International Review of Management and Marketing

ISSN: 2146-4405

available at http: www.econjournals.com

International Review of Management and Marketing, 2026, 16(6), 406-415.

Real-Time Internal Control Dynamics and Fraud Prevention: A Framework for Strengthening Financial Integrity in Public Sectors

Henry Adelakun Adinlewa[1], Ayobaye Salemcity[2]*, Elza Odendaal[2], Niyi Solomon Awotomilusi[1]

[1]Department of Accounting, Afe Babalola University Ado, Nigeria, [2]Department of Auditing, University of South Africa, South Africa. *Email: ayobaye.salemcity@aaua.edu.ng

Received: 30 December 2025 **Accepted:** 27 June 2026 **DOI:** https://doi.org/10.32479/irmm.22838

ABSTRACT

The evolving fraud dynamics in the public sector of Nigeria, despite existing control mechanisms, motivate the investigation of real-time internal control practices to mitigate fraud. This study examines how authorisation, biometric authentication, periodic checks, and information communication and technology oversight structures contribute to mitigating fraud within the Nigerian public sector. The study adopts a survey design and data were collected through structured questionnaires administered to 163 purposively selected staff members of Ekiti State Internal Revenue Service. Descriptive and inferential statistics were employed to analyse responses, while a modified econometric model was used to evaluate the impact of the variables on fraud prevention outcomes. The results indicate that real-time authorisation effectively prevents unauthorised activities, enhances compliance, and strengthens fraud prevention. Similarly, periodic checks promote instant detection of irregularities, ensuring continuous oversight and improved fraud prevention. While biometric activities like fingerprint scanning, facial recognition, and iris detection are seen as beneficial, their direct impact on strengthening accountability and traceability in the studied context was not evident. The study concludes that well-designed internal-control policies and procedures are crucial in deterring financial misconduct in the Nigerian public sector. Recommendations include implementing more stringent authorisation layers and tightening biometric verification to complement internal control measures.

Keywords: Authorisation, Biometric Authentication, Fraud Prevention, ICT Oversight, Real-Time Internal Control
JEL Classifications: H83, M42, D73, O33, C83

1. INTRODUCTION

The fabric of the public sector is threatened by a series of fraudulent activities globally. Fraudulent activities have been a damaging threat to economic growth, which could drain public resources and undermine institutional trust across both developed and developing nations. Many cases of fraud in the public sector have been reported globally. The case of Credit Suisse in 2025 on tax evasion in the United States and the missing World Bank-funded Nigerian water project in 2024 are recent fraudulent cases that can be pointed to. The case of Halima Shehu, the CEO/National Coordinator of NISPA, unauthorised movement of ₦44 billion, is also a typical failure of an internal control system that demands real-time prevention. Many scholars studied the cause of weak internal control and a lack of accountability (Rahman et al., 2019), and diversion of public resources for personal use (Abei, 2021), which have led to monetary losses, caused legal issues, eroded investor confidence, and created barriers to economic expansion.

Nwosu et al. (2025) found that poor information communication and technology (ICT) oversight is a bane to sustainable development and exposes a system to fraud and systemic failure. To curb this menace, the World Bank advocated advanced data analytics that

act on a real-time basis to expose instances of collusion, fraud, and corruption in public spending (Ortega-Nieto et al., 2023). However, the problem still exists despite the systems put in place by governments and international organisations, especially regarding real-time prevention, as the speed and complexity of fraudulent transactions usually surpass fraud detection capabilities.

Substituting proactive, technologically driven oversight through automated authorisation systems for retrospective reviews, real-time internal control practices became essential to ensure that real-time internal control systems are put in place to transform organisational risk management. Some scholars argue that sound internal control systems reduce the risk of fraud and facilitate its early detection (Abdullah et al., 2023), while Awotomilusi et al. (2023) claim that efficient internal control systems in a few Ekiti State public institutions significantly improve the prevention and detection of fraud. These studies, however, utilise after-the-fact forensic audits and traditional internal controls with no consideration for automation that can easily flag any anomalies noticed in transactions.

Scholars draw attention to the substantial underutilisation of automated and AI-driven tools, quoting capacity and infrastructure-related obstacles (Nwosu et al., 2025). Several studies also support the need for a strong conceptual foundation for real-time internal control reforms. While Shehu (2025) and Adeyemo and Obafemi (2024) explain that well-designed internal controls and the integration of ICT will significantly reduce fraud risks, Awotomilusi et al. (2023) and Musyoki (2023) advocate for mechanisms that monitor any anomalies and institutional accountability structures that support fraud deterrence. Hence, there is an urgent need to transition from traditional models to real-time systems. This transition is expected to enhance transparency, expose fraudulent activities and align with global best practices in public financial management. Thus, to improve fraud detection and prevention, the Nigerian public sector must prioritise the adoption of real-time internal control procedures supported by evidence-based policies, robust ICT oversight, and adaptive infrastructure. This study, however, attempts to investigate whether real-time internal control practices will identify and stop fraud in Nigeria's public sector, specifically on its recurrent expenditures. Some selected ministries, departments and agencies with a high level of financial transaction activity and probable exposure to fraud risk are considered in the study for a period of ten years between 2015 and 2024.

