THE IMPACT OF PROJECT MANAGEMENT OUTCOMES ON CYBER FRAUD RISK IN SELECTED BANKS IN LAGOS STATE

Babatunde Rahman YUSUF
Department of Accounting
Faculty of Management Sciences
Lagos State University, Lagos, Nigeria
babatunde.yusuf@lasu.edu.ng

Olawale Gazal HAMMED
Department of Management Technology
Faculty of Management Sciences
Lagos State University, Lagos, Nigeria
olawale.hammed@lasu.edu.ng

Corresponding Author:babatunde.yusuf@lasu.edu.ng
DOI: https://doi.org/10.57233/ijamer.v2i1.02

Article Information: Received: 28/03/2026**Revised:** 11/04/2026**Accepted:** 04/20/2026

To Cite this Article: Yusuf, B. R., & Hammed, O. G. (2026). The impact of project management outcomes on cyber fraud risk in selected banks in Lagos State.*International Journal of Accounting, Management and Economic Review, 2*(1). https://doi.org/10.57233/ijamer.v2i1.02

Abstract
This study examined the impact of project management outcomes on cyber fraud risk among selected banks in Lagos State, Nigeria. With the increasing reliance on digital banking systems, exposure to cyber fraud has heightened, necessitating an in-depth investigation of internal operational factors such as project management effectiveness. Specifically, the study focused on project completion rate, project success rate, and project performance index as key determinants of cyber fraud risk. These constructs were operationalized through a structured questionnaire distributed to 368 respondents, comprising IT staff, project managers, risk managers, and cybersecurity analysts across selected banks. Project completion rate was measured by respondents' perceptions of project timeliness, with items assessing adherence to scheduled timelines for IT and cybersecurity projects. The project success rate was assessed by examining respondents' views on whether projects met the expected cost, quality, and scope objectives. Project performance index was evaluated through key performance indicators such as project cost efficiency, schedule adherence, and stakeholder satisfaction. The survey instrument used a five-point Likert scale ranging from "strongly disagree" to "strongly agree" for quantifiable measurement. Data analysis was conducted using descriptive statistics, correlation, and regression techniques. The findings revealed that project completion rate has a positive and significant effect on cyber fraud risk, although with relatively low explanatory power. A moderate and significant relationship was found between project success rate and cyber fraud risk, while the project performance index showed a strong and significant effect on cyber fraud risk, highlighting the importance of performance monitoring and evaluation in mitigating fraud exposure. The study concludes that project management outcomes are critical determinants of cybersecurity effectiveness in the banking sector and recommends that banks strengthen project performance evaluation systems, integrate cybersecurity objectives into project success metrics, and ensure timely and effective project completion.

Keywords: Cyber fraud risk, Nigerian banking sector, project management outcomes, project performance index, project success rate.

1.0 Introduction

The rapid digitalization of financial services has transformed the global banking industry by improving efficiency while simultaneously increasing exposure to cyber fraud risks. The integration of information technology into banking operations has created complex project environments that demand effective project management practices to ensure system security and resilience. Despite these advancements, financial institutions continue to face sophisticated cyber threats such as phishing, malware, and data breaches, which exploit weaknesses in both technological systems and organizational processes (Idris et al., 2025; Alketbi et al., 2022).

While the challenges posed by cyber fraud are widely acknowledged, research often focuses on technological and organizational weaknesses as the primary sources of these risks (Almeida et al., 2022; Tade, 2021). However, limited attention has been paid to how project management outcomes such as project completion rate, project success rate, and project performance index, affect the vulnerability of financial institutions to cyber fraud. This gap in the literature is particularly significant in developing economies like Nigeria, where banks face unique challenges related to rapid digital adoption, inadequate infrastructure, and weak regulatory frameworks.

Most studies have concentrated on internal controls and cybersecurity measures but have not sufficiently explored the influence of project management practices on mitigating or amplifying cyber fraud risks. For instance, while some studies have focused on internal controls (Odukwu et al., 2022; Nyakarimi et al., 2020) and others have examined the technological infrastructure needed to combat fraud (Isibor, 2022; Ogedengbe et al., 2025), few have investigated how project management outcomes directly impact cyber fraud risk. Project completion rate, which refers to the timeliness of project delivery, project success rate, which assesses whether projects meet their objectives, and project performance index, which evaluates overall project performance in terms of cost, schedule, and quality, have not been thoroughly examined as critical factors in reducing the exposure of banks to cyber threats. This study aims to address this gap by investigating the relationship between project management outcomes and cyber fraud risk, specifically within the context of Nigerian banks.

