How to Cite:
Onyiah, I. A., Uche, J. D., Uche, H. I., Ugezu, M. E., & Udeh, H. E. (2026). The Interconnected cybersecurity, operational, and compliance risks in digital tax administration: implications for tax compliance risks in Nigeria. *International Journal of Economic Perspectives*, *20*(11), 1209–1229. Retrieved from https://ijeponline.org/index.php/journal/article/view/1429

The interconnected cybersecurity, operational, and compliance risks in digital tax administration: implications for tax compliance risks in Nigeria

Dr. Ifeanyichukwu Arthur Onyiah
Department of Accounting, Coal City University, Enugu State, Nigeria
Email: ifeanyi_fg@yahoo.com
ORCID number: 0009-0009-2970-0821

Dr. Joy Dakoru Uche
Department of Accounting, Federal University of Environment and Technology, Koroma/ Saakpenwa, Ogoni, Rivers State, Nigeria
Email: joy.dakoru@fuet.edu.ng

Dr. Henry Idoko Uche
Henry Idoko Uche & Co (Chartered Accountant)
Email: Idoko20011@gmail.com

Ugezu, Marymartina Eberechukwu
Department of Accounting, Godfrey Okoye University, Enugu State
Email: Ugezu@gmail.com

Henry Ejikeme Udeh
Department of Accounting, Abia State University, Nigeria
Email: Henry.udeh@abiastateuniversity.edu.ng

***Abstract*---**This study explored cyber-security, operational, and compliance risks in Nigeria's digital tax systems. It measured how cyber-security threats affect tax compliance, how operational issues affect digital tax stability, and how both factors act together. Using a quantitative survey, the study gathered primary data via structured questionnaires and analyzed them through Pearson correlation and regression in SPSS. The results showed a strong, positive link between cyber-security threats and tax compliance risks. Operational challenges had a minor, non-significant effect on digital system continuity. Yet, combined cyber-security and operational risks

© 2026 by The Author(s). ISSN: 1307-1637 International journal of economic perspectives is licensed under a Creative Commons Attribution 4.0 International License.
Corresponding author: *Onyiah, I.A., Email: ifeanyi_fg@yahoo.com*
Submitted: 27 September 2026, Revised: 09 October 2026, Accepted: 19 November 2026

significantly influenced tax compliance. The study concludes that inadequate protection of taxpayer information and digital tax platforms can undermine the benefits of digital tax administration. The study recommends that the Nigeria Revenue Service and State Internal Revenue Services need to boost digital tax security by using encryption, firewalls, multi-factor authentication, and intrusion detection, alongside regular audits and vulnerability tests to fix system flaws.

***Keywords*---**Digital Tax Administration, Cyber-security Risk, Operational Risk and Tax Compliance Risk.

1.0 Introduction

Digital transformation in taxation has been adjudged as a very remarkable improvement in modern administration of tax. With data integration, identity and automation processes, efficient interactions between tax authorities and taxpayers have been improved (OECD, 2020, 2025). In spite of this modernization, tax administration has been exposed to cyber-security threats, operational failures and compliance risks because of the over reliance on these digital platforms.

Cyber-security risk means that cyber threats may affect the integrity, confidentiality, or availability of digital systems and information. Such threats include data theft, phishing, malware, unauthorized access, identity manipulation, ransomware, and attacks on digital infrastructure. These threats are capable of exposing important taxpayer information, alter financial records, compromise taxpayer accounts or interrupt digital services (OECD, 2020, 2025).

According to Pascoe (2024) identifying, protecting against, detecting, responding to and recovering from cyber-security incidents are functions particularly relevant to tax authorities because their digital platforms process confidential personal, business and financial information. The reliability, credibility and continuity of tax administration will be greatly affected if there is a loss of data as result of security breach.

Another important challenge in digital tax administration is Operational risk. In a tax administration environment, operational risk functions through process, people and system failures, inadequate ICT infrastructure, insufficient staff competence, weak internal controls, poor data quality, unplanned downtime, operational loss frequency, ineffective backup and recovery arrangements. The results of these risks are delayed transactions; inaccurate assessments; unsuccessful payments and unreliable taxpayer records (Basel Committee on Banking Supervision, 2021).

The interaction between cyber-security and operational risks is complimentary. A cyber-attack can deactivate electronic tax payments platforms, corrupt files and overwhelm the tax officers responsible for maintaining tax services. Consequently, inadequate operational capacity and integrated risk management increases the

likelihood or consequences of cyber incidents. Pascoe et al. (2024) stated that cyber-security protection and operational reliability should not be treated in isolation. They stated that weakness in one area may increase the vulnerabilities in another and affect the overall performance of digital tax administration.

The negative effects of these interconnected risks become particularly significant when considered alongside tax compliance risk. Tax compliance refers to meeting statutory obligations relating to taxpayer registration, submission of tax returns, accurate reporting of taxable transactions and the payment of tax liabilities when due. Tax compliance risk arises when taxpayers fail to fulfill these obligations or when tax authorities are unable to identify, verify and address such failures effectively. According to OECD (2020; 2025) through improved information exchange, automation and data analysis, digital transformation and compliance management can be enhanced. OECD stated that where taxpayer records are compromised or inaccurate, tax authorities may not identify taxpayers, may not see discrepancies or make incorrect assessments. Oseni (2016) stressed that careless use of ICT and inadequate security could expose digital tax facilities to hackers and online fraud. Similarly, Uguagu et al. (2023) reported that electronic taxation was associated with improved tax compliance in Nigeria, while The Federal Republic of Nigeria (2021) stated that essential services and functions of the government has gradually been dependent on cyberspace and as such is exposed to cyber threats as Egbara et al. (2023) & Obiora and David (2021) confirmed that electronic taxation contributed to decrease in tax evasion and avoidance in Enugu State. Jointly, these studies agreed that digital systems enhance tax administration. For this reason, the Nigeria Data Protection Act 2023 established a legal framework for the protection of personal data and processing of information.

