OPEN ACCESS

Global Journal of Research in Business Management
ISSN: 2583-6218 (Online)
Volume 03| Issue 01 | Jan-Feb | 2023
Journal homepage: https://gjrpublication.com/gjrbm/

Original Research Article

# Analytical Internal Audit Techniques and Cyber security Scans of Fraud Control: Evidence from Nigerian Listed Consumers Goods Firms

*Promise Akor ORDU [1], Prof. Sam A.OTAMIRI [2], Cletus O.AMAH [3]

[1]Department of Accounting, Faculty of Management Sciences, Ignatius Ajuru University of Education, Rumuolumeni, Port Harcourt, Nigeria
[2]Department of Office and Information Management, Faculty of Management Sciences, Ignatius Ajuru University of Education, Rumuolumeni, Port Harcourt, Nigeria
[3]University of Port Harcourt Business School, University of Port Harcourt, Nigeria

**DOI: 10.5281/zenodo.7555473** **Submission Date:** 09 Jan. 2023 | **Published Date:** 20 Jan. 2023

***Corresponding author:** Promise Akor ORDU PhD
Department of Accounting, Faculty of Management Sciences, Ignatius Ajuru University of Education, Rumuolumeni, Port Harcourt, Nigeria

## Abstract

The study investigated the relationship between Analytical internal audit techniques and Cyber security scans of fraud control in listed consumer goods firms in Nigeria. Nomothetic (quantitative) Philosophy was adopted while the cross-sectional survey research design was adopted. The population of the study was twenty-one (21) listed consumers' goods companies on the Exchange as at June, 2022. Using purposive sampling technique 11 of the companies was selected for the study and one hundred and sixty-five (165) copies of questionnaire were used for data gathering. Primary data was used for the study. Construct and face validity were used to establish the validity of the instrument, while Cronbach's alpha coefficient was used to ascertain reliability of instruments. A value of 0.984 was obtained for all constructs hence the reliability was ascertained. Univariate and Bivariate analysis were done. Pearson's Product moment correlation coefficient (PPMC) Statistics was used for data analysis with the aid of SPSS. The result of the study shows that Analytical technique has a strong, positive and significant relationship with Cybersecurity scans of listed consumer goods manufacturing companies in Nigeria. The study concluded that Analytical technique of internal audit technique has a significant relationship with Cybersecurity scans method of fraud control in listed consumer goods firms in Nigeria, thus implies that internal audit technique adopted could either make or mar the fraud control and preventive measures in place in the firms and could undermine the actualization of objectives of the frim. The study recommended that Management of listed consumer goods firms should adopt the analytical internal audit technique in addition to their traditional audit technique so that fraud control measures would be effective in tackling fraud, Fraud control measures such as cybersecurity scans among others should be adopted by the firms as a way of fraud prevention, There should be regular review and checking of IT systems, servers and other ICT to ensure that controls are in place and vulnerability to use as means of fraud are controlled. In addition, Management should ensure that the internal auditors acquire the requisite techniques and skills in computer operations and electronic data and other digital systems that enhances audit exercise especially to enable them able to carry out analytical procedures.

**Keywords:** Analytical Internal Audit Technique, Consumer Goods Firms, Cyber Security Scan, Fraud Control, Nigeria

# 1.INTRODUCTION

In recent times, on a global level, the issue of fraud has increased with the advent of virtual operations due to the impact of COVID 19 where many businesses were forced to operate online or at least have online channels for one or more business operations (Lillard, 2021). "In global economies such as USA, Lillard (2021) documented that during

2020, the Federal Trade Commission (FTC) received more than 2.2 million reports of fraud, up 500,000 from the 1.7 million reports filed in 2019. The significant increase in fraudulent activity was largely due to the result of the shift to virtual work across all industries in response to the COVID-19 global shutdown. This is because the level of business activity now conducted digitally provides additional opportunities for fraud perpetrators to take advantage of organizations. Furthermore, the pandemic combined with growing social unrest also changed the focus of many organizations.