2. LITERATURE REVIEW

2.1. Conceptual Review

2.1.1. Fraud prevention

Fraud prevention is the act of systematically blocking or eliminating any opportunities for fraudulent activities in public sector institutions by detecting any form of financial irregularities early, effectively discouraging them and addressing them appropriately. Public sector institutions have been smeared with a series of financial fraud, which has caused damage to the economy. However, with advancements in technology, real-time internal control practices have shifted fraud management from a traditional to a preventive and continuous approach (Rahman et al., 2019). These controls offer immediate oversight that closes the gaps where fraud can occur by employing tools such as biometric verification, instant authorisation systems, and automated monitoring dashboards. According to Abei (2021) and Shehu (2025), these tools strengthen compliance, improve accountability, and significantly limit the chances for dishonest activities to thrive. Fraud prevention, therefore, has become a crucial tool for evaluating the effectiveness of real-time internal control systems in public sector institutions. Nwosu et al. (2025), in their study, underscore the strategic need for real-time internal controls to protect public funds. They point out that institutions that fail to fully adopt ICT tools and automation often struggle to build strong defenses against fraud.

2.1.2. Real-time internal control practices

The process of putting in place policies, procedures, and activities to ensure that financial and operational processes of an organisation are reliable, its assets are protected, financial reports are accurate, and its operations comply with relevant laws and regulations is termed internal control (Brenya et al., 2023). The Committee of Sponsoring Organizations of the Treadway Commission (COSO Framework, 2013) elaborates that internal control is a process carried out by an entity's board, management, and employees to provide reasonable assurance that the organisation will meet its objectives in three key areas: Efficient operations, dependable financial reporting, and compliance with applicable laws and regulations. Both Abdullah et al. (2023) and Yolanda (2021), in their complementary studies, emphasise the important role that internal control plays in fraud prevention. Abdullah et al. (2023) view internal control as a structured system of policies, procedures, and ethical oversight essential for fostering accountability and reducing risks of fraud within organisations. In contrast, Yolanda (2021), through interviewing staff members of microfinance institutions in Sweden, identifies weaknesses in internal controls, such as poor segregation of duties and limited oversight, as entry points for fraud. Yolanda (2021) stresses the need for staff compliance with procedures and a proactive, technology-driven approach that enables real-time fraud prevention, thereby enhancing the overall effectiveness and responsiveness of internal control systems. The above findings provide a foundational understanding of internal control as a reactive defense mechanism against fraud.

2.1.3. Authorisation

Authorisation is a fundamental part of internal control that allows only the right people to approve transactions or grant access to sensitive information. However, the introduction of modern automated platforms, including enterprise resource planning (ERP) systems, has challenged the effectiveness of the slow, manual approval methods inherent in traditional processes (Shehu, 2025; Adeyemo and Obafemi, 2024). Real-time authorisation is built directly into modern automated platforms such as ERP systems. Laden with other preventive measures such as multi-factor authentication, organisations can protect themselves against unauthorised activities, promote compliance, and reduce fraud risks (Abei, 2021; Nwosu et al., 2025). This is an advancement over the traditional process of authorisation. Invariably, real-time authorisation shifts the focus from a routine administrative step

to an active defense mechanism that upholds ethical behavior and strengthens modern fraud-risk management (Rahman et al., 2019).

2.1.4. Periodic checks

Periodic checks have been a part of internal control systems over time. It is traditionally the reconciliation or audit of records conducted continuously on a monthly, quarterly, biannual, annual or even daily basis. However, these checks have now shifted from rigid, scheduled reviews to more dynamic, automated processes due to the large volume of transactions occurring in recent times. In modern internal control environments, periodic checks are increasingly powered by real-time monitoring tools that flag any abnormalities noticed in a transaction. In real-time, it monitors transactions, detects unusual activities, raises alerts, and processes the data collected, providing timely reports to avert potential risks or irregularities (Awotomilusi et al., 2023; Waliullah and Alam, 2024). By implication, automated systems have the capacity to flag potential problems in real-time, strengthen the fraud prevention process and improve timely compliance actions (Shehu, 2025; Musyoki, 2023). Ultimately, automated periodic checks bridge the gap between conventional oversight and real-time, technology-driven internal control systems.

2.1.5. Biometrics

In real-time internal control systems, the need for biometric technology cannot be overemphasised. Biometric technology involves fingerprint scanning, facial recognition, and iris detection. According to Shehu (2025) and Rahman et al. (2019), traditional access methods such as passwords or identification cards rely on distinctive physical features which can invariably be lost, shared or forgotten. In contrast, Abei (2021) and Waliullah and Alam (2024) stated the need for real-time internal control systems that use biometric authentication for system logins, financial approvals, and access to restricted areas. Adeyemo and Obafemi (2024) and Nwosu et al. (2025) support that this process will not only prevent identity-related fraud in real-time but will also ensure audit trails that link each action performed or transaction to a verified user. The use of biometrics and other technologies eventually helps organisations to make a shift from traditional internal controls to modern, technology-driven internal controls that protect assets and build institutional trust (Awotomilusi et al., 2023).

2.1.6. ICT oversight structure

The ICT oversight structure is the comprehensive governance framework that guides the operation of ICT in an organisation. Rahman et al. (2019) and Waliullah and Alam (2024) explain that the framework brings policies, technical systems, and supervisory processes together and ensures that they are well deployed, secured, and monitored. This implies that real-time internal control in the organisation depends on this framework to work effectively. Its efficient performance is, however, dependent on key features such as access controls, data protection measures, audit trails, and institutional ICT policies. Nwosu et al. (2025) and Adeyemo and Obafemi (2024) explain that these features allow tools like biometrics, automated approvals, and continuous auditing to work as anticipated. Meanwhile, when oversight is not in place, instances of fraud can easily slip through (Abei, 2021; Musyoki, 2023) and the system becomes vulnerable to a series of attacks. Although the oversight function may not stop vulnerability outright, it determines the level of reliability and effectiveness of the real-time internal control system that is put in place. A strong ICT oversight function is therefore essential to improve accountability, strengthen system resilience, and protect public resources.