In spite of the successes recorded in the digitalization of tax administration, there is need for more research on cyber-security, operational and tax compliance risks. Oseni (2016), Uguagu et al. (2023) and Egbara et al. (2023), examined ICT adoption, e-taxation and tax compliance-related outcomes. These studies separately examined the effect of cyber-security threats on tax administration and the effect of operational weaknesses on tax administration. The studies further separately looked at the benefits of digital taxation. However, there was no joint examination of these risks together to develop a better knowledge of the vulnerabilities associated with digital tax administration. Against this background, this study examines Interconnected Cybersecurity, Operational and Compliance Risks in Digital Tax Administration: Implications for Tax Compliance Risks in Nigeria**.**

1.2 Statement of the Problem

Cyber-security threats may expose taxpayer information; disrupt electronic files and transactions, while operational risk such as inadequate weak internal controls, staff capacity, poor data quality, and system downtime are capable of sabotaging digital tax services. Hence the effectiveness of Information, communication and technologies depends on security, reliability and operational efficiency as it has been proven to improve taxpayer registration, filing, payment

processing, information management and compliance monitoring in Nigeria (Oseni 2016).

Mas'ud et al. (2023) also highlighted opportunities to improve digital identification and the strategic use of electronic tax data by Nigerian tax authorities. Although these studies provide useful insights, they do not directly establish how cyber-ssecurity and operational risks interact to influence tax compliance risk.

The problem is important because system failures and security incidents may obstruct taxpayers' statutory obligations by restricting platform access, compromising records, delaying transactions or weakening the verification of returns and payments. Operational weaknesses may increase exposure to cyber threats, while cyber incidents can intensify existing operational problems. Their combined effects may therefore differ from their individual effects.
Research Gap

Onyiah et al. (2026) did a study on *Digital Tax Administration and Tax Compliance Risk in Nigeria: An Empirical Assessment* and examined digital taxpayer registration, electronic tax filing and electronic tax payment in relation to compliance risk. The study revealed that Digital Taxpayer Registration has a statistically significant positive effect on Registration Compliance Risk in Nigeria and Electronic Tax Filing does not have a statistically significant effect on Filing Compliance Risk in Nigeria. The study also revealed that Electronic Tax Payment does not have a statistically significant effect on Payment Compliance Risk. These studies did not directly investigate cyber-security risk, operational risk or their joint influence. The central problem is the scarcity of empirical evidence on how cyber threats and operational issues impact tax compliance in Nigeria, especially how these risks work together to disrupt digital tax systems. This study addresses these gaps by examining the relationships and generating evidence relevant to the security, reliability and effectiveness of digital tax administration.

1.3 Objectives of the Study

The main objective is to examine the interaction between cyber-security and operational risks and their implications for tax compliance risk in digital tax administration in Nigeria. The specific objectives are to:

i. Examine the relationship between cyber-security risk and tax compliance risk in digital tax administration in Nigeria.
ii. Determine the effect of operational risk on the reliability and continuity of digital tax processes in Nigeria.
iii. Examine the joint influence of cyber-security risk and operational risk on tax compliance risk in digital tax administration in Nigeria.

2.1 Conceptual Review

2.1.1 Digital Tax Administration

Digital tax administration refers to using ICT for taxpayer registration, assessment, filing, payment, information management, auditing and compliance monitoring. Electronic platforms and digital tools can improve administrative efficiency, accuracy, accessibility and transparency (Onyiah et al., 2026).

In Nigeria, digital tax administration includes online registration, electronic return submission, tax payments and digital databases used for assessment and compliance monitoring (Ogbaisi and Ibifunmilola, 2025 & Oludi 2026). Mas'ud et al. (2023) & Awodun, Somorin, and Sanni (2024) discussed the potential of reliable infrastructure, competent personnel, effective controls, data integration, digital identification, automated tax-risk management and digital transformation as needed to modernize Nigeria's tax system and improve revenue collection.

2.1.2 Cyber-security Risk

According to Pascoe et al., (2024), Cybersecurity risk refers to threats that take advantages of computer systems weaknesses thereby causing financial loss or operational disruption. Cyber-security is generally treated with regards to integrity, availability and confidentiality of tax information. Confidentiality ensures that tax information access is only available to authorized personnel; integrity protects tax information against improper alteration or destruction while availability ensures that authorized users can access the systems when required (ISO/IEC 2022 Sanni, 2025).

2.1.3 Operational Risk

According to Basel Committee on Banking Supervision (BCBS, 2021), Platform downtime, poor data quality, processing errors, weak database integration, inadequate technical skills, unreliable internet connectivity and ineffective internal controls, inadequate or failed processes, people and systems or external events are components of Operational risk. An operational risk causes taxpayers registration, filing returns and tax payment failures. Inconsistent records are created from poor data quality while inadequate staff capacity slows the resolution of technical problems (BCBS, 2021).

2.1.4 Tax Compliance Risk

According to Nose & Mengistu, (2023) the likelihood of taxpayers failing to meet their statutory obligations with respect to registration, filing, accurate reporting and payment is known as Tax compliance risk. Betts, (2022) & Onyiah et al., (2026) stated that compliance-risk management comprises of identifying, assessing, prioritizing and addressing these risks and its mitigations. Betts, (2022) stated that as a result of poor knowledge, technological errors and administrative difficulties, taxpayers intentionally evade or underreport tax returns.

2.1.5 Interconnectedness of Cyber-security, Operational and Tax Compliance Risks

According to Betts (2025) the relationship existing among cyber-security, operational and tax compliance risks explains how vulnerabilities in one area may cause problems in the others. Cyber incidents affect the integrity and confidentiality of tax records. Distortion or manipulation of Data corrupts mandatory audit trails, while breaches of sensitive employee or client tax identifiers expose firms to data privacy fines and mandatory breach notifications to tax authorities. Aslett et al. (2024) stated that for this reason, tax authorities require reliable systems for collecting, storing, analyzing, exchanging and securing information. Cyber-security risk threatens digital systems and information while operational risk leads to failures in people, processes and

technology while tax compliance risk relates to taxpayers' possible failure to fulfill statutory obligations hence the need to manage cyber-security risks as part of broader organizational risk management (BCBS, 2021 & Pascoe et al., 2024).

