INSTITUTIONAL CYBER RISK CONTROL AND FINANCIAL PERFORMANCE OF DEPOSIT MONEY BANKS IN NIGERIA

OSUNYIKANMI, Moses Albert
Department of Accounting, Adekunle Ajasin University, Akungba-Akoko
osunyikanmim@gmail.com, ORCID: https://orcid.org/0009-0009-6140-9364

SALEMCITY, Ayobaye (PhD)
Department of Auditing, University of South Africa
salema@unisa.ac.za, ayobaye.salemcity@aaua.edu.ng
ORCID: https://orcid.org/0009-0008-8259-3343

ADEGBOYEGUN, Adekunle Emmanuel (PhD)
Department of Accounting, Adekunle Ajasin University, Akungba-Akoko
adegbae@unisa.ac.za, ORCID: https://orcid.org/0000-0002-6895-6899

OLORUNTOBA, Rufus Sunday (PhD)
Department of Financial Governance, University of South Africa
sunday.oloruntoba@aaua.edu.ng, ORCID: https://orcid.org/0000-0001-7546-8896

DOI: https://doi.org/10.64633/wissj.v10i6.21

Keywords

Human Capacity Development, Cyber Risk Controls, Employee Training, Security Audit, Financial Performance

Abstract

Research Problem: *As cyber-crimes increase globally, Nigerian Deposit Money Banks (DMBs) invest in cybersecurity to mitigate any foul play. Despite this, it still remains empirically unclear whether human-capacity-based and audit-based cyber risk controls generate measurable financial returns, as existing studies largely treat such controls as compliance costs rather than testing their econometric link to profitability.*
Methods/Theory: *Anchored jointly in Human Capital Theory and Risk Management Theory, the study adopts an ex-post facto panel design to examine the effect of Employee Training and Awareness (ETA) and Regular Security Audit and Assessment (RSAA). Ten listed Nigerian DMBs were purposively selected between 2015 and 2024.*
Results: *Effects of ETA ($\beta = 10.581$, $p < 0.05$) and RSAA ($\beta = 227.832$, $p < 0.01$) on NOPAT were positive. They jointly explain 81.9% of its variance ($F = 199.419$, $p < 0.001$). RSAA emerged as the main financial-performance driver in the study.*
Conclusion: *Human capacity development and institutional audit controls are complementary, cybersecurity governance levers that jointly and significantly shape DMB profitability, with the structural (audit) pathway carrying a disproportionately larger financial return.*
Key Contribution to Knowledge: *The study provides one of the first*

integrated econometric tests of Human Capital Theory and Risk Management Theory within a single panel model for Nigerian DMB cybersecurity governance.
Recommendation: *Nigerian DMBs should institutionalise mandatory, continuously updated cybersecurity training alongside at least annual internal and external security audits, while the Central Bank of Nigeria should mandate disclosure of cybersecurity training and audit expenditure to strengthen market discipline.*

Introduction

As cybercrimes increase globally, Nigerian Deposit Money Banks (DMBs) invest in cybersecurity to mitigate any foul play. This is expected to enhance efficiency, customer convenience, and financial inclusion. In Nigeria, the adoption of digital banking using mobile banking applications, automated teller machines (ATMs), electronic money transfers, USSD transfer codes, point of sales (POS), and real time gross settlement has enhanced the services provided by DMBs to mitigate cybercrimes. This makes banking operations better, operational bottlenecks reduced, and improvement in financial accessibility which invariably strengthens customer experience and satisfaction. Despite these breakthroughs recorded in the banking sector, the growing risk of cybercrime remains a critical concern

Cybercrime has become a major problem to Nigeria's financial system. According to the Financial Institutions Training Centre (FITC, 2023), investors lost N2.72 billion in the first six months of 2022. The Nigeria Inter-Bank Settlement System (NIBSS, 2021) also revealed that banks lost N3.5 billion to fraud between July and September 2020; which resulted to a 537% increase from the loss of N2.37 billion recorded in 2017 (FITC, 2023).