2.2. Theoretical Review

The Fraud Pentagon Theory was propounded by Crowe in 2011 to offer a useful framework for understanding why fraud is committed in society. The theory explains how and why fraud happens and why traditional control systems cannot handle the fraud rate in today's global space. It identifies pressure, opportunity, rationalisation, competence, and arrogance as the key drivers of fraud in society. According to Crowe (2011), pressure is the challenges or hardships faced by individuals - personal or work-related - that push them into unethical behaviour, while opportunity is when individuals take advantage of the gap or weaknesses in an organisation's control system that make it easier for fraud to take place. He explains further that rationalisation justifies unethical actions. Competence reflects the skills and knowledge a person has that enable them to successfully carry out and hide fraudulent activities. Arrogance shows the attitude above the law that the offender puts in place when carrying out their unethical behaviour. Real-time internal controls can directly address several of these drivers. In the context of Nigeria, the Fraud Pentagon Theory reveals that the key fraud drivers can be addressed with continuous monitoring and automated checks with strong ICT oversight functions. The theory, therefore, provides a solid foundation for evaluating how real-time internal control practices can enhance fraud prevention and rebuild public trust in Nigeria's financial governance systems.

2.3. Empirical Review and Hypotheses Development

2.3.1. Authorisation and fraud prevention

Authorisation serves as a critical gatekeeping mechanism in enhancing fraud prevention, particularly within the public sector. Empirical studies consistently affirm that robust authorisation mechanisms play a critical role in the prevention of fraud, particularly when integrated into structured internal control systems. Shehu (2025) examined in her research how internal control activities can mitigate fraud among small and medium enterprises (SMEs) in Nigeria. Primary data were gathered with the aid of questionnaires administered to 196 respondents. It was found that clearly defined approval hierarchies significantly reduced fraudulent behavior in Nigerian SMEs. While Nnah and Maccarthy (2024) in their research on digital accounting systems and fraud mitigation in the Rivers State public sector, using questionnaires to gather their data, revealed that timely authorisation within information and communication processes positively influenced fraud prevention in the public sector. Yolanda (2021) obtained primary data through semi-structured interviews with eight microfinance banks in Cameroon to understand how internal control prevents and detects fraudulent activities in the banks. In the study, it was identified that poor authorisation practices are a major enabler of internal fraud. Similarly, Nwosu et al. (2025), using a structured questionnaire to determine the effect of automated internal control on fraud prevention, observed that weak utilisation of automated approval systems in Anambra's

SMEs contributed to delays in fraud detection. Awotomilusi et al. (2023) also used a questionnaire to gather data to determine how internal control systems effectively detect and prevent fraud in public sector institutions in Ekiti State. They highlighted that supervisory approvals and transaction validations reinforced accountability in Ekiti State's public institutions. Therefore, from the foregoing, the following hypothesis was initiated:

H_{01}: Real-time authorisation mechanisms do not have a significant effect on fraud prevention in the Nigerian public sector.

2.3.2. Periodic checks and fraud prevention

Periodic checks, which traditionally involve scheduled audits, reconciliations, and supervisory reviews, have been empirically validated as essential components of internal control systems that significantly contribute to fraud prevention, particularly within the public sector and SME environments. Empirical findings confirm that periodic checks, when structured, consistent, and technology driven contribute significantly to fraud prevention. Shehu (2025) examined the effect of internal control activities on fraud mitigation among SMEs in Nigeria using questionnaires. It was revealed that regular internal reviews and compliance monitoring reduced fraudulent occurrences. Ohwo (2024), who analysed the data gathered in his study using a multiple regression model, found that periodic supervisory assessments within information systems improve fraud detection in Deposit Money Banks (DMBs). Ololade (2024) administered questionnaires to selected SMEs in Lagos and Ibadan. He found that periodic control testing helped reduce manipulation in SME accounting practices. These findings affirm that automated periodic checks play a pivotal role in strengthening fraud prevention frameworks. Hence, the following hypothesis was formulated:

H_{02}: Real-time automated periodic checks do not have a significant effect on fraud prevention in the Nigerian public sector.

2.3.3. Biometrics and fraud prevention

Organisations that tie access to unique physical traits significantly reduce impersonation, unauthorised access, and identity-driven fraud. Bobkowska et al. (2019) maintain that biometric tools are used to ensure that only the right individuals can initiate or approve sensitive transactions. Research highlights the importance of biometric technology to strengthen fraud prevention, especially through real-time identity verification and access control. Oyekunle et al. (2025) researched intelligent fraud prevention using behavioural biometrics. They used logistic regression, Wilcoxon signed-rank tests, and multivariate regression models to analyse the data and found that ethical data governance is essential to ensure the responsible use of behavioural biometrics to prevent fraud. Topsy (2025) gathered data from 154 executive members of 14 DMBs in Nigeria using structured questionnaires to determine how biometric technology applications prevent fraud in the banks. It was found that fingerprint biometrics significantly prevents fraud among listed DMBs in Nigeria. Umoh and Ekpo (2023) and Rai (2024) also studied the relationship between biometrics and fraud control using primary data. They found that biometrics has a positive impact on fraud control in the Akwa Ibom State civil service. Considering the above findings, it becomes important to know if real-time biometric authentication will prevent fraud in the Nigerian public sector. Hence, we have the following hypothesis:

H_{03}: Real-time biometric authentication does not have a significant effect on fraud prevention in the Nigerian public sector.