In Lagos State, Nigeria's commercial and financial hub, the complexity of banking operations increases the risks associated with delayed or unsuccessful projects. Evidence suggests that delays in deploying security systems and the failure to achieve project objectives heighten the risk of cyber fraud (Odukwu et al., 2022; Ogedengbe et al., 2025). Despite this, the role of project performance index as a predictor of cyber fraud risk has not been adequately studied, particularly in relation to its impact on the effectiveness of cybersecurity efforts.

This study examines the influence of project management outcomes on cyber fraud risk among selected banks in Lagos State. It seeks to assess how project completion rate affects cyber fraud risk, explore the relationship between project success rate and cyber fraud risk, and determine the extent to which project performance index influences cyber fraud risk. By addressing these issues, the research aims to provide valuable insights into how project management practices, specifically in the Nigerian banking sector, can help mitigate cyber fraud risks.

2.0 Literature Review

Project completion rate is widely regarded as a key indicator of project management effectiveness, particularly in technology-driven sectors such as banking. It reflects an organization’s ability to deliver projects within scheduled timelines, ensuring that critical systems and controls are

operational when needed. Timely completion of IT and cybersecurity projects has been identified as essential for minimizing system vulnerabilities and operational risks (Serrador & Pinto, 2021; Joslin & Müller, 2022). In banking, delays in implementing security-related projects may create exploitable gaps, thereby increasing exposure to cyber fraud.

However, while project completion rate is often linked to improved performance and reduced risk, its sufficiency as a standalone measure remains contested. Some studies suggest that timely project completion directly correlates with improved performance and risk mitigation (Meredith et al., 2021; Kerzner, 2022). However, other research contends that speed without quality and adequate risk assessment is insufficient. Ajemunigbohun and Ipigansi (2022) argue that projects completed on schedule but lacking robust risk controls can still expose institutions to fraud. Lawal et al. (2023) further describe such outcomes as "illusory efficiency." Empirical evidence shows that delays in project implementation are associated with increased cyber vulnerabilities and fraud incidents (Almeida et al., 2022; Odukwu et al., 2022), with Ajemunigbohun (2023) linking incomplete projects to weakened internal controls, which directly contribute to the risk of cyber fraud.

Despite these insights, significant gaps remain in the literature, particularly within the Nigerian banking context, where unique contextual factors such as high transaction volumes and evolving cyber threats are often overlooked (Ogundeko et al., 2024). Existing studies predominantly rely on cross-sectional data and fail to integrate project management outcomes with comprehensive cybersecurity frameworks (Joslin & Müller, 2022). This lack of integration weakens the conceptual alignment between project management practices and cyber fraud risk. Project success rate goes beyond project completion to include the achievement of defined objectives such as cost, scope, quality, and stakeholder satisfaction. In the banking sector, successful projects are those that enhance operational efficiency and strengthen cybersecurity systems. Evidence suggests that higher project success rates improve system reliability and reduce exposure to cyber threats (Too & Weaver, 2021; Müller et al., 2022).

However, the concept of project success remains contested. Traditional measures focus on the iron triangle of time, cost, and scope, whereas recent perspectives emphasize strategic alignment and risk mitigation, particularly in sectors where security is a key concern (Kerzner, 2022). Ajemunigbohun et al. (2020) argue that project success in financial institutions should be assessed based on its contribution to fraud prevention, while Lawal et al. (2023) stress that cybersecurity outcomes must be incorporated into success metrics. Successful projects, therefore, should be defined not only by their completion but also by their ability to reduce cyber fraud risk through robust security measures.

Empirical studies have shown that successful projects reduce fraud risk by improving system security (Almeida et al., 2022). Conversely, failed or abandoned projects often create vulnerabilities that fraudsters can exploit (Ajemunigbohun & Ipigansi, 2022; Ogundeko et al., 2024). Despite these findings, inconsistencies in measurement and limited context-specific research, particularly in developing economies, remain key gaps (Joslin & Müller, 2022). To bridge this gap, future research should integrate project success metrics with cybersecurity outcomes to better assess the impact on cyber fraud risk in banking.