Many shifted their attention from long-term strategic objectives to short-term remedies to cope with economic uncertainty and keep the wheels moving. The reason for this increased in fraud among businesses as Lillard (2021) pointed out was that a) many did not have the resources to allocate toward fraud prevention and cybersecurity, or b) either failed to recognize the need to allocate resources toward fraud prevention and cybersecurity while addressing the other challenges they were facing.

The situation is the same in Nigeria or even worse. Fraud in Nigeria is a subject that has received a lot of attention both in Nigeria and globally as such almost every media channel has one issue of fraud or corruption or the other as pertains to Nigeria and Nigerian businesses. According to Karwai (2013) the increase and high rate of fraud is causing a lot of havoc in all sectors of Nigeria both in public and private sectors. Okoye and Gbegi (2013) also reported that fraud is common that almost every individual cannot wash his or her hand clean of it; it is seen as a culture and a way of life. However, fraud is incipient in every aspect of Nigeria public sector while the private sector is doing its best to contain it but in terms of fraud prevention and detection. Fraud prevention is pre fraud it is basically efforts by an entity to eradicate or reduce instances of fraudulent activities. Fraud detection is post fraud it is the investigative actions taken to identify fraudulent activities that is already taken place or in the process of taking place (Ordu & Abowei, 2021; Onespan, 2021), consequently fraud control looks at preventing the fraud from occurring as well detecting it where it has occurred and thus ensure that a system is in place to prevent reoccurrence.

The Association of Certified Fraud Examiners (2008) defined fraud as the use of one's occupation for personal enrichment through deliberate misuse or misapplication of the employing organization's resources or assets. Therefore, it is any act of embezzlement, theft or misappropriation of company assets in a given economic context. It was considered as any act of deception by someone to deceive or deceive another person against someone else or to cause damage or loss to another person while the author has a clear knowledge of his intention to deceive, falsify or take advantage of the innocent and innocent victim with consequent losses or damages. Simply stated, fraud is any action, behaviour or oral expressions deliberately aimed at deception and/ or misinformation. It is a sequence of activities perpetrated to obtain money, property or services, to avoid payment or of services or to secure personal or business advantages. These acts are not dependent upon the application of threat of violence or of physical force (Ordu & Abowei, 2021).

Saleh (2016) documented that fraud in manufacturing companies in Nigeria is incessant and has a devastating effect on the sector. The sector is characterized by inefficient management composition and policies which has led to the increase in the level of fraud witnessed in the manufacturing industries. Lack of proper supervision has led to most of the fraud witnessed in the industry. Lack of training, nepotism and poor operations staff, poor segregation of duties, all have effect on numbers of fraud in the manufacturing industries (Saleh, 2016). With the increasing falling performance within the sector, it becomes important for firms to become innovative and think of ways of improving their positions including the management of assets to achieve this (Osazefua, 2019). This is where internal audit and auditors come to play. Internal audit being a unit in any establishment set up by the management of an organization for the review of internal control system as a service to the organization. The objective is to assist members of the organization including those in management and the board in the effective discharge of their responsibilities. Contemporary internal controls and well-functioning internal audit systems are meant to deliver key assurances to all stakeholders against fraud, corruption, waste, and inefficiencies such as in public services.

On the side of private institutions, effective and efficient internal audit systems help to safeguard assets, prevent fraud, waste and could ultimately lead to better performance or profitability of such entity. Thus, while carrying out its function, the internal audit uses various techniques at its disposal. This ranges from the traditional qualitative method of interview and observations to the more modern methods that involves the use of analytics and information and communication technology (ICT) to provide the assurance that financial information is of true representative and that the system of controls in not comprised so as to make the entity prone to fraud and wastages (Ordu et al., 2019; Ordu & Abowei, 2021).

Past studies have focused on other areas such as forensic accounting and fraud prevention (Okoye & Ndah, 2019; Ordu & Abowei, 2021), fraud prevention and business performance (Jezovita et al., 2018; Agwor, 2017; Saleh, 2016); internal control and financial performance, and fraud prevention (Ogwiji & Lasisi, 2022; Adeleke et al., 2020; Agyemang, 2020; Ibrahim et al, 2017), thus creating research gap in terms of sector, variable and scope. Consequently,

this study attempts to investigate the relationship between Analytical internal audit technique and cyber security scan fraud control in consumer goods manufacturing firms in Nigeria.