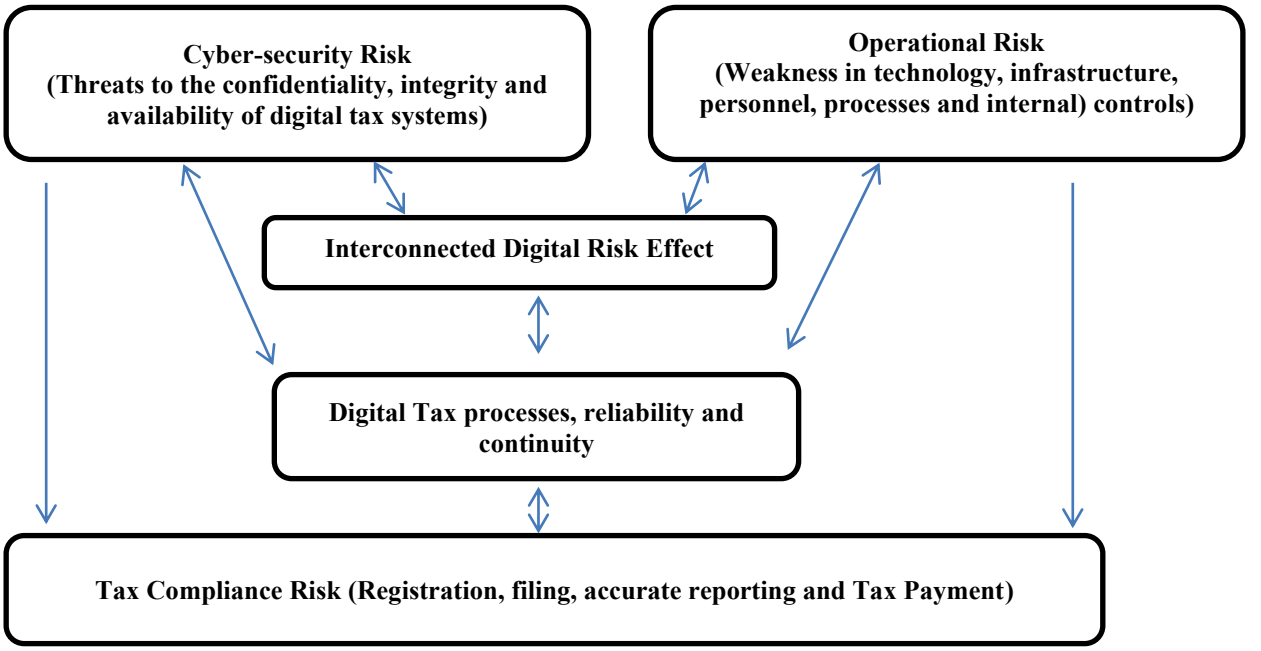

Fig 1. The Interconnected Digital Tax Risk Framework (IDTRF)

This study introduces the Interconnected Digital Tax Risk Framework (IDTRF) to link Cyber-security, operational risk, and tax compliance risk within Nigeria's digital tax system. Digital tax success relies less on portal availability and more on the security, stability, and continuity of the underlying technology and workflows. Cyber-security and operational risks serve as the two primary exposure points. Cyber-security involves threats that compromise the safety, privacy, and access to taxpayer data and systems. Operational risk stems from failures in hardware, systems, staffing, workflows, and internal controls. While distinct, these risks frequently compound one another. Cyber-security failures directly impair compliance; data breaches, hacks, or stolen records weaken the state's capacity to track and enforce tax laws. Simultaneously, operational failures such as network downtime, server crashes, or faulty processing block taxpayers from registering, filing forms, reporting earnings, or paying on time. Reliable tax systems help because digital tools must work well and stay online so taxpayers can file on time and keep good records while outages cause trouble because when systems crash, people struggle to pay taxes and the government finds it harder to monitor them.

2.2 Theoretical Review

This study is anchored on Socio-Technical Systems (STS) Theory and the Compliance Risk Management (CRM) Framework.

2.2.1 Socio-Technical Systems Theory

Research from the Tavistock Institute established that organizational success stems from balancing social elements (such as employees and operational workflows) with technical elements (such as tools and software) (Trist & Bamforth, 1951; Fox, 1995). In the context of modern tax administration, this means digital infrastructure like e-filing portals and databases must work seamlessly with the people who operate and use them. If staff lack proper training or security habits, the entire digital tax network risks downtime, security breaches, or inaccurate records.

2.2.2 Compliance Risk Management Framework

The OECD (2004) outlines its Compliance Risk Management Framework as a structured method to spot, evaluate, rank, and handle tax compliance threats**.** According to this framework, tax agencies must carry out ongoing evaluations and apply targeted solutions to manage these risks effectively in order to improve taxpayer registration, filing, and reporting and payment compliance. This enables tax administrations in recognizing threats to the tax base and allocates resources towards managing those threats (Betts, 2022). The framework covers four principal taxpayer obligations: registration, filing, accurate reporting and payment. Since non-compliance may arise at any of these stages, tax authorities must identify and manage the associated risks (Betts, 2022).

Relevance to the study: STS Theory explains the relationship between people, technology and organizational processes and the CRM Framework establishes the principal dimensions of tax compliance risk. Together, these perspectives support the examination of cyber-security and operational risks and their implications for tax compliance in Nigeria.

2.3 Empirical Review

2.3.1 Cybersecurity Risk and Tax Compliance Risk

Aniyikaye et al. (2025) looked at how cyber threats affect public auditing across federal finance and accounts departments in Nigeria, employing a descriptive survey of purposively chosen staff to assess risk management and digital oversight. Their findings pointed to a constructive link between solid risk frameworks and modern technopublic auditing, underscoring the role of risk mitigation in digital governance—though the paper bypassed direct analysis of tax compliance hazards.

Meanwhile, Inuwa et al. (2020) investigated vulnerabilities in Nigerian public-sector information systems that leave room for corruption. Through qualitative methods like interviews, focus groups, and archival reviews, they identified structural and organizational gaps enabling tech misuse, concluding that software safeguards cannot guarantee accountability in the face of flawed internal controls and human error, despite not tracking cybersecurity or tax compliance specifically. Bridging corporate behavior and digital security, Le et al. (2024) noted that businesses with stronger pre-existing IT and cybersecurity outlays absorbed the blow more effectively. Even though their focus rested on private enterprises rather than government tax agencies, the work illustrates how digital breaches spill over into tax-related outcomes.

2.3.2 Operational Risk and the Reliability and Continuity of Digital Tax Processes

Adegbie, Enerson, and Olaoye (2022) analyzed e-tax systems and revenue collection in southwestern Nigeria. Their survey and regression analysis showed that mobile payments, online billing, and user-friendly designs simplified tax filing. They noted that simpler portals and trained staff boost revenue efficiency, though they did not track system downtime.