2.3.4. ICT oversight structure and fraud prevention

Some studies made it clear that having a strong ICT oversight structure is essential for preventing fraud, especially in public sector institutions and SMEs (Mwai et al., 2023). ICT oversight encompasses the systems, policies, and supervision that ensure an organisation's technology is secure and properly managed. Across the literature, researchers agree that when ICT is well-governed, fraud becomes much harder to commit. For example, Shehu (2025) explains that automating approvals and enabling real-time monitoring help SMEs close loopholes that fraudsters often exploit. Adeyemo and Obafemi (2024) also show that banks with solid ICT policies detect fraud more quickly and more accurately.

The consequences of weak ICT capacity are, however, very serious. Studies revealed that poor infrastructure, inadequate technical capacity, and limited supervision make a system vulnerable and prone to fraudsters (Umoh et al., 2024; Agyapong and Boakye, 2024). Umoh et al. (2024), using a descriptive survey design to analyse the data they gathered, found that poor oversight, lack of technological infrastructure, and low organisational commitment are the main loopholes that fraudsters exploit to perpetrate their fraudulent activities. Agyapong and Boakye (2024), using thematic analysis in their study on cybersecurity practices and fraud prevention in Ghana, found that despite putting all the technical measures in place, there is a need for a holistic approach that combines the technical measures with an ICT oversight structure to prevent fraud. The evidence from the foregoing shows that the ICT oversight structure is a critical moderator that contributes greatly to fraud prevention in organisations. This study, therefore, hypothesises as follows:

H_{04}: ICT oversight structure does not significantly moderate the relationship between real-time internal control practices and fraud prevention in the Nigerian public sector.

3. METHODOLOGY

This study used a survey research design and collected data using self-administered structured questionnaires, covering aspects such as real-time authorisation, biometric control, automated monitoring, and ICT oversight structure as fraud prevention indicators. The population of the study comprises 326 staff members employed at the Ekiti Internal Revenue Service, Ekiti State, Nigeria, at 31st December 2024. Purposive sampling was used to select the sample because the study requires respondents with specific expertise and direct experience relevant to the research objective. The sample, therefore, consisted of 163 staff members from the Tax Compliance Unit, which constitutes 50% of the population. The data collected were analysed using descriptive and inferential statistics. This study adapted the model used by Awotomilusi et al. (2023). Hence, based on the objective of this study, the adapted model was framed as follows:

$$FRPt = \alpha + \beta_1 RTA_t + \beta_2 BIO_t + \beta_3 AMP_t + \beta_4 ICT_t + \varepsilon_t \quad (i)$$

Where:

FRP_t = Fraud prevention
RTA_t = Real-time authorisation practices
BIO_t = Use of biometric authentication
AMP_t = Automated monitoring and periodic checks
ICT_t = ICT oversight structure strength
t = time
ε_t = Error term
α is the intercept (constant)

4. RESULTS AND DISCUSSION

4.1. Descriptive Statistics

Table 1 presents the descriptive statistics for the variables used in this study.

The descriptive statistics in Table 1 show that the average response regarding authorisation (AUTH) is 4.5398, which signifies agreement with the questions raised. The standard deviation is 0.5121, which indicates that the responses vary moderately considering their distance from the mean value, showing a 11.28% coefficient of variation with a maximum value of 5 and a minimum value of 3. The responses are negatively skewed and have a skewedness of −0.2981 and a kurtosis of 1.4276, indicating that the responses are normally distributed. From the table, it is also evident that the average response regarding periodic checks (PRDCK) is 4.478, which signifies agreement with the questions raised. The standard deviation is 0.5251, which indicates that the responses vary moderately considering their distance from the mean value, showing a 11.72% coefficient of variation with a maximum value of 5 and a minimum value of 3, representing undecidedness. The responses are negatively skewed and have a skewedness of −0.17083 and a kurtosis value of 1.6105, indicating that the responses are normally distributed.

Furthermore, the average response regarding biometrics (BIOM) is 4.5705, which signifies agreement with the questions raised. The standard deviation is 0.5552, which indicates a moderate variation considering its distance from the mean value, showing a 12.14% coefficient of variation with a maximum value of 5 and a minimum value of 2, representing disagreement. The responses are negatively skewed and have a skewedness of −1.0401 and a kurtosis value of 4.30, indicating that the responses are normally distributed. Lastly, the descriptive statistics in Table 1 showed that the average response regarding ICT oversight structure (ICTOV) is 4.3251, which signifies agreement with the questions raised. The standard deviation is 0.5971, which indicates that the responses vary moderately considering their distance from the mean value, showing a 13.8 coefficient of variation with a maximum value of 5 and a minimum value of 2, representing disagreement. The responses are negatively skewed and have a skewedness of −0.434 and a kurtosis value of 3.32, indicating that the responses are normally distributed.

4.2. Test of Hypotheses

To test the hypothesis, the partial least squares structural equation modelling (PLS-SEM) technique was employed to examine the relationships and effects between the variables. This is deemed appropriate due to its superiority to other techniques in analysing small sample sizes or data with non-normal distributions, which can be the case in survey data. To test the significance of the PLS-SEM results, a bootstrapping procedure was used, and all constructs under the endogenous variable were analysed with each exogenous variable, and the path coefficients were reported. In testing the hypotheses, the relationship between real-time internal control practices and fraud prevention within the public sector in Nigeria was examined. The Spearman correlation, which is a non-parametric test suitable for hypothesis testing in survey research, was employed. Doing this established the impact of authorisation, periodic checks, biometrics and ICT oversight structure on fraud prevention in the public sector in Nigeria. The correlation results are presented in Table 2.