All over the world, banks are the target for cyberattacks because they have lots of money and important information (Debnath et al., 2025). Mellado (2018) notes that the evolving complexity of cyber threats requires organizations to adopt proactive and adaptive risk management strategies. In Nigeria, many laws were enacted and implemented by the government and Central bank to prevent and eradicate any act of cybercrimes. Despite these laws, cybercrime remains an issue of serious concern in the banking system. This shows that mere rules and technology are not enough to eradicate cybercrimes.

Impliedly, cyberattacks may not be because of technological lapses but about people. Sometimes people who work at the banks might be a threat to security either because of lack of competence or an act of negligence. The Association of Cyber Security Expert of Nigeria reveals that this is a great threat if not curtailed. This means that banks need to engage in human capacity development to be proactive and adaptive to threats in real-time. Through this, they are aware of diverse cyberattacks on other organizations and learn from their pitfalls. They can also learn how to use the available technology to protect the bank.

As DMBs in Nigeria rely on digital banking platforms for their operations, they become more exposed to vulnerabilities that are cyber-related. This includes data breaches, electronic fraud, system intrusions, and insider manipulation which invariably can lead to financial losses and indirect costs. To mitigate these incidents, banks invest in human capital development and institutional controls mechanisms to build cyber

resilience and safeguard digital assets (Kovacevic et al., 2024; Miya & Joseph, 2025). However, the effect of the investment on these controls is not overly reflected in the financial performance of Nigerian DMBs. The volatility of their financial performance raises critical empirical questions regarding the economic returns on cyber risk management investments. Prior studies show the importance of cybersecurity investments to stabilize banking operations, but they fail to acknowledge whether human and institutional cyber risk controls significantly explain variations in financial performance indicators such as Return on Assets (ROA), Return on Equity (ROE), Net Interest Margin (NIM), and Cost-to-Income Ratio (CIR). This creates uncertainty for bank management to determine the best resource allocation mix between capacity-building initiatives and technological investments that can optimize the financial performance of DMBs in Nigeria. This empirical gap between compliance-driven controls and measurable financial outcomes remains underexplored.

Critically, research consistently demonstrates that cyber breaches exploit human vulnerabilities more than technological weaknesses (Toth et al., 2025; Al-Khatib et al., 2024), underscoring that cybersecurity is fundamentally a people's problem. Cybersecurity investments might also have been treated as ordinary regulatory compliance costs rather than as strategic financial performance drivers. In response, Nigerian DMBs strategically adopt Employee Training and Awareness (ETA) as a control to build human capacity that detects and resists threats; and Regular Security Audit and Assessment (RSAA), to provide control on institutional, structural verification of the DMBs (Central Bank of Nigeria (CBN), 2018).

Despite this development, studies carried out in Nigeria singly examine training and audit quality majorly in isolation and often relate them to operational or governance outcomes, rather than to a direct profitability measure such as Net Operating Profit After Tax (NOPAT) (Eluwa et al., 2025; Oladejo et al., 2025). There has been no robust Nigerian econometric evidence that yet quantifies the return on either type of investment or clarifies how the two interact. This study therefore seeks to jointly model ETA and RSAA as distinct predictors of NOPAT within a single panel framework for Nigerian DMBs, thereby distinguishing the financial return attributable to human-capacity-based controls from that attributable to structural audit-based controls.

Accordingly, the study is guided by the following objectives:

1. To examine the effect of employee training and awareness (ETA) on the financial performance of Nigerian deposit money banks.

2. To examine the effect of regular security audit and assessment (RSAA) on the financial performance of Nigerian deposit money banks.

By jointly testing these two control mechanisms against a direct profitability measure, and by interpreting the results through the complementary lenses of Human Capital Theory and Risk Management Theory, the study contributes empirical evidence that can guide Nigerian DMBs' resource allocation between capacity-building and structural audit investments and provides regulators with an evidence base for cybersecurity disclosure policy.

