Volume: 9 Issues: 66 [September, 2024] pp. 845 – 853
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096670

EMPIRICAL STUDY ON THE IMPORTANCE OF INFORMATION TECHNOLOGY SECURITY AUDITS OF NIGERIA'S COMMERCIAL BANKS' EMERGING TECHNOLOGIES

Adeolu Abiodun Adebisi [1]
Akin Adebisi [2]
Lere Amusan [3]
Kayode Adesemowo [4]

[1] Regenesys Business School, Business Management, Johannesburg, South Africa, (Email: adeolubisi@hotmail.com)
[2] Department of Economics, School of Postgraduate Studies, Babcock University, Ilisan Remo, Ogun State, Nigeria, (Email: Adebisi0296@pg.babcock.edu.ng)
[3] Department of Political Science and International Relations, College of Management, and Social Science, Bowen University, Iwo, Nigeria, (Email: lere.amusan@bowen.edu.ng)
[4] Soams Consulting Plc. Managing Consultant, (Email: Kadesemowo@soams.co.za)

Article history
Received date : 15-8-2024
Revised date : 16-8-2024
Accepted date : 7-9-2024
Published date : 15-10-2024

To cite this document:
Adebisi, A. A., Adebisi, A., Amusan, L., & Adesemowo, K. (2024). Empirical study on the importance of information technology security audits of Nigeria's Commercial Banks' emerging technologies. *Journal of Islamic, Social, Economics and Development (JISED),* 9 (66), 845 – 853.

Abstract: *In Nigeria today, modern information technologies have revolutionized Nigerian commercial banks and the financial sector by swiftly embracing cutting-edge technology like artificial intelligence, the Internet of Things (IoT), blockchain, and cloud computing. Although sophisticated and emerging technologies provide several advantages, they also bring forth new and intricate security weaknesses that entail inherent risks. This study investigates the methodical process of examining the information technology security audits of emerging technologies in commercial banking institutions in Nigeria. This work used the systematic literature review (SLR) as the methodology. The pertinent documents were collected and meticulously inspected, including vital data on the importance of information technology security audits in the Nigerian commercial banking sector. This article emphasizes the importance of information technology security audits in reducing these risks and protecting Nigerian commercial banks. The objective of this work is to improve the implementation of strong cybersecurity measures in commercial banks in Nigeria. This will be achieved by evaluating the existing level of integration of emerging technologies, identifying any weaknesses, and developing a detailed approach for performing information technology security audits. The findings indicate that the lack of advancement in the banking industry may be ascribed to deficiencies in internal control systems, poor information technology governance, and inadequate audits of the emerging technologies used by Nigerian commercial banks.*

Keywords: *Artificial-Intelligence, IoT, Blockchain, Machine-Language, Audits, Security, and Risk.*

Volume: 9 Issues: 66 [September, 2024] pp. 845 – 853
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096670

Introduction

The emerging technologies in Nigeria's commercial banks are transforming the banking industry, with a substantial influence on consumer contentment. According to a study conducted by (Okoye *et al.*, 2018), electronic-based banking in Nigeria has improved customer satisfaction and has had a beneficial effect on several aspects of banking services. The digitalization of financial services has revolutionized user experience through internet banking, smartphone apps, and instant transactions. The effects of adopting information technology on the efficiency, client connections, and profitability of banks for the delivery of good services (Adebisi, Salamntu and Paschal, 2024). This swift adoption of emerging information technologies is to meet the need for banked and unbanked citizens in Nigeria, mostly where the physical structure of the banks cannot be erected. This has also opened up new opportunities for cybercrime, with hackers and advanced groups exploiting system weaknesses for illicit entry and fraudulent activities (Hassan *et al.*, 2024).

In recent times, nearly all the commercial banks in Nigeria have adopted modern Information technology (emerging technologies) such as blockchain, Artificial Intelligence, cloud computing, and the Internet of Things (IoT), etc, for efficient banking services delivery. There is a need for good Information Security control that is aligned with Nigerian commercial bank's governance. With the growing integration of information technology in the Nigerian financial industry, there is a pressing need to protect against common online scams like Advance Fee Fraud, also known as 419 as registered in Nigeria's criminal code of practice.