Salawu et al. (2024) & Baer et al. (2025) explored e-filing and SME tax compliance in Lagos State. Using survey data and logistic regression, they discovered that user awareness, ease of use, and expected performance drove compliance. They highlighted platform usability as a key factor, without testing technical outages. They found that stronger tax administration narrowed VAT compliance gaps

2.3.3 Digital Tax Administration and Tax Compliance Outcomes

Nose and Mengistu (2023) noted that digital tools can boost tax collection, though results depend on the specific technology and local administration. They warn that digitalization does not guarantee equal gains across all settings.

Falana, Dakhil, Abbood, and Dagunduro (2024) studied digital tax administration among 547 informal-sector operators across the six southwestern states of Nigeria. Using survey, correlation and regression analyses, they found that technical know-how and digital payment platforms significantly improved tax compliance. Their findings highlighted the importance of users' capabilities and access to digital payment facilities.

Araoye, Oladejo, and Adesokan (2024), Inegbedion (2025) & Mbobo, Mbobo, and Obodoechi (2026) examined digital tax administration and tax compliance behaviour under the Nigeria Tax Act 2025. Using survey data and structural equation modeling, they reported positive relationships between digital tax administration and compliance behaviour. Perceived usefulness, ease of use and taxpayer trust were also positively associated with compliance. However, these studies examined tax compliance behaviour generally rather than cybersecurity and operational risks.

Otekunrin et al. (2021) & Uguagu, Asomba, and Kalu, (2023) examined the effectiveness of electronic tax systems in reducing tax evasion in Nigeria. The study considered how electronic processes could support tax administration and the reduction of evasion. Its focus is relevant to the potential contribution of digital systems to record keeping and compliance monitoring, but it does not directly establish the effects of cybersecurity and operational risks.

2.3.4 Joint Influence of Cybersecurity Risk and Operational Risk on Tax Compliance Risk

Few studies, looked at how cyber-security and operational risks together affect tax compliance risk.

Inuwa et al. (2020) showed that employee and system misuse in Nigeria's public sector stems from weak controls, poor oversight, and flawed human behavior rather than just technical failure while Baer et al. (2025) & Le et al. (2024) observed that firms hit by cyber-attacks grew more aggressive with their taxes,

partly due to financial strain. Though these results do not automatically apply to Nigerian tax agencies and tax compliance directly, they show a link between digital breaches and tax habits.

2.3.4 Summary of Empirical Review and Research Gap

The reviewed literature offers three main insights. First, insight: Nigerian research links cybersecurity governance, internal controls, and system integrity to public-sector accountability (Aniyikaye et al., 2025; Inuwa et al., 2020). Second insight: Electronic tax filing studies show that usability, technical skills, taxpayer awareness, and administrative efficiency drive tax outcomes (Adegbie et al., 2022; Salawu et al., 2024). Third insight: international research links cyber incidents to tax-related behaviour and stronger tax administration performance to smaller compliance gaps (Baer et al., 2025; Le et al., 2024).

Three gaps remain. Contextual gap**:** Few Nigerian studies directly link cyber-security risk to tax compliance risk in digital tax systems. Variable gap**:** Past research focused on tech adoption, filing, or revenue collection rather than operational risk and service continuity. Methodological gap**:** No prior study tests the combined statistical effect of cyber-security and operational risks on tax compliance risk in Nigeria. The study addresses these gaps by examining the relationship between cyber-security and operational risks and their implications for tax compliance risk in digital tax administration in Nigeria.

Methodology

This quantitative study used a cross-sectional survey design in Enugu State, Nigeria. The target group of 1,200 individuals included Nigeria Revenue Service staff, Enugu State Internal Revenue Service staff, taxpayers, and tax consultants. Using Taro Yamane's formula at a 5% precision level, the sample size was set at 300 respondents chosen via purposive sampling for their tax expertise. Primary data came from a structured, five-point Likert-scale questionnaire. Method of data analysis used was inferential statistics such as Pearson's Correlation Analysis and Regression Analysis.

$$n = \frac{N}{1 + N(e)^2}$$

Where N= Population size, e = error margin which the researcher chose to be 5%. n= sample size.

$$\text{Thus } n = \frac{1{,}200}{1 + 1{,}200\ (0.05)^2} = 300 \text{ questionnaires approximately}$$

Of the 300 questionnaires administered, 250 were returned, representing a 83% response rate, while 50 were not returned. The returned questionnaires formed the basis of the analysis.

Model Specification

i. TCR = f(CSR)

Where: TCR = Tax Compliance Risk, CSR = Cybersecurity Risk

ii. $DTPRC = \beta 0 + \beta_1 OPR + \varepsilon$

Where: DTPRC = Digital Tax Process Reliability and Continuity, OPR = Operational Risk, $\beta 0$ = Constant term, β_1= Regression coefficient of operational risk, ε = Error term

iii. $TCR = \beta 0 + \beta_1 CSR + \beta_2 OPR + \varepsilon$

Where: TCR = Tax Compliance Risk, CSR = Cybersecurity Risk, OPR = Operational Risk, β_1 = Coefficient of Cybersecurity risk, β_2 = Coefficient of Operational Risk, ε = Error term.

4.1 Data Presentation

Table 4.1. Distribution of Respondents by Years of Experience in Tax-Related Activities

WORKING EXPERIENCE	**NUMBER**	**PERCENTAGE (%)**
Below 5 years	39	15.6
5- 9 years	26	10.4
10- 14 years	64	25.6
15- 19 years	54	21.6
20 years and above	67	26.8
TOTAL	250	100

Source: Field Survey 2026

Table 4.2. Distribution of Category of Respondent

DEPARTMENTS	**NUMBER**	**PERCENTAGE (%)**
Staff of Nigeria Revenue Service	72	28.8
Staff of Enugu State Internal Revenue Service	58	23.2
Taxpayer	90	36
Tax Consultant	30	12
TOTAL	250	100

Source: Field Survey 2026

Table 4.3. Distribution of Experience with Digital Tax Systems

WORKING EXPERIENCE	**NUMBER**	**PERCENTAGE (%)**
Below 3 years	47	18.8
3- 6 years	68	27.2
6- 9 years	79	31.6
9 years and above	56	22.4
TOTAL	250	100