The project performance index (PPI) is a composite measure of project efficiency that incorporates key performance indicators such as cost, schedule adherence, and quality. It serves as an important tool for monitoring and evaluating project progress, particularly in complex environments like

banking. Effective performance measurement enables organizations to detect risks early and implement corrective actions (Serrador & Pinto, 2021; Kerzner, 2022). However, concerns about the adequacy of traditional performance indices have emerged. Some scholars argue that conventional KPIs do not capture critical aspects such as cybersecurity resilience and organizational learning (Too & Weaver, 2021). Ajemunigbohun and Ipigansi (2022) further criticize performance metrics for focusing mainly on financial indicators while neglecting the implications for fraud risk, while Lawal et al. (2023) advocate for the inclusion of security-related measures in performance evaluation.

Empirical studies indicate a strong link between project performance and cyber fraud risk. Poorly performing projects often lead to weak controls, inadequate testing, and incomplete implementation, all of which increase vulnerability to cyber-attacks (Almeida et al., 2022; Odukwu et al., 2022). Ajemunigbohun (2023) associates low performance indices with higher fraud rates, while Ogundeko et al. (2024) highlight the role of performance feedback in risk reduction. However, limitations such as reliance on self-reported data and lack of standardized frameworks persist (Joslin & Müller, 2022), and there is a noticeable gap in context-specific studies, particularly within the Nigerian banking sector (Ajemunigbohun et al., 2020).

Cyber fraud risk refers to the likelihood of financial loss resulting from unauthorized access, manipulation, or exploitation of digital banking systems. With the expansion of electronic banking, cyber fraud has become a major concern globally, driven by technological vulnerabilities, human factors, and organizational weaknesses (Bouveret, 2022; Kshetri, 2023). Scholarly discussions emphasize the role of internal controls and risk management frameworks in mitigating cyber fraud. While some studies focus on technological solutions such as encryption and intrusion detection systems, others highlight the importance of organizational factors, including project management practices (Saxena et al., 2021). Ajemunigbohun and Ipigansi (2022) argue that poor project execution creates vulnerabilities that fraudsters exploit, while Lawal et al. (2023) advocate for an integrated approach combining technical and managerial strategies.

Empirical evidence in Nigeria shows a rising trend in cyber fraud incidents, largely due to weaknesses in digital systems and internal controls (NIBSS, 2024). Ajemunigbohun (2023) links inadequate project execution to increased fraud risk, while Ogundeko et al. (2024) highlight the role of weak monitoring systems. However, existing studies largely emphasize technological factors, with limited focus on project management outcomes and few longitudinal or context-specific analyses (Ajemunigbohun et al., 2020). This study aims to address this gap by linking project management outcomes directly to the mitigation of cyber fraud risk within the Nigerian banking sector.

Theoretical Review

Risk Management Theory provides a framework for identifying, assessing, and mitigating risks within an organization. The theory posits that organizations can minimize uncertainties and potential losses by implementing systematic risk management processes. In the context of banking, risk management involves identifying potential threats, evaluating their impact, and implementing strategies to mitigate them (Hopkin, 2021). This approach assumes that risks are inherent in all organizational activities and that effective management requires continuous monitoring and evaluation. One of its strengths lies in its comprehensive approach, integrating various aspects of organizational operations to minimize risks, such as those related to cyber fraud.

Critics argue that the theory can be overly complex and difficult to implement, especially in resource-constrained environments (Bromiley et al., 2021). Despite these challenges, Risk Management Theory remains highly applicable to this study due to its focus on managing operational risks, particularly those related to cybersecurity. The theory underscores the importance of project management outcomes in reducing cyber fraud risk. Project completion rate, project success rate, and project performance index are key indicators of how effectively risks are managed within an organization. Ajemunigbohun and Ipigansi (2022) emphasize that effective project management is essential for implementing robust risk management frameworks, while Lawal et al. (2023) note that poor project performance can undermine risk mitigation efforts, leaving the organization vulnerable to fraud.

While Systems Theory also offers useful insights into the interconnectedness of organizational components, it focuses more on understanding the broader system dynamics rather than directly addressing risk management and mitigation strategies. Systems Theory views an organization as a complex system composed of interrelated components that work together to achieve common objectives. It emphasizes the importance of understanding the interactions among the system's elements and how they influence overall performance (Skyttner, 2022). Although Systems Theory provides a valuable holistic perspective, its abstract nature makes it less applicable for this study, which specifically focuses on how project management practices can mitigate cyber fraud risk.