In addition, the general aims to identify barriers to the use of technology and provide solutions, which is crucial for researchers who want to comprehend the significance of information technology (IT) in the Nigerian banking sectors (Monisola *et al.*, 2024). The importance of this article is to examine the information technology security audit systems and IT audit systems in the commercial banking sector, particularly to the emerging technologies adopted and implemented by these commercial banks in Nigeria. According to (Hatsu, Ujapka and Mpimwood, 2015), the implementation of information security is crucial for commercial banks to safeguard the various information and/or data used by the commercial bank either in transit or stored in their infrastructures for performing daily financial activities minimizing business risks, and optimizing returns on investments and commercial opportunities. This is especially pertinent in the banking sector, where the menace of cyber fraud and hacking poses significant threats to the organization's data and information systems (Fatoki, 2023).

Furthermore, the internal control system and quality information technology security audit play crucial roles in the Nigerian commercial banking sector, as weaknesses in these areas have been reported (Shamsudeen, Shagari and Rafeah, 2018) to contribute to the backward development of commercial banking services in Nigeria.

Many researchers have shown that the quality of information technology security audit work and good bank operations are highly impacted by an efficient information technology control system implemented in IT infrastructures used by commercial banks. Stressing the need to implement it in all commercial banking establishments in Nigeria is crucial for modern banking systems (Nnachi *et al.*, 2020). Problems such as macroeconomic instability, corruption, and fraud risk are common, and with inherent control in place, they are very rampant in Nigeria's commercial banking sector. As a result, information security control systems are critical to the smooth operation of the commercial banking business, the provision of high-quality services, and the handling of fraud cases (Ikenna, 2024).

Volume: 9 Issues: 66 [September, 2024] pp. 845 – 853
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096670

Background

The deficiencies in the adopted and mostly designed internal control systems, governance, and inadequate IT audit work as factors contributing to the regressive growth in Nigeria's commercial banking industry (Enofe *et al.*, 2013) have been identified by the Central Bank of Nigeria (CBN). The significance of Information Technology security audits in Nigeria's commercial banks, as they embrace emerging technology, is motivated by the historical background and the logic derived from the issues encountered by the commercial banking industry in Nigeria.

The urgent need to address the vulnerabilities that exist within the commercial banks' internal control systems and IT audit work in the Nigerian commercial banking sector is the driving force for this study's focus on the emerging technologies used by Nigeria's commercial banks. The Central Bank of Nigeria (CBN) has brought attention to the detrimental impact that weakness in internal control systems, governance, and poor IT audit work have on the financial stability of Nigerian commercial banks. According to (Okoye and Ezejiofor, 2013), the number of reported cases of attempted fraud and forgery has surpassed previous records. Consequently, this highlights the critical need for efficient internal control measures to be implemented to reduce the likelihood of fraudulent activities and to ensure that the commercial banking sector in Nigeria maintains its integrity (Ikenna, 2024).

Furthermore, the increase in fraud and forgeries within commercial banking institutions has been attributed to internal control weaknesses and governance ineptitude, as has been demonstrated by the annual reports of the CBN and the Nigerian Deposit Insurance Corporation (Olaniyi, Olaoye and Okunleye, 2023). This is evidenced by the fact that the annual reports of both organizations have been compiled. According to Victory, Promise, and Mike (2022), these results highlight the crucial necessity for the function of IT security audits to have solid internal control systems and experienced cybersecurity analysts to IT control deficiency and fraud in the commercial banking sector.

The purpose of this study is to respond to those issues by investigating the mentality, capability, and level of expertise of professional information technology security audits in the process of deploying resources for fraud detection and prevention. The findings of this work would be of use to commercial banks in Nigeria, allowing them to improve their overall security posture. This study is to investigate the attitude, capabilities, and competencies of IT security auditors in terms of efficiently deploying resources for fraud detection & prevention initiatives, and enhancing the commercial banks in Nigeria to be able to improve their overall security posture that will lead to improvement of services.

Objective of the study

This study aims to assess the relevance of information technology security audits in Nigerian commercial banks' acceptance of emerging technologies. This work will investigate the challenges of security system audits and IT audit systems as well as their consequences on system deployment and information security. Given the rising prevalence of cybercrime, the results of the study fit the theory that more strict control and proactive assessments of fraudulent risks are desperately needed. This work aims to raise knowledge of the importance of information technology security audits for Nigerian commercial banking.