Source: Field Survey 2026

Table 4.4. Distribution of Respondents by Department/Unit

Department/Unit	**NUMBER**	**PERCENTAGE (%)**
Tax Administration	66	26.4
Audit/Investigation	54	21.6
ICT/Information Technology	29	11.6
Taxpayer Services	39	15.6
Finance/Accounts	38	15.2
Legal/Compliance	24	9.6
TOTAL	250	100

Source: Field Survey 2026

Table 4.5. Questionnaire on Examining the Relationship Between Cyber-security Risk and Tax Compliance Risk in Digital Tax Administration in Nigeria

Obj 1	**Cyber-security Risk (CSR)**	**SA**	**A**	**UN**	**D**	**SD**
1	Digital tax platforms are exposed to unauthorized access to taxpayers' confidential information.	167	83	0	0	0
2	Cyber-attacks pose a significant threat to the security of taxpayer information held by tax authorities.	180	70	0	0	0
3	Digital tax records are vulnerable to manipulation, alteration or deletion by unauthorized persons.	130	120	0	0	0
4	Inadequate cyber-security controls expose digital tax platforms to data breaches and other security incidents.	173	77	0	0	0
	Tax Compliance Risk (TCR)	**SA**	**A**	**UN**	**D**	**SD**
5	Taxpayers face the risk of failing to register appropriately with the relevant tax authorities.	175	75	0	0	0
6	Taxpayers face the risk of failing to submit their tax returns within the prescribed period.	174	76	0	0	0
7	Inaccurate or incomplete disclosure of taxable income increases the risk of tax non-compliance.	166	59	5	13	17
8	Taxpayers face the risk of failing to pay their assessed taxes within the stipulated period.	172	78	0	0	0

Source: Field Survey 2026

Table 4.6. Questionnaire on Determining the Effect of Operational Risk on the Reliability and Continuity of Digital Tax Processes in Nigeria

Obj2	**Operational Risk (OPR)**	**SA**	**A**	**UN**	**D**	**SD**
1	Frequent downtime of digital tax platforms disrupts the delivery of tax administration services.	133	117	0	0	0
2	Technical failures in digital tax systems affect the accurate processing of tax transactions.	150	100	0	0	0
3	Inadequate ICT infrastructure exposes digital tax administration to operational disruptions.	181	69	0	0	0
4	Poor integration between digital tax platforms and other relevant information systems creates operational difficulties.	172	77	1	0	0
	Digital Tax Process Reliability and Continuity (DTPRC)	**SA**	**A**	**UN**	**D**	**SD**
5	Digital tax platforms are consistently available when taxpayers and tax administrators need to use them.	80	51	5	55	59
6	Digital tax transactions are processed accurately and without unnecessary delays.	83	58	4	55	50
7	Digital tax services can be restored promptly following technical disruptions.	100	70	5	40	35
8	Digital tax platforms maintain continuity of service during periods of operational difficulty.	30	49	0	71	100

Source: Field Survey 2026

4.2 Data Analysis and Interpretation

Table 4.7 Pearson Correlation Analysis of Cyber-security Risk and Tax Compliance Risk in Digital Tax Administration in Nigeria

		CSR	TCR
CSR	Pearson Correlation	1	.968**
	Sig. (2-tailed)		.000
	N	20	20
TCR	Pearson Correlation	.968**	1
	Sig. (2-tailed)	.000	
	N	20	20

**. Correlation is significant at the 0.01 level (2-tailed).
Source: SPSS, 2026

Table 4.7 presents the Pearson correlation between Cybersecurity Risk (CSR) and Tax Compliance Risk (TCR). The result shows a correlation coefficient of 0.968, a p-value < 0.001 and 20 observations. The coefficient indicates an exceptionally strong positive relationship between the two variables. This suggests that higher cyber-security risk is associated with greater tax compliance risk, while improved cyber-security may correspond with reduced compliance risk. The statistically significant result provides evidence of a strong association between cyber-security vulnerabilities and tax compliance challenges in digital tax administration in Nigeria. Specifically, unauthorized access, cyberattacks, data breaches and manipulation of taxpayer records may compromise information integrity, weaken compliance monitoring and increase the likelihood of taxpayers failing to meet their statutory obligations.

Table 4.8 Model Summary of Operational Risk on the Reliability and Continuity Of Digital Tax Processes in Nigeria

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics					Durbin-Watson
					R Square Change	F Change	df1	df2	Sig. F Change	
1	.430[a]	.185	.139	28.08865	.185	4.077	1	18	.059	1.162

a. Predictors: (Constant), OPR
b. Dependent Variable: DTPRC
Source: SPSS, 2026

Table 4.8 reveals a **moderate positive link (R = 0.430\)) between operational risk and digital tax process reliability and continuity**. Operational risk explains 18.5% of the variance (R square = 0.185), or 13.9% after adjusting for sample size and predictors. Outside model external factors account for the remaining 81.5%. The model carries a standard error of 28.08865, and a Durbin–Watson score of 1.162 suggests potential positive residual autocorrelation.

Table 4.9 Coefficients of Operational Risk on the Reliability and Continuity Of Digital Tax Processes in Nigeria

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Correlations		
		B	Std. Error	Beta			Zero-order	Partial	Part
1	(Constant)	40.381	7.883		5.123	.000			
	OPR	.192	.095	.430	2.019	.059	.430	.430	.430

a. Dependent Variable: DTPRC
Source: SPSS, 2026

In table 4.9, the regression coefficient for operational risk is positive (B = 0.192), with a standardized beta coefficient of 0.430, t-statistic of 2.019 and p-value of 0.059. The positive coefficient suggests that a one-unit increase in the operational risk score is associated with a 0.192-unit increase in the digital tax process reliability and continuity score, holding other factors constant. However, this relationship is not statistically significant at the 5% level. The estimated regression equation is: [DTPRC=40.381+0.192(OPR)]. The constant of 40.381

represents the predicted value of digital tax process reliability and continuity when the operational risk score is zero.