The proposition that human error, rather than technological deficiency, drives the majority of cyber breaches in financial institutions is now well established (Toth et al., 2025; Al-Khatib et

al., 2024), and a fairlyconsistent empirical picture has emerged around how training addresses this vulnerability. Behavioural-security studies converge on the finding that structured, continuous awareness training measurably improves detection and reporting behaviour: Parsons et al. (2014) linked HAIS-Q-based training to reduced insider risk, and Da Veiga and Martins (2015) tied awareness levels to lower incident rates, while the Association of Cybersecurity Experts of Nigeria has separately warned that insider threats intensify wherever training is episodic rather than continuous. Within the Nigerian context specifically, Omodunbi et al. (2016); and Emmanuel and Oreoluwa (2022) both attribute a substantial share of financial-sector cyber fraud to weak institutional training and employee negligence, arguing independently for continuous awareness interventions as the primary mitigation strategy — a convergence across two separately conducted studies that strengthens the claim.

A second, more finance-oriented stream of literature moves beyond behavioural outcomes to test training's effect on organisational and financial performance directly. It is this stream that the present study's ETA variable draws on most closely. Aliu and Alenoghena (2023) found a significant positive training effect on organisational performance using survey data from 450 DMB personnel, a finding echoed by Akamobi and Unachukwu (2022). Using longitudinal panel data spanning more than four decades, Eluwa et al. (2025) showed training investment improving return on assets across seven banks, while Orshi et al. (2026), studying twelve listed banks, found that training amplifies rather than merely supplements the profitability effect of intellectual capital. Read together, however, these studies are methodologically uneven — several rely on cross-sectional survey designs vulnerable to common-method bias and self-reported performance measures, and none tests training against a direct profit-based metric such as NOPAT within a panel framework that controls bank- and time-specific heterogeneity. This measurement gap,behavioural and perceptual outcomes standing in for financial outcomes, is precisely what the present study's ETA–NOPAT specification is designed to close. Accordingly:

H_{01}: Employee training and awareness has no significant influence on the profitability of Nigerian deposit money banks.

2.2 Regular Security Audit and Assessment

Where employee training addresses the human dimension of cyber risk, regular security audits and assessments (RSAA) address its institutional dimension, providing structured verification of technical vulnerabilities, control effectiveness, and regulatory compliance. Mellado (2018) frames continuous auditing as indispensable to catching evolving vulnerabilities before they crystallise into losses, a position operationalised in Nigeria through the CBN's risk-based cybersecurity framework, which mandates regular risk assessments and board-level oversight of security audit activity (Central Bank of Nigeria, 2018). Audit effectiveness, however, is not purely mechanical: Khayat et al. (2025) show that a well-trained auditor extracts substantially more actionable intelligence from a given penetration test than a minimally prepared one, while also cautioning that technical competence alone does not preclude an employee enabling a breach through negligence or fraud, a finding that foreshadows this study's expectation that ETA and RSAA operate as complementary rather than independent controls.

The financial-performance evidence for audit-based controls is, if anything, more consistent than that for training. Biener et al. (2015) provide the most direct precedent for the RSAA variable, showing through panel analysis that training and internal audit jointly reduce cyber loss severity. Muotolu and Nwadialor (2019) and Oladejo et al. (2025) both confirm, using panel data on fourteen and twelve Nigerian DMBs respectively, that audit quality and audit objectivity significantly improve financial performance, while Inneh et al. (2022) sharpen this claim by showing that it is audit process quality and timeliness; not merely the existence of an audit function that drives the return on assets. This body of work is more methodologically comparable to the present study than the training literature is, since several of its members already use panel designs on Nigerian DMB samples; however, none directly measures audit-related expenditure against NOPAT, and none tests audit effects alongside training effects within a single model to establish their relative financial magnitude. Accordingly:

H_{02}: Regular security audit and assessment has no significant impact on the profitability of Nigerian deposit money banks.

2.3 Theoretical Framework

2.3.1 Human Capital Theory

Human Capital Theory (HCT), propounded by Schultz (1961), conceives of investment in employee skills, knowledge, and training as an economically productive investment analogous to investment in physical capital, one that raises individual and organisational efficiency and, ultimately, financial performance. Applied to banking cybersecurity, HCT predicts that expenditure on training cybersecurity personnel, running awareness programmes, and funding professional certification builds a stock of firm-specific human capital that improves employees' capacity to detect, resist, and respond to cyber threats, and that this capacity should be observable, over time, as improved financial performance.