## Conceptual framework

The diagram in figure 1.1 is used to illustrate the interaction of predictor variables and the criterion variables

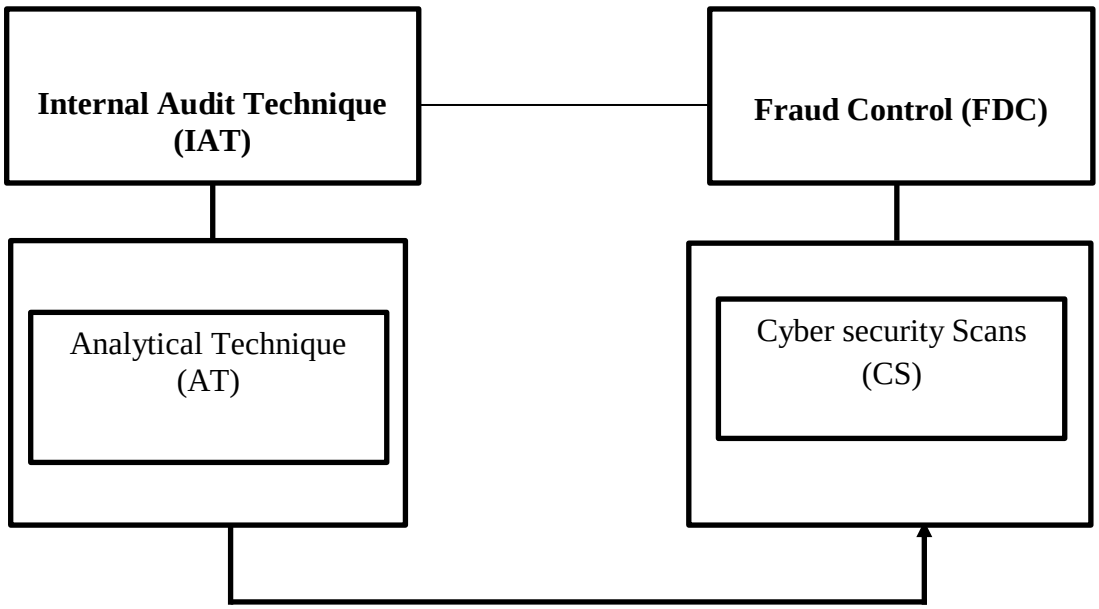



Figure 1.1: Conceptual Framework for the study
Source (Adapted from Gallagher, 2022; Lillard, 2021; Onoja & Usman, 2015)

**Objective of the Study**

- To investigate the relationship between Analytical Internal audit technique and Cyber security scans fraud control of listed consumer goods manufacturing companies in Nigeria

**Research Question**

- What is the relationship between Analytical technique and Cyber security scans of listed consumer goods manufacturing companies in Nigeria?

**Hypothesis**

- **HO:** There is no significant relationship between Analytical technique and Cybersecurity scans of listed consumer goods manufacturing companies in Nigeria.

## 2. LITERATURE REVIEW

## Conceptual Review

## Analytical Internal Audit Techniques

Analytics is not a technology; it's a concept. It refers to the use of certain technologies, skill sets, and processes for the exploration, evaluation, and investigation of business operations. It can be used to drive planning, gain insight, and optimize the internal audit lifecycle. The practice of analytics makes extensive use of data, statistical and quantitative analysis, explanatory and predictive modeling, and fact-based management to drive decision making. There are several disciplines contained within the scope of an analytics initiative: analytics methodology, analysis tools, performance management, descriptive statistics, exploratory data analysis, confirmatory data analysis, as well as data management. Used together, the disciplines of analytics provide hindsight, insight, and foresight. There are several factors that have really fueled the rise in the use of analytics in Internal Audit functions. Analytics — which is already used in many areas of the business, such as finance, workforce management, supply chain management, and customer relationship management — can help meet these expectations. Applying analytics to the internal audit process can facilitate moving beyond the traditional internal audit activities toward an environment of more sophisticated risk analysis and monitoring.