Table 4.10 Model Summary of joint influence of Cyber-security Risk and Operational Risk On Tax Compliance Risk in Digital Tax Administration in Nigeria

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics					Durbin-Watson
					R Square Change	F Change	df1	df2	Sig. F Change	
1	.981[a]	.963	.959	13.84807	.963	222.207	2	17	.000	1.278

a. Predictors: (Constant), OPR, CSR
b. Dependent Variable: TCR
Source: SPSS, 2026

The model summary of Table 4.10 indicates a multiple correlation coefficient (R) of 0.981. This represents a very strong positive relationship between the combined independent variables—cybersecurity risk and operational risk—and tax compliance risk. The coefficient of determination (R^2) is 0.963, indicating that cybersecurity risk and operational risk jointly explain 96.3% of the variation in tax compliance risk. The remaining 3.7% may be explained by other factors not included in the model. The adjusted R^2 of 0.959 indicates that the model explains approximately 95.9% of the variation in tax compliance risk after adjustment for the number of predictors and observations. This suggests a very high explanatory power. The standard error of the estimate is 13.84807, representing the average variation between the observed values of tax compliance risk and those predicted by the regression model. The Durbin–Watson statistic of 1.278 is also reported.

Table 4.11 Coefficients of joint influence of Cyber-security Risk and Operational Risk On Tax Compliance Risk in Digital Tax Administration in Nigeria

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Correlations		
		B	Std. Error	Beta			Zero-order	Partial	Part
1	(Constant)	.645	3.897		.166	.870			
	CSR	.488	.145	.490	3.372	.004	.968	.633	.157
	OPR	.510	.146	.505	3.479	.003	.969	.645	.162

a. Dependent Variable: TCR
Source: SPSS, 2026

Table 4.11 presents the individual effects of Cyber-security and operational risks on tax compliance risk when both variables are included in the model. Cyber-security Risk (CSR): (β = 0.490) (t = 3.372), (p = 0.004). CSR significantly and positively drives tax compliance risk (unstandardized β = 0.488). A one-unit rise in CSR increases tax compliance risk by (0.488) units, holding operational risk constant. Operational Risk (OPR): (β = 0.505) (t = 3.479), (p = 0.003). OPR has a significant positive effect on tax compliance risk (unstandardized β = 0.510). A one-unit rise in OPR increases tax compliance risk by (0.510) units, holding cyber-security risk constant. Comparatively, operational risk (β = 0.505) has a

slightly greater relative influence on tax compliance risk than cyber-security risk (β = 0.490).

4.2 Test of Hypotheses

Hypothesis One:

i. There is no significant relationship between Cyber-Security Risk and Tax Compliance Risk in Digital Tax Administration in Nigeria.
ii. There is a significant relationship between Cyber-Security Risk and Tax Compliance Risk in Digital Tax Administration in Nigeria.

Decision Rule: Reject the null hypothesis if the p-value is less than 0.05. Do not reject the null hypothesis if the p-value is greater than 0.05. Based on table 4.7 Pearson Correlation result and since the probability value of $p < 0.001 < 0.05$, the null hypothesis was rejected. Consequently, the alternate hypothesis is accepted that there is a statistical significant relationship between Cyber-Security Risk and Tax Compliance Risk in Digital Tax Administration in Nigeria.

Hypothesis Two:

i. Operational risk has no significant effect on the reliability and continuity of digital tax processes in Nigeria.
ii. Operational risk has a significant effect on the reliability and continuity of digital tax processes in Nigeria.

Table 4.12 ANOVA of Hypothesis Two

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	3216.494	1	3216.494	4.077	.059[b]
	Residual	14201.506	18	788.973		
	Total	17418.000	19			

a. Dependent Variable: DTPRC
b. Predictors: (Constant), OPR
Source: SPSS, 2026

The ANOVA table shows an F-statistic of 4.077 and a significance probability of 0.059. **Decision rule:** The decision rule states that the null hypothesis should be rejected where the p-value is less than 0.05; otherwise, it should not be rejected. Since the p-value of 0.059 exceeds the 5% significance level, the null hypothesis is not rejected. Consequently, the study concludes that operational risk does not have a statistically significant effect on the reliability and continuity of digital tax processes in Nigeria.

Hypothesis Three

i. Cyber-security Risk and Operational Risk do not have a significant joint influence on tax compliance risk in digital tax administration in Nigeria.
ii. Cyber-security Risk and Operational Risk have a significant joint influence on tax compliance risk in digital tax administration in Nigeria.

Table 4.13 ANOVA of Hypothesis Three

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	85224.926	2	42612.463	222.207	.000[b]
	Residual	3260.074	17	191.769		
	Total	88485.000	19			

a. Dependent Variable: TCR
b. Predictors: (Constant), OPR, CSR
Source: SPSS, 2026

The ANOVA result of table 4.13, reports an F-statistic of 222.207, with degrees of freedom of 2 and 17, and a significance value of 0.000 ($p < 0.001 < 0.05$). Since the probability value is below the 5% significance level (0.05), the null hypothesis is rejected. Consequently, the study establishes that Cyber-security Risk and Operational Risk jointly have a statistically significant influence on tax compliance risk in digital tax administration in Nigeria.

4.3 Results and Discussion

4.3.1 Cyber-security Risk and Tax Compliance Risk in Digital Tax Administration in Nigeria

The findings indicate a very strong, positive and statistically significant relationship between cyber-security risk and tax compliance risk in digital tax administration in Nigeria ($r = 0.968$, $p < 0.001$). **Cyber-security weaknesses expose taxpayers and digital platforms to greater tax compliance risks**. These vulnerabilities weaken tax administration and lower compliance rates. This aligns with Sanni (2025), who found that phishing, ransomware, identity theft, and data breaches erode public trust in digital systems. Consequently, higher cyber-security threats directly drive up tax compliance risks.

4.3.2 Operational Risk and the Reliability and Continuity of Digital Tax Processes in Nigeria.

The result indicates that operational risk has a positive but statistically insignificant effect on the reliability and continuity of digital tax processes in Nigeria ($\beta = 0.430$, $p = 0.059$). Mitigating factors include Support teams, backups, and recovery plans prevent immediate service breakdowns. Underlying issues: Weaknesses still erode overall efficiency and service delivery. Prior research: Mas'ud, Mohammed, and Gimba (2023) noted that state revenue services require better integration, automation, and analytics.