2.3.2 Risk Management Theory

Risk Management Theory (RMT) holds that organisations facing uncertain, potentially severe loss exposures of which cyber risk is a leading contemporary example, improve expected financial outcomes by systematically identifying, assessing, and controlling those exposures rather than absorbing losses passively (Markowitz, 1959). Applied here, RMT predicts that structured, recurring security audits function as an institutional control mechanism. It does this by surfacing vulnerabilities before they are exploited, and by verifying that existing controls remain effective as threats evolve, regular auditing reduces the frequency and severity of costly cyber incidents and thereby protects and enhances bank profitability.

2.3.3 Theoretical Positioning of the Present Study

Much of the extant literature invokes HCT or RMT singly, and largely descriptively, to justify a training or an audit variable without testing whether the two theories' predictions hold jointly, or which mechanism dominates empirically. This study departs from that convention in two respects. First, it tests HCT and RMT jointly within a single panel model rather than treating them as alternative explanations for isolated variables, allowing a direct empirical comparison of the human-capital and structural-control pathways to profitability rather than an assumed equivalence between them. Second, by comparing the estimated coefficients of ETA and RSAA rather

than merely confirming their statistical significance, the study is positioned to show that RMT's structural-control mechanism carries a substantially larger marginal financial return than HCT's human-capital mechanism in this context, a nuance that neither theory predicts on its own and that a mechanical, single-theory application would not have revealed. In this sense, the study extends both theories by demonstrating their complementary but unequal contribution to DMB financial performance, rather than adopting either theory as an unexamined given.

2.4 Literature Synthesis and Research Gap

Read as a whole, the reviewed literature establishes two reasonably solid but largely parallel claims: that employee training reduces human-error-driven cyber losses, and that structural security audits reduce control-failure-driven cyber losses. What it has not done is test these two claims against each other, or against a common financial-performance metric, within a single rigorous panel framework for Nigerian DMBs. Prior Nigerian studies are constrained by cross-sectional designs, self-reported or survey-based outcome measures, or narrow single-construct models that cannot speak to the relative financial return of competing cyber-risk-control investments. This is the gap the present study addresses: by jointly modelling ETA and RSAA against NOPAT in a fixed-effects panel design that controls for bank- and time-specific heterogeneity, it provides the first Nigerian evidence — to the researchers' knowledge — of the relative financial return on human-capacity versus structural cyber risk controls in the deposit money banking sector.

3. Materials and Methods

3.1 Research Design

The study adopted an ex-post facto panel research design, appropriate because it analysed financial and governance events that have already occurred and are recorded in audited historical disclosures, and because it permits control for both firm-specific heterogeneity and temporal effects through panel estimation.

3.2 Study Population

The twenty-five (25) listed deposit money banks (DMBs) licensed by the Central Bank of Nigeria as at 31st December 2024 formed the population of the study. They were operating in Nigeria as at the end of the study period. The population was narrowed down by purposively selecting banks with a full, continuous record of audited financial statements and cybersecurity-related disclosures across the ten-year study window (2015–2024), since the panel design requires balanced firm-year observations.

3.3 Sample Size and Sampling Technique

Secondary data were extracted from audited annual financial statements and corporate governance reports of ten purposively selected Nigerian DMBs for the period 2015–2024, yielding 100 firm-year observations (10 banks × 10 years). Purposive sampling was employed to ensure inclusion of banks disclosing consistent cybersecurity governance information across the study period. Ethical considerations are addressed by relying exclusively on publicly available audited statements, with all data sources properly acknowledged.