By leveraging the power of analytics, the internal audit process can produce insights and conclusions that help decision makers take action quickly and make more effective, timely decisions, (Delloitte 2012). Analytics provides answers to decision makers from three perspectives: historical, current, and future — i.e., it provides hindsight, insight, and foresight. It can help users ask such questions as, What happened, and why?, Where is the problem, and what actions

do I need to take to solve it?, What will happen if these trends continue?, and finally, and perhaps most importantly, What's the best/worst that could happen? This predictive capability of analytics supports the shift toward dynamic risk-focused audit planning and audit execution over static traditional planning approaches. Perhaps one of the biggest challenges that the internal audit process faces today is the expectations of the C-suite and Audit Committee, that Internal Audit should support the business by delivering deeper insight and greater value more efficiently and effectively. Some of the more challenging expectations of Internal Audit include:

(i) Being more efficient and achieving more with less
(ii) More effectively identifying and responding to risk
(iii) Delivering more robust and effective analysis of key issues
(iv) Providing more meaningful actionable insights
(v) Driving change within the business

By applying analytic tools and techniques, internal auditors obtain deeper insight into their data, systems, and processes and gain the ability to ask — and answer — new and more complex questions about government transactions. They can move from asking What do we need to do? to What do we need to know? The shift is subtle, but powerful (Onoja & Usman, 2015)

Concurring with the assertions of Onoja and Usman (2015), Jezovita et al. (2018) noted that internal auditors are facing today's fast-paced business conditions that challenge them to implement adequate information technology and use analytical procedures as key audit techniques. Continuous technology improvement enables the development and application of analytical procedures that were unimaginable in the time of 'paper-based auditing' (Jezovita et al., 2018). It is argued that the importance of using analytical procedures can be confirmed by the positive effects these procedures have in internal auditing as they increase its effectiveness and efficiency PWC (2018) concludes that analytics is a perennial high-impact area for several reasons. First, beyond-the basics analytics is the single most powerful booster of Internal Audit efficiency and effectiveness available. Second, the continuing digitalization of business generates huge quantities of data, which analytics can transform into valuable information and business insights. Third, the tools for analyzing and visualizing data are now simpler, cheaper, more available, and easier to use than ever (PWC, 2018). Analytical techniques to be employed may be: quantitative, which may employ simple techniques (e.g. frequency counts) or more sophisticated techniques (e.g. regression analysis). Computer assisted audit techniques (CAATs) are often an essential part of quantitative analysis. In summary the analytical techniques are Frequency counts, Ration Analysis, Comparative Analysis, Trend analysis, Variance Analysis, Regression Analysis (Jezovita et al. 2018).

## Application of Analytic Technique in Fraud Detection

Where analytics can be applied is in fraud detection and exception identification algorithms; these are often based upon anomaly detection schemes. Myriad techniques can be employed from logical risk scoring to decision trees to stochastic link analysis. Applying these techniques in combination detects transactions that are the most likely to exhibit fraudulent or exceptional characteristics. Further automating and scheduling these routines helps Internal audit to move toward automated detection and exception-based auditing.

## Reasons for the use of Analytic Audit technique

There are several factors that have really fueled the rise in the use of analytics in Internal Audit functions. The first is the explosion of data volumes both structured and unstructured. With this explosion have come innovations in the capture of, and reporting on, that data. The next is the increasing expectations of key stakeholders' vis-à-vis the nature and value of reported information that the internal audit process produces. As the revenue accruing to an entity for example the local government in recent years grows increasingly, stakeholders require deeper insights and clearly stated facts to support decisions, build greater value, and create a more dynamic focus on accountability (Onoja & Usman, 2015).