4.3.3 Cyber-Security Risk and Operational Risk on Tax Compliance Risk in Digital Tax Administration in Nigeria

Cyber-security and operational risks significantly increase tax compliance risk in Nigeria. The model accounts for 96.3% of this variation, showing that weak security and poor operations heighten exposure. This supports Gambo and Onuorah (2025), who found that fragile digital infrastructure, low literacy, and cyber threats hinder e-taxation. They urged better security and tech investments to boost revenue. This study builds on their work by proving the joint impact of both risks. In addition, Aslett et al. (2024) emphasized accurate taxpayer data,

risk profiling, and targeted audits to control compliance risks. This supports the present finding, as cyber-security breaches and operational failures can compromise taxpayer information and weaken compliance monitoring.

5.0 Summary of Findings, Conclusions and Recommendation

5.1 Summary of Findings

i. Cyber-security Risk has a strong, positive and statistical significant relationship with Tax Compliance Risk in Digital Tax Administration in Nigeria.
ii. Operational Risk has a positive but no statistical significant effect on the reliability and continuity of digital tax processes in Nigeria.
iii. Cyber-security Risk and Operational Risk jointly have a statistically significant positive influence on tax compliance risk in digital tax administration in Nigeria.

5.2 Conclusions

i. The study concludes that inadequate protection of taxpayer information and digital tax platforms can undermine the benefits of digital tax administration. Cyber-security should therefore be an essential part of tax administration and compliance risk management.
ii. The study concludes that operational risk are influenced by factors such as infrastructure quality, system maintenance, staff competence and technical support. Its importance should not be overlooked despite its statistically insignificant effect on digital tax process reliability and continuity.
iii. The study concludes that effective digital tax administration requires coordinated cyber-security protection and operational risk management. Weaknesses in these areas can compromise taxpayer records, disrupt tax transactions, weaken compliance monitoring and hinder the enforcement of tax obligations.

5.3 Recommendations:

i. The Nigeria Revenue Service and State Internal Revenue Services need to boost digital tax security. They should use encryption, firewalls, multi-factor authentication, and intrusion detection, alongside regular audits and vulnerability tests to fix system flaws.
ii. Tax agencies must build reliable backup and recovery plans. They should also set up alternative service options, train staff, and provide strong technical support to keep digital tax systems running smoothly.
iii. Tax authorities should create a combined risk-tracking system. This tool will monitor cyber and operational threats together covering taxpayer registration, filing, reporting, and payments to spot risks early and improve compliance.

Statements and Declarations

All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by [Dr. Ifeanyichukwu Arthur Onyiah], [Dr. Joy Dakoru Uche], [Dr. Henry Idoko Uche]. [Ugezu, Marymartina Eberechukwu] and [Henry Ejikeme Udeh]. The first draft of the manuscript was

written by [Dr. Ifeanyichukwu Arthur Onyiah] and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

Competing Interests

- The authors did not receive support from any organization for the submitted work.
- No funding was received to assist with the preparation of this manuscript.
- No funding was received for conducting this study.
- No funds, grants, or other support was received.

References

Adegbie, F. F., Enerson, J., & Olaoye, S. A. (2022). An Empirical Investigation into the relationship between Electronic Tax Management System and Tax Revenue Collection Efficiency in selected states in South West, Nigeria. *Archives of Business Research, Volume 10, issue (4), 93–109. https://doi.org/10.14738/abr.104.12195*

Aniyikaye, S. O., Apalowowa, O. D., & Ayoko, O. (2025). Cybersecurity challenges and Technopublic Auditing: Safeguarding digital accountability mechanisms in the Nigerian public institutions. *Asian Journal of Economics, Finance and Management https://hal.science/hal-05301508*

Araoye, F. E., Oladejo, A. H., & Adesokan, J. A. (2024). Impact of Digital Tax Administration on Tax Misfeasance and Revenue in Southwestern State of Nigerian. *FUOYE Journal of Accounting and Management.*

Aslett, J., González, G., Hamilton, S., & Pecho, M. (2024). Tax administration: Essential analytics for Compliance Risk Management. *International Monetary Fund, Technical Notes and Manuals No. 2024/001. https://doi.org/10.5089/9798400260063.005*

Awodun, M., Somorin, O., & Sanni, A. (2024). Optimizing Tax Administration in Nigeria through Digital Transformation of a Harmonized Tax System. *Journal of Accounting and Taxation, 16(4), 217–225. https://doi.org/10.5897/JAT2024.0625*.

Baer, K., Barra, P. A., & Benitez, J. C. (2025). Closing the Gap: How Tax Administration Performance Shapes Compliance *(IMF Working Paper No. 2025/209). International Monetary Fund. https://doi.org/10.5089/9798229027076.001.A001*

Basel Committee on Banking Supervision. (2021). Revisions to the Principles for the Sound Management of Operational Risk. *Bank for International Settlements. https://www.bis.org/bcbs/publ/d515.htm*

Betts, S. E., (2022). Revenue Administration: Compliance Risk Management: Overarching Framework to Drive Revenue Performance. *Published by International Monetary Fund Technical Notes and Manuals 2022/005, Volume 2022: Issue 005, , DOI: https://doi.org/10.5089/9798400215216.005*

Betts, S., Annette C., Philip F., and Pierre K., (2025). "How to Use the Assessment Tool of the IMF Framework for International Tax Administration Strengthening. IMF How to Note 2025/008, International Monetary Fund, Washington, DC. *https://www.imf.org/-/media/files/publications/howtonotes/2025/english/htnea2025008.pdf*

Egbara, E. A., Asomba, I. U., & Ofodu, H. I. (2023). Electronic Taxation and Improved Tax compliance: The case of Tax Evasion and Avoidance in Enugu State, Nigeria. *International Journal of Accounting Research, 8(2), 59–63. https://doi.org/10.65453/ijar.v8i2.1196*

Falana, G. A., Dakhil, M. S., Abbood, F. G., & Dagunduro, M. E. (2024). Digital Tax Administration and Tax Compliance in Nigerian informal sector. *Economy, Business and Development: An International (EB&D) Journal, 5(2), 32–45. https://doi.org/10.47063/EBD.00020*.