In contrast, Risk Management Theory offers a more direct and practical approach to understanding how project management outcomes, such as timely project completion, achieving project objectives, and monitoring project performance, can influence the risk of cyber fraud in banks. The focus on risk identification and mitigation aligns more closely with the study's objectives, making Risk Management Theory the more suitable framework for examining the impact of project management practices on cyber fraud risk in the banking sector.

Therefore, this study adopts Risk Management Theory as the primary framework, which allows for a clearer understanding of how project completion rate, project success rate, and project performance index serve as indicators of effective risk management, while cyber fraud risk represents a key operational risk. By focusing on this framework, the study provides a more targeted and actionable approach to understanding how project management outcomes influence the vulnerability of banks to cyber fraud.

3.0 Research Methods

This study adopts a quantitative research approach using a cross-sectional survey design. While organizational risk is inherently dynamic, a cross-sectional approach is methodologically appropriate for this study's primary objective. This design facilitates the collection of standardized data from a broad sample of IT and risk professionals across Lagos State banks, providing a high-resolution snapshot of the industry's current risk posture and variable correlations at a fixed point in time. This provides the necessary empirical baseline from which future longitudinal studies can track temporal shifts. Based on verified human resource records from five participating banks, the total eligible staff population is 1,247.

The sample size is calculated using Yamane's (1967) formula with a 95% confidence level and 5% margin of error:

$$n = \frac{N}{1 + N(e)^2} = \frac{1247}{1 + 1247(0.05)^2} = \frac{1247}{1 + 3.1175} = \frac{1247}{4.1175} \approx 303$$

To account for a design effect of 1.2 (due to stratified sampling) and an anticipated 10% non-response rate, the final target sample is:

$$, n_{final} = 303 \times 1.2 \times 1.1 \approx 400$$

A stratified random sampling technique is employed. Strata are defined by professional group: IT staff, project managers, risk managers, and cybersecurity analysts. A complete sampling frame was obtained from each bank's HR department. Proportional allocation is used to ensure each stratum's representation in the sample matches its representation in the population.

The proportional allocation formula is:

$$n_h = \frac{N_h}{N} \times n_{final}$$

where:

n_h = sample size for stratum h
N_h = population size for stratum h
N = total population size (1,247)
n_{final} = final target sample size (400)

Table 1:
Stratification Table

Stratum (Professional Group)	Population Size (N_h)	Population Proportion (N_h/N)	Proportional Sample (n_h)	Rounded Sample
IT Staff	482	0.386 (38.6%)	154.5	**156**
Project Managers	351	0.281 (28.1%)	112.4	**112**
Risk Managers	237	0.190 (19.0%)	76.0	**76**
Cybersecurity Analysts	177	0.142 (14.2%)	56.8	**57**
Total	**1,247**	**100%**	**399.9**	**400**

Source: Researchers (2026).

Within each stratum, respondents are selected using simple random sampling via a random number generator applied to the sorted HR list for each professional group. Primary data are collected using a structured questionnaire aligned with the study variables. The instrument is divided into sections capturing Project Completion Rate, Project Success Rate, Project Performance Index, and Cyber Fraud Risk Assessment, using a five-point Likert scale ranging from strongly disagree (1) to strongly agree (5), which allows for quantifiable measurement of respondents' perceptions.

The validity of the instrument is ensured through content and construct validity. Content validity is established through expert review by professionals in project management, banking, and cybersecurity, while construct validity is achieved by aligning the questionnaire with established literature. Reliability is tested using Cronbach's Alpha with a threshold of 0.70, and the results

indicate high internal consistency: Project Completion Rate (α = 0.81), Project Success Rate (α = 0.84), Project Performance Index (α = 0.79), and Cyber Fraud Risk (α = 0.86).

Data analysis is conducted using SPSS, employing both descriptive statistics such as mean and standard deviation, and inferential techniques including correlation and multiple regression to test the study hypotheses. Ethical standards are maintained by ensuring voluntary participation, informed consent, confidentiality, and anonymity. Respondents are also informed of their right to withdraw at any time, and the study ensures that no harm is caused during the research process.

4.0 Data Analysis and Discussion of Findings

This section describes the demographic profile of the 399 respondents, including gender, age, education, banking experience, and professional position, using frequency and percentage distributions.