The correlation results show that fraud prevention (FRDPV) has a positive relationship with authorisation (AUTH) and the relationship is significant in such a way that a 1-time improvement in authorisation (AUTH) will increase fraud prevention (FRDPV) by 22.58%. This is evidenced by the coefficient of 0.22.58* and the P = 0.0038. The correlation results show that periodic checks (PRDCK) have a positive relationship with fraud prevention (FRDPV) and the relationship is significant in such a way that a 1-time improvement in periodic checks (PRDCK) will increase fraud prevention (FRDPV) by 42.25%. This is evidenced by the coefficient of 0.4225* and the P = 0.0000. It is also evident from Table 2 that fraud prevention (FRDPV) has a positive relationship with biometrics (BIOM) and the relationship is significant in such a way that a 1-time improvement in biometrics (BIOM) will increase fraud prevention (FRDPV) by 33.75%. This is evidenced by the coefficient of 0.3375* and the P = 0.0000. Likewise, fraud prevention (FRDPV) has a positive relationship with ICT oversight structure (ICTOV), and the relationship is significant in such a way that a 1-time improvement in ICT oversight structure (ICTOV) will increase fraud prevention (FRDPV) by 41.19%. This is evidenced by the coefficient of 0.4119* and the P = 0.0000. It is further observed that the independent variables, which serve as the measurements of real-time internal control practices, have a positive relationship with one another.

Table 1: Descriptive statistics of variables

Stats	Fraud prevention	Authorisation	Periodic checks	Biometrics	ICT oversight structure
Mean	4.5950	4.5398	4.4785	4.5705	4.3251
SD	0.5047	0.5121	0.5251	0.5552	0.5971
C.V	0.1098	0.1128	0.1172	0.1214	0.1380
Min	3	3	3	2	2
Max	5	5	5	5	5
Skewness	−0.5315	−0.2981	−0.1708	−1.0401	−0.4348
Kurtosis	1.6392	1.4276	1.6105	4.3011	3.3206

4.3. Real-Time Internal Control Practices and Fraud Prevention

The specific objective of the study is to investigate how well real-time internal control practices identify fraud in Nigeria's public sector. It assesses how well authorisation, recurring checks, and biometrics mitigate fraud to achieve this objective, employing Partial Least Squares Structural Equation Modelling (PLS-SEM). The path coefficient, t-statistic value, probability value and R-Square determination, effect size (ƒ2), the predictive relevance of the model, and the predictive relevance of the model index and the other statistical information are presented in subsequent tables.

Tables 3a-e indicate the quality of the measurements and items employed in the analysis. Not all the items met the criteria of the 0.5 threshold for the outer loadings which implies that they were a perfect reflective measurement of the constructs of the study and therefore they were all included in the measurements analysed. The items were also tested for internal consistency. Even though the Cronbach

Table 2: Correlation of the variables

Variables	Spearman's Rho	Fraud prevention	Authorisation	Periodic checks	Biometrics	ICT oversight structure
Fraud prevention	Coefficient	1.000				
	Sig. (2-tailed)	-				
Authorisation	Coefficient	0.02258*	1.000			
	Sig. (2-tailed)	0.0038	-			
Periodic checks	Coefficient	0.4225*	0.2554*	1.000		
	Sig. (2-tailed)	0.0000	0.0010	-		
Biometrics	Coefficient	0.3375*	0.3395*	0.2779*	1.000	
	Sig. (2-tailed)	0.0000	0.0000	0.0000	-	
ICT oversight structure	Coefficient	0.4119*	0.2706*	0.3448*	0.3630*	1.000
	Sig. (2-tailed)	0.0000	0.0000	0.0000	0.0000	-

Table 3a: Construct reliability and validity for authorisation

Variables	Indicators	Factor loadings	Cronbach Alpha	Composite reliability	Average Variance Extracted	No of Items
Authorisation	AUTH1	0.496	0.687	0.699	0.443	5
	AUTH2	0.495				
	AUTH3	0.655				
	AUTH4	0.531				
	AUTH5	0.620				
	AUTH6	0.727				
	AUTH7	0.647				

Table 3b: Construct reliability and validity for biometrics

Variables	Indicators	Factor loadings	Cronbach alpha	Composite reliability	Average variance extracted	No of items
Biometrics	BOMTR1	0.569	0.800	0.828	0.457	7
	BOMTR2	0.778				
	BOMTR3	0.727				
	BOMTR4	0.526				
	BOMTR5	0.707				
	BOMTR6	0.621				
	BOMTR7	0.763				

Table 3c: Construct reliability and validity for periodic checks

Variables	Indicators	Factor loadings	Cronbach alpha	Composite reliability	Average variance extracted	No of items
Periodic checks	PECHK1	0.664	0.791	0.801	0.847	7
	PECHK2	0.657				
	PECHK3	0.702				
	PECHK4	0.764				
	PECHK5	0.597				
	PECHK6	0.599				
	PECHK7	0.664				

Table 3d: Construct reliability and validity for fraud prevention

Variables	Indicators	Factor loadings	Cronbach alpha	Composite reliability	Average variance extracted	No of items
Fraud prevention	FRDPV1	0.679	0.729	0.736	0.480	5
	FRDPV2	0.658				
	FRDPV3	0.734				
	FRDPV4	0.695				
	FRDPV5	0.696				

Alpha is mostly used in social sciences, composite reliability is most preferred in PLS-SEM analyses. All the variables have a composite reliability of more than the 0.7 required threshold. The convergent validity is measured using average variance extracted (AVE), and it shows that the convergent validity for the variables is valid as no one is <0.50, as suggested by Bagozzi et al. (1998).