3.4 Variables and Measurement

Table 1: Variable Measurement

S/N	Type	Variable	Proxy	Measurement
1	Dependent	Financial Performance	NOPAT	Net operating profit after tax (₦ million)
2	Independent	Employee Training &Awareness	ETA	Annual expenditure on cybersecurity training (₦ million)
3	Independent	Regular Security Audit & Assessment	RSAA	Annual expenditure on security audits & vulnerability assessments (₦ million)

Source: Authors' compilation, 2026

3.5 Model Specification

Based on the functional relationship NOPAT = f(ETA, RSAA), the econometric model is specified as:

$$NOPAT_{it} = \alpha + \beta_1 ETA_{it} + \beta_2 RSAA_{it} + \mu_i + \lambda_t + \varepsilon_{it}$$

where i denotes banks (i = 1, …, 10), t denotes years (t = 2015, …, 2024), μ_i captures bank-specific fixed effects, λ_t captures time fixed effects, and εit is the idiosyncratic error term. Pooled OLS, Fixed Effects (FEM), and Random Effects (REM) estimators were considered. The Hausman specification test was applied to select between FEM and REM. Multicollinearity was assessed via the Variance Inflation Factor (VIF) and normality via Skewness/Kurtosis tests and Shapiro-Wilk W tests. Heteroskedasticity was examined using Cameron and Trivedi's IM-test.

3.6 Technique of Data Analysis

Descriptive statistics such as mean, standard deviation, skewness, and kurtosis were used for the distributional properties of NOPAT, ETA, and RSAA. Meanwhile, correlation between variables were tested to avoid multicollinearity. Where there is existence of multicollinearity, diagnostic test was carried out using the Variance Inflation Factor (VIF). Skewness/Kurtosis and Shapiro–Wilk W tests were used for normality, Cameron and Trivedi's IM-test for heteroskedasticity, and the Hausman specification test for model selection which was conducted to establish the appropriate estimator and confirm that its underlying assumptions were satisfied or appropriately addressed. Given the Hausman test's confirmation of Fixed Effects as the preferred estimator, the panel regression model was estimated using Stata version 17, with robust standard errors applied in view of the detected heteroskedasticity.

4 Data Analysis and Results

4.1 Descriptive Statistics

Table 2: Descriptive Statistics

Variable	Obs	Mean	Std. Dev.	Min	Max	Skewness	Kurtosis
NOPAT	100	124,000	203,000	-1,786	1,032,895	2.866	11.173
ETA	100	1,970.81	2,560.756	12	13,390	2.325	8.745
RSAA	100	632.92	764.335	103	4,157	2.749	11.176

Source: Researchers' Computation, 2026. Values in ₦ million.

NOPAT ranged from a minimum loss of ₦1,786m to a maximum profit of ₦1,032,895m with a mean of ₦124,000m. ETA expenditures averaged ₦1,970.81m (range: ₦12m–₦13,390m) while RSAA expenditure averaged ₦632.92m (range: ₦103m–₦4,157m). All three variables are positively skewed (>1) and leptokurtic (>3), reflecting the presence of outliers consistent with the heterogeneous nature of Nigerian DMBs. High standard deviations (>50% of mean) indicate substantial cross-bank and temporal variation in cybersecurity investment and profitability.

4.2 Correlation Analysis

Table 3: Pairwise Correlation Analysis

Variable	(1) NOPAT	(2) ETA	(3) RSAA
(1) NOPAT	1.000		
(2) ETA	0.741*	1.000	
(3) RSAA	0.909*	0.767*	1.000

***Strong positive correlation (>0.6). Source: Researchers' Computation, 2026.**

The implication of all correlations exceeding 0.6 is that there are strong positive relationships between NOPAT-ETA (r = 0.741) and NOPAT-RSAA (r = 0.909). The inter-predictor correlation (ETA-RSAA = 0.767) is notable but within an acceptable range, and subjected to further examination through VIF.

4.3 Diagnostic Tests

There was no problematic multicollinearity as shown in Table 4. The Table reveals that the VIF for both ETA and RSAA is 2.432 (< 5). The table also shows the Skewness/Kurtosis tests (all $p < 0.001$) and Shapiro-Wilk W tests (W-statistics: 0.591–0.714, all $p < 0.001$) which confirms the non-normality tests across variables of the study. Cameron and Trivedi's IM-test detects heteroskedasticity ($\chi^2 = 40.13$, df = 5, $p < 0.001$). This confirms there is non-constant error variance. Meanwhile, the Hausman test ($\chi^2 = 0$, $p < 0.01$) reveals that the Fixed Effect (FE) is the better as the appropriate estimator.