Federal Republic of Nigeria. (2021). National Cybersecurity Policy and Strategy. *Https://Cert.Gov.Ng/Ngcert/Resources/National_Cybersecurity_Policy_And_Strategy_2021.Pdf*

Federal Republic of Nigeria. (2023). Nigeria Data Protection Act, 2023. Nigeria Data Protection Commission. *https://ndpc.gov.ng/download/nigeria-data-protection-act-2023*

Fox, W. M. (1995). Sociotechnical System Principles and Guidelines: Past and Present. The *Journal of Applied Behavioral Science, 31(1), 91–105. https://doi.org/10.1177/0021886395311009*

Gambo, J. S., & Onuorah, L. O. (2025). Impact of Electronic Taxation on Revenue Generation in Nigeria: Perspective from Federal Inland Revenue Services. *Journal of the Management Sciences, 62(2), 118–136. https://journals.unizik.edu.ng/jfms/article/view/7287*

Inegbedion, H. E. (2025). Acceptance of Electronic Tax System And The Contribution of SMES to Tax Revenue Through The Mediation Of Tax Compliance. *Journal of Innovation and Entrepreneurship, 14, 129. https://doi.org/10.1186/s13731-025-00582-w*.

International Monetary Fund (IMF). (2022). Betts, S. E. Revenue administration: Compliance Risk Management: Overarching Framework to Drive Revenue Performance. *IMF Technical Notes and Manuals, 2022(005). https://doi.org/10.5089/9798400215216.005*

International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC). (2022). Information security, Cybersecurity and Privacy Protection— Guidance on managing information security risks (4th ed.). *ISO/IEC 27005 ISO. https://www.iso.org/standard/80585.html*

Inuwa, I., Ononiwu, C., & Kah, M. M. O. (2020). Dimensions that Characterize and Mechanisms that Cause the Misuse of information systems for Corrupt Practices in the Nigerian public sector. *The Electronic Journal of Information Systems in Developing Countries, 86(6), Article e12136. https://doi.org/10.1002/isd2.12136*

Le, A.-T., Huang, H., & Do, T. K. (2024). Navigating through Cyberattacks: The Role of Tax Aggressiveness. *Journal of Corporate Finance, 88, Article 102649. https://doi.org/10.1016/j.jcorpfin.2024.102649*

Mas'ud, A., Mohammed, S. D., & Gimba, Y. A. (2023). Digitalisation and Subnational Tax Administration in Nigeria (African Tax Administration Paper 29). *International Centre for Tax and Development. https://doi.org/10.19088/ICTD.2023.031*

Mbobo, M. E., Mbobo, E. U., & Obodoechi, E. U. (2026). Digital tax administration and tax compliance behaviour: An evaluation of the Nigeria Tax Act 2025. *Advance Journal of Management, Accounting and Finance*.

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

Nigeria Data Protection Act, 2023. Nigeria Data Protection Commission: Resources.

Nose, M., & Mengistu, A. (2023). *Exploring the Adoption of Selected Digital Technologies in Tax Administration: A Cross-Country Perspective. IMF Notes, 2023/008. https://doi.org/10.5089/9798400258183.068.*

Obiora, F., & David, S. (2021). Effect of adoption of TaxPro-Max on FIRS Tax Remittance in *Nigeria. International Journal of Trend in Scientific Research and Development, 6(1), 1348–1355.* *https://www.ijtsrd.com/papers/ijtsrd48006.pdf*

Ogbaisi, S. A., & Ibifunmilola, M. (2025). Digitalization of Tax Systems and Tax Reforms in Nigeria: A Conceptual Discourse. *Malete Journal of Accounting and Finance, Vol 5(2).*

Oludi, S. A. (2026). Advancing Taxation in Nigeria through Artificial Intelligence: Challenges and Framework for Adoption. *BW Academic Journal, Vol. 2 (2025): 2025: Bushwealth Academic Journals*

Organisation for Economic Co-operation and Development. (2020). Tax administration: The Digital Transformation Of Tax Administration. OECD Publishing. https://doi.org/10.1787/ca274cc5-en

Organisation for Economic Co-operation and Development (OECD). (2004). Compliance risk Management: Managing and Improving Tax Compliance. *https://www.oecd.org/content/dam/oecd/en/topics/policy-issues/tax-administration/compliance-risk-management-managing-and-improving-tax-compliance.pdf*

Organisation for Economic Co-operation and Development (OECD). (2025). Tax Administration. *OECD Publishing. https://www.oecd.org/en/publications/tax-administration-2025_cc015ce8-en.html*

Organisation for Economic Co-operation and Development. (2025). Tax administration Digitalisation and Digital Transformation Initiatives. *OECD Publishing. https://doi.org/10.1787/c076d776-en*

Organisation for Economic Co-operation and Development. (2026). Digital Continuous Transactional Reporting for Value Added Tax: Policy and Design Considerations for Introduction and Operation. *OECD Publishing. https://doi.org/10.1787/34c88c39-en*

Oseni, M. (2016). Sustenance of Tax Administration by Information and Communications Technology in Nigeria. *Archives of Business Research, 4(1). https://doi.org/10.14738/abr.41.1734*

Otekunrin, A. O., Nwanji, T. I., Eluyela, D. F., Inegbedion, H., & Eleda, T. (2021). E-Tax System Effectiveness in Reducing Tax Evasion in Nigeria. Problems and Perspectives in Management, *Vol. 19 (4), 175–185. https://doi.org/10.21511/ppm.19(4).2021.15*

Pascoe, C., Quinn, S., & Scarfone, K. (2024). *The NIST Cybersecurity Framework (CSF) 2.0 (NIST Cybersecurity White Paper 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29*

Trist, E. L., & Bamforth, K. W. (1951). Some Social and Psychological Consequences of the Longwall Method of Coal-Getting: *An Examination of the Psychological Situation and Defences of a Work Group in Relation to the Social*

Structure and Technological Content of the Work System. Human Relations, 4(1), 3–38. https://doi.org/10.1177/001872675100400101

Salawu, M. K., Adigun, O. A., Lawal, Q. A., & Olaleye, J. A. (2025). Electronic Tax Filing System and Compliance among Small and Medium-Sized Enterprises in Lagos State, Nigeria. International Journal of Economics and Financial Issues, 15(1), 32–41. https://doi.org/10.32479/ijefi.17309

Sanni, O. (2025). Taxpayer data protection: The Cybersecurity Imperative. *World Journal of Advanced Research and Reviews, Vol. 28(2), 1107–1117. https://doi.org/10.30574/wjarr.2025.28.2.3833*

Uguagu, N. G., Asomba, I. U., & Kalu, I. O. (2023). E-taxation and Tax Compliance in Nigeria: Periscoping Change Perspectives. *Journal of Social Development, 12(1), 29–42. https://doi.org/10.4314/ngjsd.v12i1.3*