Table 2:
Descriptive Statistics

		Frequency	Percentage
Indicate your gender	Male	225	61.1%
	Female	143	38.9%
Indicate your age bracket	18 but less than 30	33	9.0%
	30 but less than 40	103	28.0%
	40 but less than 50	93	25.3%
	50 but less than 60	80	21.7%
	60 and above	59	16.0%
Indicate your educational qualification	Bachelor's Degree / HND	51	13.9%
	Master's Degree	48	13.0%
	Doctorate Degree	73	19.8%
	Professional Certificate(s)	129	35.1%
	Others (ND, SSCE, GCE etc.)	67	18.2%
Years of experience in the Banking Sector	Less than 2 Years	95	25.8%
	2-5 Years	111	30.2%
	6-10 Years	81	22.0%
	More than 10 Years	81	22.0%
Position in the Organisation	IT Staff	110	29.9%
	Project Manager	95	25.8%
	Risk Manager	84	22.8%
	Cybersecurity Analyst	79	21.5%
	Others	0	0.0%

Source: Researchers (2026).

The demographic results indicate that the respondents are largely representative of experienced, professionally qualified personnel in the banking sector. The sample is predominantly male, with a workforce largely concentrated in the middle to older age brackets, suggesting a mature, knowledgeable respondent base. Educationally, most respondents hold professional certifications and advanced degrees, indicating a high level of technical and professional competence relevant to project management and cybersecurity.

Furthermore, the distribution of work experience shows a balanced mix of early-career and seasoned professionals, while the occupational roles are well spread across IT staff, project managers, risk managers, and cybersecurity analysts. This implies that the data were obtained from individuals directly involved in both project execution and cyber risk management, thereby enhancing the reliability and relevance of the findings for assessing the relationship between project management outcomes and cyber fraud risk in the banking sector.

Hypothesis Testing

This section presents the results of correlation and hierarchical multiple regression analyses used to test the study's hypotheses regarding the relationship between project management outcomes and cyber fraud risk, at the = 0.05 significance level.

H_{01}: Project completion rate has no significant effect on cyber fraud risk among selected banks in Lagos State.

Result of Hypothesis I

Table 3:

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.232[a]	.054	.051	.76614

a. Predictors: (Constant), Comp_Rate

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	12.179	1	12.179	20.750	.000[b]
	Residual	214.833	366	.587		
	Total	227.012	367			

a. Dependent Variable: Fraud_Risk

b. Predictors: (Constant), Comp_Rate

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	2.918	.165		17.661	.000	2.593	3.243
	Comp_Rate	.213	.047	.232	4.555	.000	.121	.305

a. Dependent Variable: Fraud_Risk

Source: Researchers (2026).

The results of Hypothesis One examine the effect of project completion rate on cyber fraud risk among selected banks in Lagos State. The model summary shows a correlation coefficient (R) of 0.232, indicating a weak positive relationship between project completion rate and cyber fraud risk. The coefficient of determination ($R^2 = 0.054$) reveals that approximately 5.4% of the variation in cyber fraud risk is explained by project completion rate. Although this explanatory power is

relatively low, it still suggests that project completion rate contributes to changes in fraud risk within the banking sector.

The ANOVA results indicate that the regression model is statistically significant ($F = 20.750$, $p < 0.001$), confirming that the model provides a better fit than one with no predictors. Furthermore, the coefficient results show that project completion rate has a positive and significant effect on cyber fraud risk ($\beta = 0.232$, $t = 4.555$, $p < 0.001$). This implies that changes in project completion rate significantly influence cyber fraud risk levels. Based on these findings, the null hypothesis (H01), which states that project completion rate has no significant effect on cyber fraud risk, is rejected. It can therefore be concluded that project completion rate has a statistically significant effect on cyber fraud risk among selected banks in Lagos State.

H_{02}: There is no significant relationship between project success rate and cyber fraud risk among selected banks in Lagos State.

Correlations
Table 4:
Result of Hypothesis 2

		Success_Rate	Fraud_Risk
Success_Rate	Pearson Correlation	1	.308**
	Sig. (2-tailed)		.000
	N	368	368
Fraud_Risk	Pearson Correlation	.308**	1
	Sig. (2-tailed)	.000	
	N	368	368

Source: Researcher's Coputation (2026). **. Correlation is significant at the 0.01 level.

The results of Hypothesis Two examine the relationship between project success rate and cyber fraud risk among selected banks in Lagos State. The correlation analysis shows a Pearson correlation coefficient (r) of 0.308, indicating a moderate positive relationship between project success rate and cyber fraud risk. This suggests that changes in project success rate are associated with corresponding changes in cyber fraud risk. The significance value (p=0.000) is less than the 0.01 level, indicating that the relationship is statistically significant.