Volume: 9 Issues: 66 [September, 2024] pp. 845 – 853
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096670

Literature Review

A systematic literature review (SLR) is an academic method of evaluating relevant literature on a topic to derive a conclusion and answer a question under the research work (Mengist, Soromessa, and Legese, 2020). Various scholars have contributed significantly to highlighting the significance of information technology security audits for commercial banking in Nigeria via their research initiatives. The literature research on information technology security audits in the commercial banking sector demonstrates the importance of internal control mechanisms and quality IT audit work in guaranteeing financial institutions' integrity and stability

Enofe et al,.(2013) demonstrate the importance of efficient internal control in improving the quality of IT audit work in Nigerian commercial banks. Their findings pointed out the need for a solid internal control system, and good IT governance in combating fraud, which might pose a huge danger to the Nigeria economy

The study of Ojeka et al,.(2017) posits that Nigerian banks' audit committees lack the independence, IT governance, Control implementations, and technological competence necessary to successfully manage cybersecurity. The study finds a negative relationship between cyber security compliance in the Nigerian commercial banking sectors and audit committee characteristics such as independence, financial competence, and technological skills. However, the correlation is not statistically significant as stated. To increase cyber security monitoring, Nigeria's commercial banking sectors must employ people with technological and financial expertise while remaining independent.

Abiola (2014), the study examines how ICT affects Nigerian banks' internal control systems, particularly electronic fraud prevention, and detection. ICT has increased corporate transactions and marketing but decreased internet use. The report says exploring these sectors might attract foreign investment.

The study conducted by Adedokun and Oyewole (2013) examined the influence of monitoring and control measures on the identification of fraudulent activities in certain Nigerian commercial banks that were published. The research examined the relationship between monitoring and fraud detection, as well as the influence of control activities on fraud detection. Their research revealed that banks are notifying regulatory bodies about instances of fraud, nevertheless, the perpetrators of fraud are continuously improving their techniques, resulting in a rise in the number of fraud cases. Adherence to monitoring and control measures may thwart fraudulently conduct, but inadequate ethics training for bank personnel may be a factor in facilitating fraud.

Hassan et al.,(2024) study examines cybersecurity procedures in the banking sector, with a particular emphasis on Nigerian commercial banking institutions. The banking sector globally is increasingly concerned about cybersecurity due to the rising frequency and complexity of cyber-attacks. This report presents a comprehensive analysis of the worldwide state of cybersecurity in the banking sector, with a particular emphasis on the observed practices in Nigeria. The study provides a comprehensive overview of cybersecurity in the banking sector, focusing on Nigeria's unique methodologies, and emphasizing the importance of robust cybersecurity measures in safeguarding financial system integrity.

Samuel et al., (2022) work examines the significance of information technology and relevant controls deployed to the bank infrastructures and fraud risk assessment in commercial banks

Volume: 9 Issues: 66 [September, 2024] pp. 845 – 853
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096670

and financial institutions in Nigeria. Their research work investigates the problem of fraud in the Nigerian banking industry as well as financial institutions, specifically focusing on the evaluation of fraud risks associated with the use of information technology. The study places special emphasis on card-related fraud occurring in ATM and POS transactions.

Hatsu et al. (2015) stress the need for information security and IT audit systems in Ghanaian banks to secure data, maintain business operations, and maximize return on investment (ROI). This study shows the increased complexity of regulating data access and maintaining confidentiality correctness, and accessibility, especially in banking sector-connected networks. These studies further stress the need for strong internal control systems and thorough information Security System audits in Ghanaian commercial banks. With the rise of emerging technologies, this is vital to prevent fraud and enhance accounting information systems.

Methodology and Design

The systematic literature review (SLR) is the methodology used for this work, where many pieces of literature relevant to the topics were gathered, and evaluated to answer the question of investigating the attitude, capabilities, and competencies of IT security auditors in terms of efficiently deploying resources for fraud detection & prevention initiatives, and enhancing the commercial banks in Nigeria. A methodical strategy was used in this paper to analyze the information technology security audits that were performed on the emerging technologies utilized by Nigeria's commercial banks. The study approach includes a complete examination of some current accessible literature on Information Technology security audit, IT risk management methodologies, IT governance, Cybersecurity, internal control systems, and quality IT audit work in the Nigerian commercial banking business. To locate relevant content, a comprehensive search strategy was used. This search strategy included the utilization of academic databases, industry journals, and relevant organizational websites.

After a careful thorough empirical analysis of the data gathered from the selected studies, complete conclusions were drawn on the importance of Information technology security audits in light of Nigeria's commercial banks' emerging technological infrastructure capabilities. With the help of this methodology, it was possible to fully understand the state of information technology security audits in Nigeria's commercial banking sector and to draw insightful conclusions about how these audits might affect the commercial banks' risk management practices and overall performance.