## Concept of Fraud Control

To be able to understand what fraud control entails, we will first of all define and explain what fraud is generally. Albrecht (2003) defines fraud as a representation about a material fact which is false and intentionally or recklessly so, which is believed and acted upon by the victim, to the victim's damage. The Association of Certified Fraud Examiners (2008) defined fraud as the use of one's occupation for personal enrichment through deliberate misuse or misapplication of the employing organization's resources or assets. Therefore, it is any act of embezzlement, theft or misappropriation of company assets in a given economic context. It was considered as any act of deception by someone to deceive or deceive another person against someone else or to cause damage or loss to another person while the author has a clear knowledge of his intention to deceive, falsify or take advantage of the innocent and innocent victim with consequent losses or damages (Ordu & Abowei, 2021).

According to Udoayang and James, (2004), fraud is simply stealing by tricks. Ramamoorti and Olsen (2007), in their definition of fraud argued that it is a human endeavor, involving deception, purposeful intent, intensity of desire, risk of apprehension, violation of trust and rationalization, Several authors (Hamilton & Gabriel, 2012) agree that a fraudulent

activity involves the use of deceit and tricks to change the truth so as to deprive another person of his right. Fraud is any action, behaviour or oral expressions deliberately aimed at deception and/ or misinformation. It is a sequence of activities perpetrated to obtain money, property or services, to avoid payment or of services or to secure personal or business advantages. These acts are not dependent upon the application of threat of violence or of physical force (International Standards for Professional Practice of Internal Auditing, 2002).

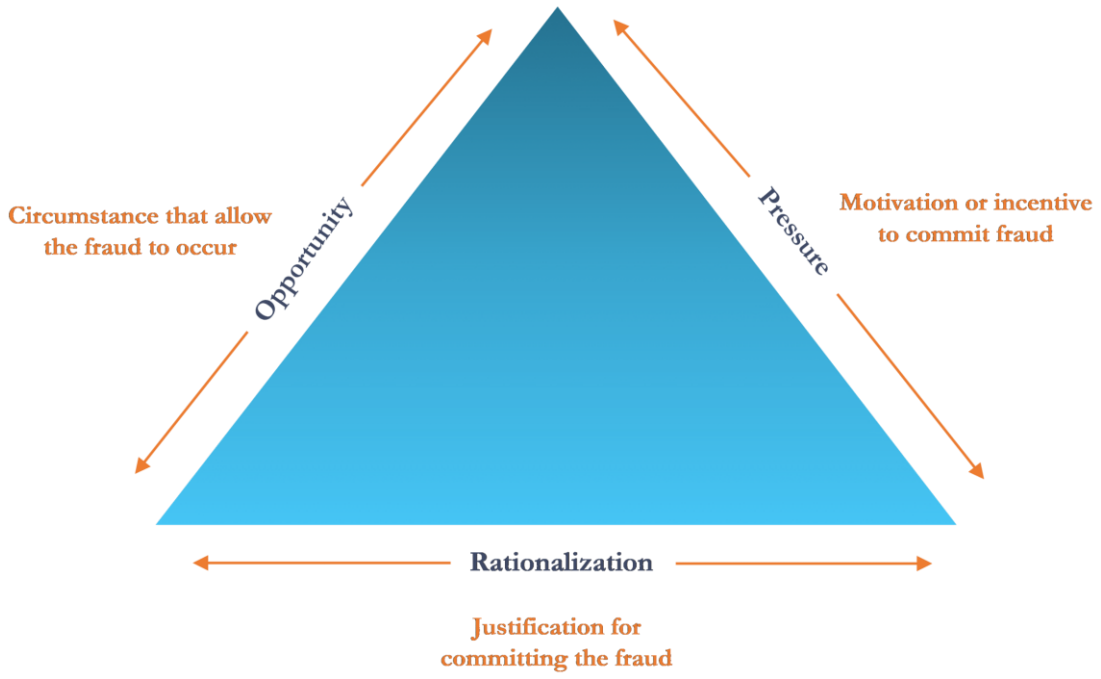
Pedneault et al. (2007), agree that modern definition of fraud appears to be derived from case and statute law even though many of the ancient components still obtain. It can be traced to the Latin noun fraus, which conveys a range of meaning centered on the idea of harm, deceit and wrong doing (Silverstone & Sheetz, 2007). The modern definition derived from case law focuses on the intent of the fraudster(s) to separate the trusting victim from property or a legal right through deception for his or her own benefit (Silverstone & Sheetz, 2007). In any case, all the definitions of fraud stresses on acts that are capable of misleading and misappropriation committed deliberately. Such acts are carried by somebody or group of persons against another person or an organization, and can be expressed verbally or through behavior (Ogundana et al., 2018).