Given that the relationship is both positive and significant, the null hypothesis (H_{02}), which states that there is no significant relationship between project success rate and cyber fraud risk, is rejected. This implies that project success rate is an important factor influencing cyber fraud risk among selected banks in Lagos State. In practical terms, it suggests that variations in how successfully projects are executed can significantly affect the level of exposure to cyber fraud within the banking sector.

H_{03}: Project performance index does not significantly affect cyber fraud risk among selected banks in Lagos State**.**

Table 5:
Result of Hypothesis 3
Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.556[a]	.309	.307	.65473

a. Predictors: (Constant), Perf_Index

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	70.119	1	70.119	163.573	.000[b]
	Residual	156.893	366	.429		
	Total	227.012	367			

a. Dependent Variable: Fraud_Risk
b. Predictors: (Constant), Perf_Index

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	1.574	.166		9.498	.000	1.248	1.900
	Perf_Index	.552	.043	.556	12.790	.000	.467	.637

Source: Researcher's Coputation (2026).Dependent Variable: Fraud Risk

The results of Hypothesis Three examine the effect of project performance index on cyber fraud risk among selected banks in Lagos State. The model summary shows a correlation coefficient (R) of 0.556, indicating a strong positive relationship between project performance index and cyber fraud risk. The coefficient of determination ($R^2 = 0.309$) reveals that approximately 30.9% of the variation in cyber fraud risk is explained by project performance index. This suggests that project performance index is a substantial predictor of cyber fraud risk compared to other variables examined in the study.

The ANOVA results indicate that the regression model is statistically significant ($F = 163.573$, $p < 0.001$), confirming the overall fitness of the model. The coefficient results further show that project performance index has a positive and significant effect on cyber fraud risk ($\beta = 0.556$, $t = 12.790$, $p < 0.001$). This implies that improvements or changes in project performance index significantly influence the level of cyber fraud risk within the banking sector. Based on these findings, the null hypothesis (H03), which states that project performance index does not significantly affect cyber fraud risk, is rejected. It can therefore be concluded that project performance index has a strong and statistically significant effect on cyber fraud risk among selected banks in Lagos State.

Discussion of Findings

The findings of the study indicate that project completion rate has a positive and statistically significant effect on cyber fraud risk among selected banks in Lagos State. This suggests that

delays or inefficiencies in project completion increase the likelihood of exposure to cyber fraud. Although the strength of the relationship is relatively weak, its significance highlights the importance of timely execution of IT and security-related projects in minimizing system vulnerabilities. When such projects are not completed as scheduled, gaps in system protection may arise, making banking systems more susceptible to cyber threats. This finding aligns with Almeida et al. (2022), who observed that delays in project implementation create opportunities for cybercriminal exploitation. Similarly, Ajemunigbohun (2023) emphasized that operational inefficiencies weaken internal control systems and heighten fraud risk. However, the weak explanatory power supports Kerzner's (2022) assertion that timely completion alone is insufficient without quality execution and effective risk management. In Lagos State, where banks operate in a highly digital and high-volume transaction environment, delays in implementing cybersecurity projects can significantly increase fraud incidents, as also reflected in NIBSS (2024). This reinforces the relevance of Risk Management Theory, which underscores timely implementation of risk controls as essential to reducing exposure to threats (Hopkin, 2021).

The study further revealed a moderate, positive, and statistically significant relationship between project success rate and cyber fraud risk. This implies that the extent to which projects achieve their intended objectives plays a critical role in determining fraud vulnerability. Projects that fail to meet scope, cost, or quality requirements may leave unresolved security gaps that can be exploited by cybercriminals. This finding is consistent with Joslin and Müller (2022), who linked project success to improved organizational performance and risk outcomes, and with Ajemunigbohun (2023), who found that failed projects often lead to system vulnerabilities. Lawal, Hammed, and Ayanleke (2023) also argued that project success in risk-sensitive sectors must incorporate security effectiveness rather than focusing solely on traditional performance measures. The result reflects the complexity of banking systems in Lagos State, where integrated digital platforms require comprehensive project execution to ensure security. This supports Systems Theory, which emphasizes that inefficiencies in one component of an organization can affect overall system performance (Skyttner, 2022). Consequently, redefining project success to include cybersecurity outcomes is essential for reducing fraud risk.