Table 4: Summary of Diagnostic Tests

Test	Statistic	Decision
VIF – ETA / RSAA	2.432 / 2.432 (< 5)	No multicollinearity
Shapiro-Wilk W – NOPAT / ETA / RSAA	0.591 / 0.714 / 0.645 (all $p < 0.001$)	Non-normal distribution
Skewness/Kurtosis – all variables	Prob > $\chi^2 = 0.000$	Non-normal distribution
Heteroskedasticity (IM-test)	$\chi^2 = 40.13$, $p = 0.000$	Heteroskedasticity present
Hausman Test	$\chi^2 = 0$, $p < 0.01$	Fixed Effects preferred

Source: Researcher' Computation, 2026.

4.4 Fixed Effects Regression Results

Table 5: Fixed Effects Regression (Dependent Variable: NOPAT)

Variable	Coefficient	Std. Error	t-value	p-value	Significance
ETA	10.581	5.156	2.05	0.043	**
RSAA	227.832	16.506	13.80	0.000	***
Constant	-40,604.728	11,441.783	-3.55	0.001	***

$R^2 = 0.819$ | F-test = 199.419 | Prob > F = 0.000 | N = 100 | AIC = 2521.725*** $p < 0.01$, ** $p < 0.05$, * $p < 0.10$. **Source: Researchers' Computation, 2026.**

There is also a positive and significant relationship between Employee training and awareness (ETA) and NOPAT ($\beta = 10.581$, $t = 2.05$, $p = 0.043$). This shows that every additional ₦1 million invested in cybersecurity training is associated with an approximately ₦10.58 million increase in NOPAT, consistent with the contention that well-trained employees prevent costly cyber incidents, reduce operational errors, and improve efficiency, and enhancing profitability collectively.

Regular security audit and assessment (RSAA) exerts a strongly significant positive effect on NOPAT ($\beta = 227.832$, $t = 13.80$, $p < 0.001$). The magnitude of this coefficient reflects that there is a very huge financial return on structured security auditing. Each ₦1 million invested in security assessments is associated with approximately ₦227.83 million in additional NOPAT. This suggests that audit-driven vulnerability remediation prevents disproportionately large financial losses. The value of R^2 (0.819) indicates that the explanatory variables included in the model explicitly explain 81.9% of the variation that occurs in NOPAT. The model is statistically significant ($F = 199.419$, $p < 0.001$). This confirms that the overall fit of the data is commendable.

5. Discussion of Findings

5.1 Employee Training and Awareness

The significant positive relationship between ETA and NOPAT confirms H_{01} and aligns with Human Capital Theory: investments in cybersecurity workforce competencies generate financial returns by reducing the frequency and severity of cyber incidents attributable to human error. This finding both corroborates and refines prior Nigerian evidence: whereas Aliu and Alenoghena (2023) demonstrate training's effect on organisational or employee-level performance using survey data, the present study extends this line of work by showing a smaller, though still statistically significant, direct effect on a hard profitability measure (NOPAT) within a panel framework. This suggests that training's financial payoff, while real, is more modest than its behavioural payoff reported elsewhere. The result affirms that employee training is not merely a compliance exercise but a material driver of bank profitability, since the reduction of phishing-related breaches, compliance failures, and operational errors translates directly into lower financial losses and improved NOPAT.

5.2 Regular Security Audit and Assessment

The highly significant and economically substantial positive coefficient for RSAA (β = 227.832, $p < 0.001$) confirms H_{02} and resonates with Risk Management Theory: systematic identification and remediation of cybersecurity vulnerabilities protect banks from the disproportionate financial costs of cyber incidents. The direction of this result is consistent with Oladejo et al. (2025), Muotolu and Nwadialor (2019), Alashe and Oyeshola (2021), and Biener et al. (2015). However, its magnitude is considerably larger than any audit-performance elasticity reported in that literature, most of which relies on non-panel or shorter-panel designs and non-monetary audit proxies. The present study's use of a direct expenditure-based audit proxy and a ten-year balanced panel may explain why the estimated financial return here is both statistically stronger and economically larger than in prior work. The large coefficient magnitude relative to ETA further suggests that institutional structural controls yield higher marginal financial returns than human capacity development alone, reinforcing the complementary nature of the two governance mechanisms: skilled employees execute controls more effectively, while robust audit frameworks catch what training misses.

