & Ojo, O. O. (2024). The impact of digital transformation on banking operations in developing economies. *World Journal of Advanced Research and Reviews, 23*(3), 460–474. https://doi.org/10.30574/wjarr.2024.23.3.2706

Oyewole, A. T., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies application. *World Journal of Advanced Research and Reviews, 21*(3), 625–643. https://doi.org/10.30574/wjarr.2024.21.3.0707

Ristanović, V., Primorac, D., & Mulović Trgovac, A. (2025). Banking in the age of blockchain and FinTech: A hybrid efficiency framework for emerging economies. *Journal of Risk and Financial Management, 18*(8), Article 458. https://doi.org/10.3390/jrfm18080458

Sajid, R., Ayub, H., Malik, B. F., & Ellahi, A. (2023). The role of fintech on bank risk-taking: Mediating role of bank's operating efficiency. *Human Behavior and Emerging Technologies, 2023*, Article 7059307. https://doi.org/10.1155/2023/7059307

Türegün, N. (2025). Digital transformation and cybersecurity risks. *International Journal of Accounting Information Systems, 56*, Article 100749. https://doi.org/10.1016/j.accinf.2025.100749

Uddin, M. H., Mollah, S., & Ali, M. H. (2020). Does cyber tech spending matter for bank stability? *International Review of Financial Analysis, 72*, Article 101587. https://doi.org/10.1016/j.irfa.2020.101587

Uddin, M. H., Mollah, S., Islam, N., & Ali, M. H. (2023). Does digital transformation matter for operational risk exposure? *Technological Forecasting and Social Change, 197*, Article 122919. https://doi.org/10.1016/j.techfore.2023.122919

Umoga, U. J., Sodiya, E. O., Amoo, O. O., & Atadoga, A. (2024). A critical review of emerging cybersecurity threats in financial technologies. *International Journal of Science and Research Archive, 11*(1), 1810–1817. https://doi.org/10.30574/ijsra.2024.11.1.0284

Verma, S. S., Sreenu, N., & Kushwaha, G. S. (2025). Exploring the impact of financial technology on commercial banking efficiency. *Journal on Innovation and Sustainability RISUS, 16*(2), 94–106. https://doi.org/10.23925/2179-3565.2025v16i2p94-106

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Waliullah, M., George, M. Z. H., Hasan, M. T., Alam, M. K., Munira, M. S. K., & Siddiqui, N. A. (2025). Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: A systematic literature review. *American Journal of Advanced Technology and Engineering Solutions, 1*(1), 226–257. https://doi.org/10.63125/fh49gz18

Wang, Y., Sui, X., & Zhang, Q. (2021). Can fintech improve the efficiency of commercial banks? An analysis based on big data. *Research in International Business and Finance, 55*, Article 101338. https://doi.org/10.1016/j.ribaf.2020.101338

Zhao, J., Li, X., Yu, C.-H., Chen, S., & Lee, C.-C. (2022). Riding the FinTech innovation wave: FinTech, patents and bank performance. *Journal of International Money and Finance, 122*, Article 102552. https://doi.org/10.1016/j.jimonfin.2021.102552

Zhu, K., & Guo, L. (2024). Financial technology, inclusive finance and bank performance. *Finance Research Letters, 60*, Article 104872. https://doi.org/10.1016/j.frl.2023.104872

Vol.14 (2026) no.3, pp.344-365; DOI 10.2478/mdke-2026-0019

Appendix A. Survey instrument

All items were measured on a five-point Likert scale (1 = strongly disagree, 5 = strongly agree). The instrument was administered in Arabic; the English wording below is a translation. Item numbers correspond to the indicators reported in Table 2 (Item 1 to Item 25).

Section 1. FinTech adoption (Items 1–6)

1. The bank systematically relies on FinTech solutions in conducting its daily banking operations.
2. Digital systems and solutions are fully integrated into core banking operations, reducing reliance on manual and paper-based procedures.
3. The bank provides diverse digital channels (such as banking applications and internet banking) for payments, transfers, and banking services.
4. Digital channels enable customers to complete most banking services fully without needing to visit a branch.
5. The bank uses advanced digital systems to manage customer relationships and improve communication quality across multiple channels.
6. The bank uses advanced digital technologies for identity verification, compliance, and transaction monitoring (such as multi-factor authentication and e-KYC systems).

Section 2. Cybersecurity readiness — Technical readiness (Items 7–11)

7. The bank has a secure digital infrastructure that supports the efficient execution of its banking operations.
8. The bank has advanced systems and equipment to protect networks and systems from cyber threats.
9. Security systems and devices are updated regularly to address vulnerabilities and strengthen protection.
10. The bank has effective backup and data-recovery plans for emergencies.
11. The bank ensures the continuity of its technical systems and reduces the likelihood of interruption or downtime.

Section 3. Cybersecurity readiness — Human readiness (Items 12–15)

12. Bank staff receive periodic training on cybersecurity practices relevant to their duties.
13. The bank runs regular awareness programmes to strengthen a security culture among employees.
14. The bank has a specialised cyber-incident response team with clear tasks and authority.
15. Formal, clear, and accessible mechanisms exist for reporting incidents or suspicious behaviour.

Section 4. Operational efficiency — Process acceleration (Items 16–18)

16. FinTech adoption has reduced the time needed to complete banking transactions.
17. Digital solutions have simplified and organised banking procedures more efficiently.
18. FinTech has eased operational pressure and accelerated the processing of customer requests.

Section 5. Operational efficiency — Cost reduction (Items 19–22)

19. FinTech has reduced operational errors within the bank.
20. FinTech has improved the use of time and resources.
21. Digital solutions have improved the use of time and of human and material resources.
22. FinTech adoption has enabled the bank to deliver banking services of higher quality and greater efficiency.

Section 6. Operational efficiency — Financial inclusion (Items 23–25)

23. FinTech has facilitated access to banking services for underserved groups.
24. Digital banking services have reduced the cost of obtaining financial services for customers.
25. Digital solutions have simplified account-opening procedures and access to basic services.

© 2026 Author(s). This is an open-access article licensed under the Creative Commons Attribution-NonCommercial-NoDerivs License (http://creativecommons.org/licenses/by-nc-nd/4.0/).