In addition, the findings showed that project performance index has a strong, positive, and statistically significant effect on cyber fraud risk, with the highest explanatory power among the variables examined. This indicates that project performance, as measured through efficiency, quality, and adherence to standards, is a major determinant of cyber fraud risk in banks. Poorly performing projects often reflect weak monitoring, inadequate testing, and ineffective implementation, all of which increase vulnerability to cyber fraud. This finding is consistent with Almeida et al. (2022), who established a strong link between project performance and cybersecurity effectiveness, and with Ajemunigbohun (2023), who highlighted the role of weak project evaluation in increasing fraud risk. Ogundeko, Lawal, and Ajemunigbohun (2024) further noted that strong performance management systems are necessary for achieving both security resilience and competitive advantage in financial services. Saxena et al. (2021) also emphasized that effective internal controls embedded in project performance frameworks are critical in mitigating fraud. In the Lagos banking environment, where cyber threats are constantly evolving, continuous performance monitoring is essential to ensure system security. This finding strongly supports Risk Management Theory, which advocates continuous evaluation and control as key to managing risks effectively (Bromiley et al., 2021).

The findings demonstrate that project management outcomes significantly influence cyber fraud risk among selected banks in Lagos State. While project completion rate has a relatively weaker effect, project success rate and project performance index exert stronger influences on fraud risk. This suggests that beyond completing projects, the quality, effectiveness, and performance of project execution are critical in mitigating cyber threats. The results highlight the need for banks to integrate project management practices with cybersecurity strategies, ensuring that all stages of project execution contribute to risk reduction. However, since this study was limited to selected banks in Lagos State, the findings should be interpreted with caution, and future research should explore whether these outcomes apply to other regions within Nigeria to validate their broader applicability.

5.0 Conclusion and Recommendations

The study concludes that project management outcomes significantly influence cyber fraud risk among selected banks in Lagos State. Project completion rate, project success rate, and project performance index all contribute to variations in cyber fraud risk, with project performance index emerging as the most influential factor. Ineffective project execution, inadequate performance monitoring, and failure to achieve project objectives increase vulnerability to cyber threats. This underscores the importance of effective project management in enhancing cybersecurity and minimizing fraud risk within the banking sector.

Based on these findings, banks should prioritize the timely completion of projects, especially those related to cybersecurity, to reduce exposure to system vulnerabilities. It is also important to adopt comprehensive definitions of project success that incorporate cybersecurity outcomes, ensuring that projects contribute to fraud prevention. Furthermore, banks should implement robust performance evaluation systems that integrate key performance indicators with cybersecurity measures, while strengthening monitoring and evaluation processes to enable early risk detection. Continuous training and capacity development for staff are equally necessary to improve project management capabilities and response to emerging cyber threats.

In this study, regression models examine each predictor separately to assess their individual effects on cyber fraud risk. However, it is acknowledged that a comprehensive multivariate model, including all explanatory variables simultaneously, would provide a more holistic understanding of how these factors collectively influence cyber fraud risk. Future studies should consider adopting such an integrated approach to capture the interdependencies between project completion rate, project success rate, project performance index, and other relevant variables. Future studies should employ longitudinal designs to examine changes over time and conduct comparative analyses across regions to enhance generalizability. Additional variables such as organizational culture, regulatory compliance, and technological innovation should also be explored.

Acknowledgements:
This paper is sponsored by the Tertiary Education Trust Fund (TETFUND)

References

Ajemunigbohun, S. S. (2023). Risk financing techniques and SMEs performance: Empirical evidence from Nigeria. *Journal of Financial Crime, 28*(4), 1205-1220.

Ajemunigbohun, S. S., & Ipigansi, P. (2022). Financial knowledge, financial confidence and risk attitudes: Evidence from selected motor insurance policyholders in Nigeria. *Fuoye Journal of Accounting and Management, 5*(1), 1-22.

Ajemunigbohun, S. S., Isimoya, O. A., & Elegunde, A. F. (2020). Risk attitude, insurance patronage and SMEs performance: Empirical evidence from Lagos, Nigeria. *Annals of the University Dunarea de Jos of Galati: Fascicle I, Economics and Applied Informatics, 26*(2), 70-78.

Alketbi, A., Alshamsi, S., & Almazrouei, H. (2022). Cybersecurity threats and financial institutions: A global perspective. *Journal of Financial Crime, 29*(3), 1021-1035.