Agwor (2017) stated that companies put polices and procedure in place. An employee committing fraud circumvent those policies and procedures, thus an employee committing fraud is not making a mistake but deliberately circumventing the system. The employee uses various methods to conceal his/her actions. Lies are told, document are falsified, transaction recording are misrepresented, internal controls are abused (Agwor, 2017).
Ramaswany (2007) discussed the classifications of frauds to include these categories:

(i) **Employee fraud:** fraud committed by an employee against an organization.
(ii) **Management fraud:** fraud committed by management using financial statements to defraud stockholders, lenders and others who rely on those statements.
(iii) **Investment scams:** fraud committed by individuals to trick their victims into investing their money in scams and false investments.
(iv) **Vendor fraud:** fraud committed by vendors by overcharging or falsely charging a company.
(v) **Customer fraud:** fraud committed by customers that trick organizations into giving them something that they should not have.
(vi) **Identity theft:** fraud committed by individuals who steal personal information from a victim and then go on to purchase goods or services using this information.
(vii) **E-commerce fraud:** fraud committed using the Internet and electronic transactions.

## Explanations for Why People commit Fraud

Like any other crime, fraud can be analyzed using the three elements of motive, means and opportunity (Ramaswany, 2007). These are represented in the Fraud triangle.



The Fraud Triangle notes the following three elements that give way to fraudulent activity. Anyone or a combination of the three elements can ultimately result in fraudulent activity.

(i) **Motives:** Why do people commit fraud? Fraud is usually committed to benefit oneself or benefit an organization. Personal reasons could include financial pressures, gambling or drugs, and work related pressures where an employee feels overworked and underpaid and unrecognized. For an organization, financial statement fraud is usually for obtaining cheap capital or for increasing stock value and therefore the value of stock options to management.

(ii) **Means:** Like a smoking gun, fraud can be committed using computers, telephones, the Internet, annual reports, bank accounts, and things as simple as a cash register.

(iii) **Opportunity:** Within an organization, lack of adequate internal controls provides a prime opportunity for fraud. Lack of audit trails and failure to punish the perpetrators also send signals encouraging fraud. In other cases, lack of access to important information, and ignorance and apathy can breed fraud.

**Types of Fraud**

a) Larceny (Theft): It involves the unlawful taking from another's possession or unlawful appropriation of property by a person to whom it has been entrusted with the intention or permanently depriving the other from it. Theft may be internal or external, it may be carried out by the staff or outsiders (customers) and both may even jointly perform the operation.

b) Forgery: It is the making of a false document in order that it may be Used as a genuine document with the intention of deceiving or defrauding.

c) Transfer or Legal Title: This covers fraudulent transfer or legal title to assets and fraudulent creation of liabilities.

d) Manipulation of Figures: This involves the accounting for slims either lesser or greater than those actually received, also depending on the objective of the fraudulent party. It also includes: Destroying, defacing, canceling or falsifying of records required for accounting purpose.

e) Misappropriation of Assets: Involves converting money or assets in money's worth obtained in one's official capacity for the use of another person or business into one's own use without authority for such use.

**Other Forms Defined**

a) Falsity: A document is a false one if it is not what it proposes to be or it has been materially altered without authorization since it was made.

b) Making of a false Authorization: This refers to altering or attaching of a seal or stamp to the document. It also includes the addition or deletion of material words, letters or figures.

c) Uttering: This is merely a fraudulent offer. It should-be noted that, the use of a photocopy of a forgery is an offence (Ordu & Abowei, 2021).