Exclusion and Inclusion Data Criteria

To conduct empirical research on operational audit, internal audit control systems, quality audit work, and information technology security systems audit in Nigeria’s commercial banking business, this study used certain criteria to select and exclude data sources. To provide a comprehensive analysis of the relevance of IT security audits in the emerging technological landscape of Nigeria’s commercial banks, this technique was used to ensure that the data was both pertinent and correct. A SLR methodology that was both clear and methodical was intended to be provided by the empirical research analysis to facilitate data selection and analysis.

Search Criteria

To do the actual study of this work, the author carefully gathered relevant literature and data on commercial banks in Nigeria, emerging technologies, and IT security audits. The search looked through internet sources such as PubMed, Google Scholar, academia, and Scopus, as well as

Volume: 9 Issues: 66 [September, 2024] pp. 845 – 853
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096670

academic journals, conference proceedings, and unpublished material. Peer-reviewed publications, reports, and studies from different magazines were among the factors for admission. Information technology security audit systems, IT audit systems, and information systems in the business banking field were all part of the approach.

Data Analysis

The empirical study involves retrieving and examining data from carefully selected Nigerian commercial banks. The technique included gathering data, extracting information, and evaluating evidence to assess the effectiveness of monitoring and control activities in detecting fraud. It also evaluated the extent to which information technology audit security and IT audit systems were implemented(Adedokun and Oyewole, 2013). This research investigates the control activities and fraud detection systems used by selected banks. The text examines the impact of Information Technology security audit methods on safeguarding data integrity and mitigating business risk, as explored by (Hassan *et al.*, 2024) and (Hatsu, Ujapka and Mpimwood, 2015)

This research aimed to analyze the investigative methods used to get significant insights into the significance of Information Technology security audits about emerging technologies in commercial banks in Nigeria. This statement highlights the need to implement efficient monitoring, control procedures, and information security measures to identify fraudulent activity and safeguard data integrity.

Empirical Findings

The findings of this study shed light on the social repercussions that are associated with fraud within the Nigerian banking sector, revealing that it hurts the overall functioning of the business.

There are fraudulent activities in the Nigerian Commercial banking sector.

The results indicate that the presence of fraudulent activities in the banking sector not only hinders the performance of the business as a whole but also implicates institutions in facilitating such illegal actions. The conclusions of this research, which are based on empirical evidence, provide useful insights into the landscape of information technology security audits for emerging technologies used by commercial banks in Nigeria. Regarding the topic matter, the study takes into consideration the opinions and conclusions of the other authors, journals, and scholars that have contributed to the study. Added to this, the significance of this is to evaluate the significance of information technology security audits and IT audit systems, as well as the influence that these factors have on the overall performance of information security audits performed by commercial banks in Nigeria for emerging technologies.

Complexity of protecting the confidentiality, integrity, and availability of data in the Nigeria commercial banking sector

The finding revealed notable trends regarding the importance of Information Technology audit security in Nigerian commercial banks. In addition, the increasing complexity of overseeing access and protecting the confidentiality, integrity, and availability of data in the banking sector has made information security management crucial for ensuring ongoing banking operations and mitigating risks. The ever-increasing interconnectedness of networks has heightened the need to implement Information Technology security audits to prevent system failure and protect against dangers such as cyber fraud, vulnerabilities, and hacking. To be compliant with the triage of information security is very important which are confidentiality, Integrity, and

Volume: 9 Issues: 66 [September, 2024] pp. 845 – 853
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096670

availability. When these three serve as the watchwords and are well aligned with good internal controls, this will serve as a deterrent to criminals and cyber fraudsters. It is crucial for banks to have robust Information Technology security audit systems and IT audit systems, as emphasized by (Hassan *et al.*, 2024)(Hassan et al., 2024).

There are security flaws in the banking apps and other adopted technologies

The studies indicated that there were security flaws in the banking apps, Internet Banking, Mobile Banking, and Point of Sales (POS) terminals which highlighted the fact that mobile banking transactions are susceptible to security risks (Chen *et al.*, 2020; Adeolu Adebisi, 2024, p. iii). As a result of the exhaustive empirical review, inadequacies in the data management of banking applications were discovered, which brought to light the possibility of significantly reduced financial losses. According to the findings of the investigation, the applications that were kept by subsidiary banks demonstrated worse levels of security when compared to those that were taken care of by parent banks. Furthermore, vulnerabilities that manifest themselves as a result of using outdated versions of libraries provided by third parties were shown to be especially sensitive to being exploited. The results that were acquired from this empirical assessment give valuable insights that may be used to improve the security measures of banking apps, as well as other means by which commercial banks in Nigeria are doing financial transaction businesses and the resolution of differences among the different stakeholders.