Table 4 presents the results for the discriminant validity, which is obtained using the Fornell-Larcker Criterion and it is calculated using the square root of AVE in each latent variable. This test is important to validate the degree to which measures of different traits are unrelated to prevent multicollinearity issues.

Table 5 presents the influence of real-time internal control practices on fraud prevention.

The results shown in Table 5 indicate that fraud prevention (FRDPV) is achievable, having a 43.8% variance explained by real-time internal control practices, which can be regarded as high variance. The model is a good fit as the standardised root mean square residual (SRMR) has a value not above 0.1 and the normed fit index (NFI) is close to 1 (Henseler et al., 2014). The contribution of each attribute to the R-square was indicated by the effect size (F-Square). It is evident that authorisation (AUTH) has a strong influence with a value of 0.161, which indicates that if other exogenous variables are held constant while authorisation (AUTH) is removed or stopped in the public sector, R-square will vary by 16%. It is further evident that if other exogenous variables are held constant while biometrics (BIOM) are removed, it will cause R-square to vary by 1%, indicating a low influence. It is also evident that if other exogenous variables are held constant while periodic checks (PRDCK) are removed, it will cause R-square to vary by 10.5%, signifying a moderate influence.

Considering the predictive relevance of each exogenous variable in the model, as indicated by Q^2, it shows that the model has predictive relevance since the value is >0. From Table 5, the P-values of two of the constructs show a significant influence as they are less than ≤0.05. It indicates that authorisation (AUTH) has a direct positive and significant influence on fraud prevention (FRDPV), reflected by the coefficient of 0.354, t-statistics of 4.377 and P = 0.000. This means that having layers of authorisation in the financial process before an action is finalised prevents misappropriation, as fraud will be extremely difficult when the transaction is not handled by just one person from start to finish. Also, the fact that officers who authorise an action can be held accountable when there is an error in the validation of financial actions will allow scrutiny of the process. Likewise, it was observed that biometrics (BIOM) have a positive but insignificant influence on fraud prevention (FRDPV), indicated by the coefficient of 0.102, t-statistics of 1.258 and P = 0.208. This means that developing a unique method of identifying individuals for verification will expose irregularities and intentions of fraud. However, the insignificant effect of biometrics implies that the potential of the usage of the tool to prevent impersonation has not been maximised, as staff members still undergo manual identity confirmation during verification exercises.

From Table 5, it is also evident that periodic checks (PRDCK) have a positive and significant influence on fraud prevention (FRDPV), indicated by the coefficient of 0.331, t-statistics of

Table 3e: Construct reliability and validity for ICT oversight structure

Variables	Indicators	Factor loadings	Cronbach alpha	Composite reliability	Average variance extracted	No of items
ICT oversight structure	ICTOV1	0.412	0.790	0.799	0.492	6
	ICTOV2	0.670				
	ICTOV3	0.745				
	ICTOV4	0.527				
	ICTOV5	0.732				
	ICTOV6	0.737				
	ICTOV7	0.754				

Table 4: Discriminant validity

Study variables	Authorisation	Biometrics	Fraud prevention	Periodic checks
Authorisation	0.666			
Biometrics	0.425	0.676		
Fraud prevention	0.566	0.461	0.693	
Periodic checks	0.509	0.627	0.576	0.666

Table 5: Influence of real-time internal control practices on fraud prevention

Constructs	Path co-efficient	T-statistics	P-values
Authorisation -> Fraud prevention	0.354	4.377	0.000
Biometrics -> Fraud prevention	0.102	1.258	0.208
Periodic checks -> Fraud prevention	0.331	2.775	0.006
Study Variable	**R-square**	**R-square adjusted**	**Q^2**
Fraud prevention	0.438	0.428	0.377
Study Variable	**F-square (effect size)**	**Model_ Fit Summary**	
Authorisation	0.161	SRMR-0.093	
Biometrics	0.011	NFI-0.598	
Periodic Checks	0.105	RMSE–0.565	

Table 6: Moderating effect of ICT oversight on real-time internal control practices and fraud prevention

Constructs		Path Co-efficient	T-statistics	P-values
ICT oversight×authorisation>fraud prevention		−0.133	1.942	0.052
ICT oversight×biometrics>fraud prevention		0.058	0.624	0.532
ICT oversight×periodic checks>fraud prevention		0.009	0.069	0.945
Study Variable	**R-square**	**R-square adjusted**	**Q^2**	
Fraud prevention	0.592	0.574	0.490	
Study Variable	**F-square (effect size)**	**Model_ Fit Summary**		
Authorisation	0.006	SRMR-0.092		
Biometrics	0.000	NFI-0.578		
Periodic Checks	0.047	RMSE–0.734		

2.775 and P = 0.006. This implies that the frequent examination of records for irregular patterns relating to spending and revenue has significantly prevented fraud in the public sector. Hence, the real-time internal control process can significantly reduce fraud, thereby aiding accountability in the public sector. Two of the constructs turned out to have P-values lower than 5%; therefore, the null hypothesis that real-time internal control practices have no significant effect on fraud prevention in the public sector of Nigeria is rejected.

The results of this study align with the empirical evidence of Shehu (2025), who found that clearly defined approval hierarchies significantly reduced fraudulent behaviour in Nigerian SMEs. Adeyemo and Obafemi (2024) also revealed that timely authorisation within information and communication processes positively influenced fraud prevention in DMBs. The results also supported the findings of Awotomilusi et al. (2023) that supervisory approvals and transaction validations reinforced accountability in Ekiti State's public institutions. Hossen et al. (2025), in their study on control environments in South Asian public institutions, furthermore, linked frequent review cycles with enhanced compliance and reduced fraud risk.