Fraud control involves the implementation of strategies to prevent and detect fraudulent transactions and activities in the organization. It involves two activities together, which are fraud prevention and fraud detection. Fraud prevention is pre fraud it is basically efforts by an entity to eradicate or reduce instances of fraudulent activities. Fraud detection is post fraud it is the investigative actions taken to identify fraudulent activities that is already taken place or in the process of taking place (Ordu & Abowei, 2021; Onespan, 2021), consequently fraud control looks at preventing the fraud from occurring as well as detecting it where it has occurred and thus ensure that a system is in place to prevent reoccurrence. On the other hand, fraud prevention involves the integration of all efforts that may be used to reduce or limit the opportunities to commit fraud, ensure employees are able to meet their needs in order to reduce pressure on them that would lead to commit fraud and lastly ensure that there is no justification by employees to commit fraud (Nyakarimi et al., 2020). Fraud prevention can be effective if the organization maintains ethical practices, maintains organizational honesty culture, assess the possibilities and eliminate risks, reduce the fraudulent activities and implement internal control mechanism (Ogbwiji & Lasissi, 2022).

Fraud prevention and cybercrime are connected and always changing. As fraud prevention professionals develop new authentication and fraud detection solutions, the fraudsters are networking with each other, monetizing, and exchanging information on the Dark Web. Fraudsters today are using sophisticated strategies and malware to succeed in their fraudulent activities. Though fraud prevention technology has made great advances and continues to do so, it's important to be aware of fraudulent tactics and understand how to prevent fraud (Onespan, 2021), thus makes is necessary for internal audit techniques to be in tandem with the modern and sophisticated nature of fraudulent activities in this modern times otherwise, control systems will continue to be undermined.

Lillard (2021) asserted that basic fraud prevention techniques include low-cost, high-value tools that help minimize the risks associated with the elements of the Fraud Triangle. He argued that the most important aspect of each is ensuring that it is custom-tailored to fit your organization's context and overall risk appetite. Following implementation, these tools must be regularly monitored or evaluated for ongoing effectiveness. Fraud control and prevention is an ongoing process that changes with the organization and the external environment. Some of the techniques used include internal

controls, employee trainings, policies and procedures; employee evaluation cyber security scans among others (Lilliard, 2021).

## Cyber security Scans

Cyber Security Scans is the process of checking the IT systems, servers and other ICT to ensure that controls are in place and vulnerability to use as means of fraud are controlled. According to Shah et al (2020), Cybersecurity has received significant attention from researchers and professionals. It has become an integral part of business activities in all organisations regardless of their size and nature and has become particularly important for online businesses. Cybersecurity readiness can be achieved by implementing a resilient culture against cyber related threats and attacks. This culture would be useful for organisations to mitigate the impact of cyber-attacks. However, these businesses are facing cybersecurity threats/attacks from both internal and external sources (Manhart & Thalmann, 2015). Cyber threats/attacks and frauds are increasing and posing many challenges for online organisations. These challenges include externals/internals threats accidental damage and technical/organisational weaknesses.

Cyber threats include identity theft (Humaidi, & Balakrishnan, 2018) and unauthorised access to an organisational network (Da Veiga, 2016). Denial of Service (DoS) attacks, malicious insiders, web-based attacks (Clark, & Harrell, 2013), human error (Da Veiga, 2016), phishing emails and inadequate security monitoring (Safa, & Von Solms, 2016) are also documented threats. There are some reasons which contribute to the success of these attacks, for example, preventative equipment failures (Reason, 2016), lack of technical awareness (Pieters et al., 2016), unauthorised access (Da Veiga, 2016) and malicious employees (Clark, & Harrell, 2013). Some basic security controls such as encryption, anti-virus software, firewalls and intrusion detection systems (IDS) suggested by Sen et al., (2015) could be used to prevent cyber-attacks. Unified Threat Management Systems (UTMS) provide more security to the network layer, hardware and software than standard security methods (Kent, et al., 2016). Secure authentication and authorisation systems are useful in preventing ID theft (Sharma, et al., 2015). Regular assessment of security controls and monitoring of internal and external security systems may reduce the risk of cyber-attacks (Taylor, 2016).