Discussion

The study's empirical findings highlight the significance of internal control mechanisms and high-quality IT audit security work in Nigeria's banking industry. The Central Bank of Nigeria (CBN) has emphasized the detrimental effects of deficiencies in internal control systems and inadequate IT audit work on the decreasing growth of the banking industry. According to the conclusions of the report that the CBN issued, the findings were in agreement with those generated by other authors that highlighted the substantial impact of well-functioning internal control system controls. According to (Enofe et al., 2013), the paper emphasizes the significance of having an effective control system to guarantee the consistent quality of IT audit work that is performed in Nigerian commercial sectors. The findings of this study underscore the need to put in place robust internal control systems to effectively limit the risk of fraud, which poses a significant danger to the economy of Nigeria. The aforementioned assertion has substantial repercussions in connection with various fields.

Conclusion and Recommendation

In the study conducted and published by Lu et al.'s 2020 work, the empirical research has offered useful insights into the relevance of information technology security audits for the emerging technologies of Nigeria's commercial banks. These audits have also highlighted critical areas that need development. The findings shed light on the importance of sturdy and well-tailored internal control systems, good governance, adequate and well-aligned IT controls, and high-quality information technology security auditing work that is well performed by experienced IT auditors, either internally or externally contracted service providers. The primary objectives should be in the context of lowering the rate of fraud and enhancing the financial stability of commercial banks in Nigeria. This is in line with the standards that are imposed by regulatory bodies in the banking industry, such as the Basel Committee on Banking Supervision, which highlight the need for proactive assessments and management processes to reduce the risk of cyber fraud and other hazards (Hatsu, Ujapka and Mpimwood, 2015)

Volume: 9 Issues: 66 [September, 2024] pp. 845 – 853
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096670

It is recommended that Nigerian banks make the implementation and routine auditing of information security systems a top priority to both improve overall efficiency and protect themselves from potential dangers. They should make use of the results of studies that are analogous to those that were carried out in the commercial banking business in Nigeria. By providing a framework for future audits into the specific challenges and most successful techniques for managing information technology security audits and IT audits of emerging technologies at Nigeria's commercial banks, these practical proposals give a platform for further investigation. This article indicates that to properly handle the widespread problem of fraud and cybercriminals in the Nigerian commercial banking sector. According to (Adeolu Adebisi, 2024, pp. 279–281) it is recommended to use stringent measures such as increased regulatory oversight, the enforcement of ethical standards, and the internal purging of fraudulent elements inside organizations. The necessity for aggressive actions to protect the integrity and stability of Nigeria's commercial banking industry is brought to light by these works, which stress the urgent need for such measures.

Through careful assessment of the findings and the oversight of the CBN on the audits of information technologies on the emerging technologies of Nigerian commercial banks. The impacts and weaknesses of the internal controls have been identified which shows that the alignment of security strategies and business objectives is not in tandem with today's modern-day commercial banking standards. This work contributes to the body of knowledge by emphasizing the need for comprehensive information technology security audits for Nigerian commercial banks for effective maintenance of data integrity, IT assets, check-mating the cybercriminals, and efficient resource utilization.

References

Abiola, J. (2014) 'An Assessment of Information and Communication Technology Effectiveness in the Banking Sector : Lessons from Nigeria', 2(1), pp. 1–14.

Adebisi, A., Salamntu, L. and Paschal, W. (2024) 'Point of Sales (POS) Terminals for Bank Service Delivery, the needs for Management of Information Security: A case of Nigeria's Banking Sectors', in *2024 Conference on Information Communications Technology and Society (ICTAS)*. Durban: IEEE, pp. 150–160. Available at: https://doi.org/10.1109/ICTAS59620.2024.10507146.

Adedokun, I.A. and Oyewole, T. (2013) 'Evaluation of the Effect of Monitoring and Control Activities on Fraud Detection in Selected Nigerian Commercial Banks .', 4(6), pp. 57–63.

Adeolu Adebisi (2024) *POINT OF SALES (POS) SECURITY INFORMATION MANAGEMENT (POSSIM): AN ASSESSMENT OF TRUST AND SECURITY PERCEPTION*. Regenesys Business School.

Chen, S. *et al.* (2020) 'An empirical assessment of security risks of global Android banking apps', in *Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering*. New York, NY, USA: ACM, pp. 1310–1322. Available at: https://doi.org/10.1145/3377811.3380417.