However, the results of this study contradict the submission of Nwosu et al. (2025) on biometrics' potential in preventing impersonation and enhancing approval security, as the results show an insignificant effect on fraud prevention. Although Ariyo-Edu (2024) submitted that biometric systems are effective fraud deterrents in environments where manual signatures were often forged or bypassed, this study found that biometric systems are underutilised and hence their effect in preventing fraud is not significant yet.

4.4. Moderating Effect of ICT Oversight Structure on Real-Time Internal Control Practices and Fraud Prevention

Table 6 presents the moderating effect of ICT oversight on real-time internal control practices and fraud prevention.

The results shown in Table 6, respectively, indicate that the ICT oversight structure has no moderating effect on how real-time internal control practices reduce fraud prevention (FRDPV). Although the model is a good fit, as the standardised root mean square residual (SRMR) has a value not above 0.1 and the normed fit index (NFI) is close to 1 (Henseler et al., 2014). The contribution of each attribute to the R-square was indicated by the effect size (F-Square), and it is evident that none of the moderating effects has a strong influence, as none has a 0.1 influence.

Considering the predictive relevance of each exogenous variable in the model, as indicated by Q^2, it shows that the model has predictive relevance since the value is >0. The P-values of all the constructs show an insignificant influence as they are greater than ≤0.05. This indicates that authorisation (AUTH) moderated by ICT oversight (ICTOV) has a direct positive but insignificant influence on fraud prevention (FRDPV), indicated by the coefficient of −0.133, t-statistic of 1.942 and P = 0.052. The implication is that digital authorisation activities and technical infrastructure to track and monitor activities in the public sector do not improve the layers of authorisation in the financial process to prevent misappropriation and fraud. Though it will make fraud extremely difficult, it is not effective in ensuring the scrutiny of the process. Likewise, it was observed that biometrics (BIOM) moderated by ICT oversight (ICTOV) have a positive but insignificant influence on fraud prevention (FRDPV), shown by the coefficient of 0.058, t-statistics of 0.624 and P = 0.532. The implication is that highly sensitive digital environments do provide a unique method of identifying individuals for verification purposes but do not significantly reveal misuse or breach. The insignificant moderating effect may imply that synergy between the biometric system and the ICT facilities in public institutions has not yet been achieved.

From Table 6, it is also evident that periodic checks (PRDCK) have a positive and significant influence on fraud prevention (FRDPV), indicated by the coefficient of 0.009, t-statistics of 0.069 and P = 0.945. The implication is that when digital operations are regularly reviewed by experts familiar with system control and security, even with the integrity of the technical tools in place, it does not make frequent examination of records for irregular patterns relating to spending and revenue yield effective results. Therefore, the moderating effect of ICT oversight structure on real-time internal control practices does not significantly reduce fraud prevention in the public sector. Hence, the null hypothesis that the ICT oversight structure does not significantly moderate the relationship between real-time internal control practices and fraud prevention in the Nigerian public sector is accepted.

5. CONCLUSION AND RECOMMENDATIONS

Public institutions are known for being porous and major fraud activities are recorded in the public sector, especially in

Nigeria. This study examined the capacity of real-time internal control practices in creating a sound internal control system and whether it has a significant effect on lowering the risk of fraud and aids in early detection of fraud by enforcing accountability. Specifically, the study assessed how well authorisation, recurring checks, and biometrics mitigate fraud and the moderating effect of ICT oversight structure in strengthening real-time internal control in preventing fraud in Nigeria's public sector. A survey research design was employed; data were obtained through a closed-ended questionnaire and analysed using PLS-SEM with the aid of SMARTPLS. The results indicate that real-time authorisation prevents unauthorised activities, enforces compliance, and strengthens fraud prevention. Also, it is found that periodic checks encourage instant detection of irregularities, simulating continuous oversight and enhancing fraud prevention, while biometric activities like fingerprint scanning, facial recognition, and iris detection do not significantly strengthen accountability and traceability. The study concludes that policies, procedures, and activities employed by an organisation to guarantee the integrity of financial procedures are significant in deterring financial misconduct and reducing financial mismanagement in the Nigerian public sector.

Based on the study's findings, it is recommended that more layers of authorisation should be introduced before any financial action is finalized to reduce financial misconduct and promote fraud prevention; biometric verification should be tightened to prevent impersonation that can aid fraud; accuracy of records through periodic checks should be given priority to expose irregularities in financial transactions and prevent fraud; systems and structures of digital operation in public institutions should be reviewed to complement internal control practices in the protection of public resources.

REFERENCES

Abdullah, M.W., Hanafie, H., Bayan, A.Y.M. (2023), Internal governance and fraud prevention system: The potentiality of the spiritual quotient. Journal of Governance and Regulation, 12(4), 34-51.

Abei, Y.A. (2021), Impact of Internal Control on Fraud Detection and Prevention in Microfinance Institutions. Sweden: Digitala Vetenskapliga Arkivet, p.68.

Adeyemo, K., Obafemi, F.J. (2024), A survey on the role of technological innovation in Nigerian deposit money bank fraud prevention. South Asian Journal of Social Studies and Economics, 21(3), 33-150.

Agyapong, K., Boakye, I. (2024), Cybersecurity practices and fraud prevention among Ghanaian telecommunication firms: A mixed method analysis. European Journal of Social Sciences Studies, 10(4), ???.