Almeida, F., Santos, J., & Monteiro, J. (2022). Project management and cybersecurity: An empirical analysis. *International Journal of Project Management, 40*(5), 512-524.

Bouveret, A. (2022). *Cyber risk for the financial sector: A framework for quantitative assessment*. International Monetary Fund.

Bromiley, P., Rau, D., & McShane, M. (2021). Enterprise risk management: Review and future directions. *Long Range Planning, 54*(1), 101-115.

Central Bank of Nigeria. (2023). *Financial stability report*. Author.

Ebere, N. C. (2024). Online transaction fraud and financial performance of deposit money banks in Nigeria. *International Journal of Public Administration, 3*(2), 376-395.

Gee, J., & Button, M. (2019). The financial cost of fraud: Global trends. *Journal of Financial Crime, 26*(3), 677-692.

Hopkin, P. (2021). *Fundamentals of risk management*. Kogan Page.

Idris, A., Ogedengbe, F. A., & Altalhi, A. (2025). Cybersecurity practices and operational performance in Nigerian banks. *Spectrum Journal of Social Sciences, 3*(1), 25-42.

Isibor, A. (2022). Internal control systems and fraud prevention in Nigerian banks. *International Journal of Accounting Research, 10*(2), 45-60.

Joslin, R., & Müller, R. (2022). Relationships between a project management methodology and project success. *International Journal of Project Management, 40*(3), 204-217.

Kerzner, H. (2022). *Project management: A systems approach to planning, scheduling, and controlling*. Wiley.

Koech, C., & Kimani, D. (2018). Control environment and fraud detection in organizations. *International Journal of Economics and Finance, 10*(6), 45-56.

Kshetri, N. (2023). Cybercrime and cybersecurity in financial institutions. *Telecommunications Policy, 47*(2), 102-118.

Lawal, Y. A., Hammed, O. G., & Ayanleke, A. O. (2023). Risk management and performance of construction projects in Lagos State, Nigeria. *Management, 11*(1), 1-13.

Meredith, J., Mantel, S., & Shafer, S. (2021). *Project management in practice*. Wiley.

Müller, R., Drouin, N., & Sankaran, S. (2022). Organizational project management and performance. *Project Management Journal, 53*(1), 3-15.

Nigeria Inter-Bank Settlement System. (2024). *Annual fraud landscape report 2023*. Author.

Nyakarimi, S. N., Kariuki, P., & Wanjohi, J. (2020). Internal control systems and fraud detection in financial institutions. *International Journal of Finance and Accounting, 9*(1), 12-25.

Odukwu, V. C., Eke, P., & Chukwumati, M. (2022). Impact of cybersecurity on fraud prevention in Nigerian commercial banks. *Jurnal Akuntansi, Keuangan dan Manajemen, 4*(1), 15-27.

Ogedengbe, F. A., Idris, A., & Altalhi, A. (2025). Cybersecurity and operational resilience in Nigerian banks. *Journal of Banking Regulation, 26*(1), 88-104.

Ogundeko, S. T., Lawal, Y. A., & Ajemunigbohun, S. S. (2024). Effect of blockchain technology adoption on the competitive advantage of financial services providers in Lagos, Nigeria. *International Journal of Scientific Research in Multidisciplinary Studies, 10*(8), 44-51.

Olulade, M., Ilugbusi, O., & Awoniyi, M. (2019). Fraud prevention mechanisms in banking institutions. *Journal of Accounting and Finance, 19*(4), 98-110.

Otuogha, C. (2021). Fraud risk management in Nigerian banking sector. *African Journal of Business Management, 15*(4), 112-120.

Saxena, R., Gupta, P., & Singh, A. (2021). Internal controls and fraud mitigation. *Journal of Risk and Financial Management, 14*(6), 250.

Serrador, P., & Pinto, J. (2021). Does agile work? A quantitative analysis of project success. *International Journal of Project Management, 39*(4), 312-322.

Skyttner, L. (2022). *General systems theory: Problems, perspectives, practice*. World Scientific.

Tade, O. (2021). Fraud and risk assessment in Nigerian financial institutions. *Journal of Financial Regulation and Compliance, 29*(2), 245-260.

Too, E., & Weaver, P. (2021). The management of project management: A conceptual framework. *International Journal of Project Management, 39*(3), 234-245.

Von Bertalanffy, L. (2021). *General system theory: Foundations, development, applications*. Braziller.