6. Conclusion and Recommendations

Conclusion

This study set out to establish whether human-capacity-based and structural audit-based cyber risk controls generate measurable financial returns for Nigerian deposit money banks, a question the extant literature had left largely untested within a single empirical framework. The Fixed Effects panel evidence answers this question affirmatively for both control types: employee training and awareness (ETA) and regular security audit and assessment (RSAA) both exert statistically significant, positive effects on NOPAT, jointly explaining 81.9% of its variance. Read through Human Capital Theory and Risk Management Theory jointly rather than singly, the findings are more informative than either theory alone would suggest: they confirm both theories' core prediction that their respective mechanisms improve financial performance, while also revealing, a finding neither theory anticipates on its own, that the structural, audit-based mechanism (RSAA) carries a substantially larger marginal financial return (β = 227.832) than the

human-capital mechanism (ETA, β = 10.581). This should be read as an empirical observation about the relative magnitude of two statistically significant effects within this specific sample, rather than as evidence that training is unimportant. The two mechanisms remain theoretically, and per the significant ETA-RSAA correlation (r = 0.767), practically complementary rather than substitutable.

Compared with prior Nigerian work, which has generally tested training and audit effects separately and against organisational rather than profitability outcomes, this study's joint, profit-based test is consistent with the general direction of that literature (positive effects of both training and auditing) while being more precise about their relative economic size, a distinction the existing literature could not draw. The study's principal contribution to knowledge is this integrated, comparative empirical test itself.It is among the first, to the researchers' knowledge, to position Human Capital Theory and Risk Management Theory as jointly testable, rather than singly applied, provides frameworks for Nigerian DMB cybersecurity governance, and to ground the resulting policy prescriptions in panel econometric evidence rather than theoretical assertion alone.

Methodologically, the study's principal strengths lie in its ten-year balanced panel design, its use of a direct financial-performance outcome (NOPAT) rather than a perceptual or governance proxy, and its explicit diagnostic testing (VIF, normality, heteroskedasticity, Hausman) to justify the Fixed Effects specification. These are the features that address several of the design limitations identified in the reviewed literature. As with any single-context panel study, however, these conclusions are bounded by the ten purposively selected banks and the 2015–2024 window studied, and should be extended cautiously to DMBs outside this sample until replicated on a wider population.

Recommendations

For Bank Management: Cybersecurity training programmes should form a first-line allocation in the annual budgets of DMBs, ensuring that all frontline and IT staff receive mandatory awareness training covering phishing, social engineering, incident reporting, and data protection protocols. Training content should be updated at minimum semi-annually to reflect the evolving threat landscape, and training outcomes should be linked to performance appraisals to incentivise genuine competency development.

For Institutional Risk Governance: DMBs should embed regular security audits encompassing vulnerability scanning, penetration testing, access control reviews, and policy compliance assessments. These should serve as non-negotiable components of enterprise risk management. Both internal and external audits should be conducted at least annually, with remediation tracking integrated into board-level risk reporting.

For Regulators: The Central Bank of Nigeria should strengthen mandatory disclosure requirements for cybersecurity training expenditure and security audit outcomes in banks' annual reports, facilitating market discipline and enabling the research community to further examine cybersecurity governance effectiveness. The CBN should also consider minimum quantitative benchmarks for cybersecurity investment as a proportion of IT budgets.

For Future Research: Subsequent studies should extend the sample to include all listed DMBs, incorporate additional control variables (bank size, capital adequacy, loan quality), and

explore the mediating role of cybersecurity incident frequency between governance mechanisms and financial performance.

References

Al-Khatib, S. F., Ibrahim, Y. Y., &Alnadi, M. (2024). Cybersecurity practices and supply chain performance in the banking sector. *Administrative Sciences,* 15(1), 1–18.