Ariyo-Edu, A.A. (2024), Impact of internal control system on prevention of fraud in the public sector in North Central Nigeria. Journal of Accounting, Finance, and Contemporary Management Research, 1(2), 66-83.

Awotomilusi, N.S., Oke, O.E., Dada, S.A., Dagunduro, M.E. (2023), Assessing the effectiveness of internal control systems on fraud prevention and detection of selected public institutions of Ekiti State, Nigeria. Asian Journal of Economics, Finance and Management, 5(1), 231-244.

Bagozzi, R.P., Yi, Y., Nassen, K.D. (1998), Representation of measurement error in marketing variables: Review of approaches and extension to three-facet designs. Journal of Econometrics, 89(1-2), 393-421.

Bobkowska, K., Nagaty, K., Przyborski, M. (2019), Incorporating iris, fingerprint and face biometric for fraud prevention in e-passports using fuzzy vault. IET Image Processing, 13(13), 2516-2528.

Brenya, B.A., Appiah, K.O., Gyimah, P., Owusu-Afriyie, R. (2023), Public sector accountability: Do leadership practices, integrity and internal control systems matter? IIM Ranchi Journal of Management Studies, 2(1), 4-15.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013), Internal Control-Integrated Framework. Englewood: COSO.

Crowe, H. (2011), Why the Fraud Triangle is no Longer Enough. Available from: https://www.crowehorwath.com

Henseler, J., Dijkstra, T.K., Sarstedt, M., Ringle, C.M., Diamantopoulos, A., Straub, D.W., & Calantone, R.J. (2014), Common beliefs and reality about PLS: Comments on Rönkkö and Evermann (2013). Organizational Research Methods, 17(2), 182-209.

Hossen, M.D., Abedin, M.Z., Chowdhury, T.M., Islam, Z., and Kabir, M.R. (2025), Unveiling the impact of E-governance on the transformation from digital to smart Bangladesh. Pakistan Journal of Life and Social Sciences, 23(1), 85-108.

Musyoki, K.M. (2023), Internal control systems and their role in financial fraud prevention in Kenya. African Journal of Commercial Studies, 3(3), 173-180.

Mwai, R., Wabala, S., Ogada, K. (2023), Role of ICT risk management on insider fraud prevention in commercial banks in Nairobi County. International Journal of Technology and Systems, 8(2), 36-64.

Nnah, L. & Maccarthy, M.I.T., 2024. Digital accounting system and fraud mitigation in federal public enterprises in Rivers State, Nigeria. International Journal of Management, Accounting and Finance, 10(1); 93-121.

Nwosu, N.L., Onyemaobi, N. & Odimmega, C.G., 2025. Utilization of automated internal control system for effective fraud prevention in small and medium scale enterprises in Anambra State. Unizik Journal of Educational Research, Science and Vocational Studies, 1(1); 158-176.

Ohwo, O.K., 2024. Managing fraud in contemporary business environment: The role of information security management—A study of quoted deposit money banks (DMBs) in Nigeria. Management & Marketing Journal, 22(2); 225 - 241.

Ololade, B.M., 2024. Internal control systems of SMEs in Nigeria: A proactive or reactive strategy against employees' fraud? Journal of Financial Crime, 32(1); 49–63.

Ortega-Nieto, D., Fazekas, M., Vaz Mondo, B., Tóth, B., & Braem Velasco, R. A., 2023. Governance Risk Assessment System (GRAS): Advanced Data Analytics for Detecting Fraud, Corruption, and Collusion in Public Expenditures. Washington, D.C.: World Bank Group. https://www.govtransparency.eu/wp-content/uploads/2023/11/WBG-GRAS-Fazekas-Vaz-Mondo-Tóth.pdf.

Oyekunle, S.M., Popoola, A.D., Kolo, F.H.O., Ogunmolu, A.M., Adesokan-Imran, T.O. (2025), Intelligent fraud prevention information banking: A Data governance-centric approach using behavioural biometrics. Asian Journal of Research in Computer Science, 18(5), 525-543.

Rahman, N.H.A., Jamaluddin, A., Hamzah, N., Aziz, K.A. (2019), Establishing an effective internal control system for fraud prevention: A structured literature review. Asia-Pacific Management Accounting Journal, 14(3), 21-47.

Rai, H.B. (2024), Impact of internal control system in preventing, detecting accounting frauds and errors in educational institutions of

Khotang District, Nepal. DMC Journal, 9(8), 86-100.
Shehu, T. (2025), Internal control system and fraud mitigation: A case of selected SMEs in Nigeria. Asian Journal of Advanced Research and Reports, 19(4), 301-15.
Topsy, M.F. (2025), Effect of biometric technology application on fraud prevention among listed deposit money banks in Nigeria. ANUK College of Private Sector Accounting Journal, 2(1), 164-181.
Umoh, B.U., Ofurum, U.D., Folasade, O.A.S. (2024), The impact of bank fraud on economic stability and public trust in Nigeria's financial system. Global Academic Journal of Economics and Business, 6(6), 187-195.
Umoh, U.E., Ekpo, M.E. (2023), Biometrics and fraud control in the Akwa Ibom State civil service. AKSU Journal of Administration and Corporate Governance, 2, 17-31.
Waliullah, M., Alam, M.A. (2024), Fraud Detection in Financial Transactions through Data Science for Real-Time Monitoring and Prevention. Available from: https://www.ssrn
Yolanda, A.A. (2021), Impact of internal control on fraud detection and prevention in microfinance institutions. Karlstad Business School, 5, 1-68.