Enofe, O. *et al.* (2013) 'Internal Control System and Quality Audit Work', *Research Journal of Finance and Accounting*, 4(13), pp. 100–106.

Fatoki, J.O. (2023) 'The influence of cyber security on financial fraud in the Nigerian banking industry', *International Journal of Science and Research Archive*, 9(2), pp. 503–515. Available at: https://doi.org/10.30574/ijsra.2023.9.2.0609.

Hassan, O. *et al.* (2024) 'CYBERSECURITY IN BANKING: A GLOBAL PERSPECTIVE WITH A FOCUS ON NIGERIAN PRACTICES', *Computer Science & IT Research Journal*, 5(1), pp. 41–59. Available at: https://doi.org/10.51594/csitrj.v5i1.701.

Volume: 9 Issues: 66 [September, 2024] pp. 845 – 853
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096670

Hatsu, S., Ujapka, M. and Mpimwood, E. (2015) 'An examination of the extent of implementation of the information security system and IT audit system in Ghananian Banks [J]', *Journal of Mass Spectrometry*, 5(11), pp. 33–42. Available at: https://core.ac.uk/download/pdf/234677262.pdf.

Ikenna, M. (2024) 'Operational Risks Faced by Financial Institutions in the Digital Age: A Case of Nigeria', *International Journal of Modern Risk Management*, 2(1), pp. 34–43. Available at: https://doi.org/10.47604/ijmrm.2642.

Mengist, W., Soromessa, T. and Legese, G. (2020) 'Method for conducting a systematic literature review and meta-analysis for environmental science research', *MethodsX*, 7, p. 100777. Available at: https://doi.org/10.1016/j.mex.2019.100777.

Monisola, O. *et al.* (2024) 'REVIEW OF IT INNOVATIONS, DATA ANALYTICS, AND GOVERNANCE IN NIGERIAN ENTERPRISES', *Computer Science & IT Research Journal*, 4(3), pp. 300–326. Available at: https://doi.org/10.51594/csitrj.v4i3.685.

Nnachi, R.A. *et al.* (2020) 'Effect of bank verification number on fraud management of selected commercial banks in Ebonyi State, Nigeria', *International Journal of Engineering Research and Technology*, 13(6), pp. 1165–1172. Available at: https://doi.org/10.37624/ijert/13.6.2020.1165-1172.

Ojeka, S., Ben-Caleb, E. and Ekpe, I. (2017) 'International Review of Management and Marketing Cyber Security in the Nigerian Banking Sector: An Appraisal of Audit Committee Effectiveness', *International Review of Management and Marketing*, 7(2), pp. 340–346. Available at: http:www.econjournals.com.

Okoye, P.V.C. and Ezejiofor, R. (2013) 'An Appraisal of Cashless Economy Policy in Development of Nigerian Economy', *Research Journal of Finance and Accounting*, 4(7), pp. 237–252. Available at: www.cenbank.org/out/speeches/2012/g...

Okoye, U. *et al.* (2018) 'Technology-based financial services delivery and customer satisfaction: A study of the Nigerian banking sector', *International Journal of Civil Engineering and Technology*, 9(13), pp. 214–223.

Olaniyi, O.O., Olaoye, O.O. and Okunleye, O.J. (2023) 'Effects of Information Governance (IG) on Profitability in the Nigerian Banking Sector', *Asian Journal of Economics, Business and Accounting*, 23(18), pp. 22–35. Available at: https://doi.org/10.9734/ajeba/2023/v23i181055.

Samuel, D., Grace, O. and Kensington, O.O. (2022) 'Information Technology Control and Fraud Risk Assessment in Deposit Money Banks (DMBs) in Nigeria', *The International Journal of Business & Management*, 10(4), pp. 7–18. Available at: https://doi.org/10.24940/theijbm/2022/v10/i4/BM2204-004.

Shamsudeen, L., Shagari, A. and Rafeah, M.S. (2018) 'A proposed model on the impact of internal control quality on accounting information system effectiveness in Nigeria', *Institute of Research Management Innovation*, 15(2).

Victory, C.O., Promise, E. and Mike, C.N. (2022) 'Impact of Cyber-Security on Fraud Prevention in Nigerian Commercial Banks', *Jurnal Akuntansi, Keuangan, dan Manajemen*, 4(1), pp. 15–27. Available at: https://doi.org/10.35912/jakman.v4i1.1527.