Alashe, A. K., &Oyeshola, B. A. (2021). The impact of internal audit on financial performance of deposit money banks in Nigeria. *African Journal of Accounting and Financial Research*, 4(3).

Aliu, F. O., &Alenoghena, R. O. (2023).Employee training and organisational performance of selected deposit money banks in Lagos State, Nigeria.*International Journal of Research and Innovation in Social Science,* 7(2), 129–140.

Biener, C., Eling, M., & Wirfs, J. H. (2015).Insurability of cyber risk.*The Geneva Papers,* 40(1), 131–158.

Central Bank of Nigeria.(2018). Risk-based cybersecurity framework and guidelines for deposit money banks and payment service providers. Abuja: CBN.

Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security,* 49, 162–176.

Debnath, A., Sharmin, S., & Hassan, M. (2025).Securing Financial Information in the Digital Age: An Overview of Cybersecurity Threat Evaluation in Banking Systems. *Journal of Ecohumanism*, *4*(2), 1508-1517.

Eluwa, F. N., Ani, W. U., &Ezeudu, I. J. (2025). Assessing the impact of staff training and development on financial performance of commercial banks in Nigeria.*Journal of Research in Management and Social Sciences,* 11(1), 187–200.

Emmanuel, O. G., & Oreoluwa, D. O. (2022).Forensic Audit and Fraud Prevention in the Nigerian Deposit Money Banks. *Journal of Taxation and Economic Development*, *21*(1), 66-74.

Financial Institutions Training Centre (2023). Fraud and forgeries report (Q1 & Q2 2022). Lagos: FITC.

Inneh, E., Fakunle, I. O., Busari, R. R., & Olatunji, I. G. (2022).Audit characteristics and financial reporting timeliness of Nigerian listed non-financial institution. *Journal of Economics and Behavioral Studies*, *14*(2), 13-25.

Khayat, M., Barka, E., Serhani, M. A., Sallabi, F., Shuaib, K., & Khater, H. M. (2025). Empowering security operation center with artificial intelligence and machine learning—A systematic literature review. *IEEE Access*, *13*, 19162-19197.

Kovacevic, A., Radenkovic, S. D., & Nikolic, D. (2024). Artificial intelligence and cybersecurity in banking sector: opportunities and risks. arXiv preprint arXiv:2412.04495.

Markowitz, H.M. (1959). *Portfolio selection: efficient diversification of investment.* Cowles Foundation Monograph, 16, John Wiley and Sons, New York.

Mellado, D. (2018). Cybersecurity risk management in financial institutions. *Computers & Security*, 74, 1–13.

Miya, N. F., & Joseph, N. (2025).Banking on resilience: 20 years of cybersecurity evolution.South African *Journal of Information Management,* 27(1).

Muotolu, P. C., &Nwadialor, E. O. (2019).Effect of audit quality on the financial performance of deposit money banks in Nigeria.*International Journal of Trend in Scientific Research and Development,* 3(2).

Nigeria Inter-Bank Settlement System.(2021). Fraud landscape report. Lagos: NIBSS.

Oladejo, O. S., Yinus, S. O., & Oladejo, M. O. (2025). Internal audit practices and financial performance: Evidence from deposit money banks in Nigeria. *Journal of Accounting, Finance, and Contemporary Management Research,* 2(1).

Omodunbi, B. A., Odiase, P. O., Olaniyan, O. M., & Esan, A. O. (2016). Cybercrime in Nigeria: Causes, effects and the way out. *International Journal of Computer Science and Mobile Computing,* 5(8), 313–322.

Orshi, T. S., Idris, A. A., &Dafioghor, E. J. (2026).Intellectual capital, staff development and profitability of banks in Nigeria.*International Journal of Banking and Finance,* 21(1), 35–50.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014).Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q).*Computers & Security*, 42, 165–176.

Schultz, T. W. (1961). Investment in human capital.*American Economic Review,* 51(1), 1–17.

Toth, R., Dubniczky, R., Limonova, O., & Tihanyi, N. (2025).Sustaining cyber awareness: Long-term impact of phishing training.*Computers & Security,* 148.