Cybersecurity readiness includes security policies, processes and procedures that are employed in the organisation to manage cyber threats. Furthermore, a review of cybersecurity readiness includes examinations of security functions, to check whether these functions operate in line with relevant policies, standards or procedures (Pereira & Santos, 2010). The importance of cybersecurity readiness has been increasingly recognised worldwide. Many leading countries have invested in their cybersecurity and have published official strategy documents for their cybersecurity; these include USA, UK, Canada, Australia, Japan, Germany and Russia (Klimberg, 2012). Cybersecurity breaches are becoming increasingly common against companies regardless of their size and nature (Waly et al., 2012). Cyber-attacks are malicious acts usually originating from an anonymous source that either steals, alters or destroys a specified target by hacking into a susceptible system.

According to Uma and Padmavathi (2013), several dimensions of cyber-attacks can be found in existing literature, but the primary objective of such attacks is to compromise the confidentiality, integrity and availability of information resources. These cyber-attacks tend to be successful due to weaknesses in technical infrastructure (Shinde, & Ardhapurkar, 2016). Due to a lack technical awareness, people become victims of cyber-attacks (Pieters, et al., 2016). Therefore, this research focuses on cybersecurity readiness in the technical perspective to aid the online retail company in mitigating against potential cyber risk. With the advancement in the technology, new methods of cyber-attacks are also emerging (Waly et al., 2012). It is the responsibility of management to perform risk analyses and highlight flaws and vulnerabilities in the information systems, as neglecting these tasks can increase the likelihood of successful cybersecurity attacks. As a result, online retail organisations must maintain update infrastructure to reduce the impacts of cyber-attacks in the organisation. Ultimately, these attacks affect organisations in the form of significant financial losses and reputational damage.

There are many technical threats that are possible reasons for cybersecurity breaches in online retail organisations. These include: Malware, Spam, Phishing, Spear-Phishing Attack, Denial of Service (DoS) attack, Distributed Denial of Service (DDoS), Man in Middle Attack, Hacking, Social Engineering, Spoofing, Keylogging, Cookies, Backdoor Trojan, SQL Injection and Identify Theft.

Cybersecurity threats are a growing concern for online retail organisations. Organisations considered cyber-attacks to be the biggest threat to businesses. A recent study by Hui et al. (2017) indicated that many DDOS attacks targeted banks (24%), telecommunications companies (23%) and financial services organizations (20%), indicating they were likely financially motivated. Another survey conducted by the PWC (2018) indicates that the average financial cost of cybersecurity incidents (including costs relating to business operations and data) is £857,000. The same report also pointed out that UK organisations are more reluctant in combating against cyber-attacks than peer organisations in the other countries.

The above discussion was about cybersecurity threats and attacks that affect online businesses in various forms. Effective counter measures are needed to prevent cybersecurity threats from materialising. There are several factors such

as technical, organisational and human which increase the success rate of these attacks, for example, Uma and Padmavathi (2013) stated that there is a lack of proper understanding and technical awareness of the nature of cyber-attacks. By implementing security measures and controls, companies can help mitigate against these attacks. Legitimate antivirus or endpoint security software along with user awareness regarding threats posed by clicking on suspicious links would be useful in mitigating cyber-attacks. Organisations also use anti-spam software to limit the spam attacks, coupled with other countermeasures such as two factor authentication, web application scans, firewalls, access control, encryption and unified threat management appliances.

.

However, cybersecurity readiness from a technical perspective can be achieved by proper implementation of technical controls to safeguard organisational infrastructure to mitigate the potential cyber-attacks (Shah et al., 2020). Conducting regular cybersecurity scans is critical to staying ahead of hackers and proactively enhancing your cybersecurity posture. Internal IT departments can acquire these technologies affordably to run on their own systems and organizations who outsource their IT can request their Managed Service Provider or outside consultant provide these services (Lillard, 2021).

## Theoretical Framework

### Policeman Theory

This theory of auditing is based purely on the arithmetical accuracy and on the prevention and detection of fraud. This theory makes the auditor to detect and prevent errors and fraud in organizations. In other words, as this theory posits, the auditor has to act as a policeman with actions and intentions to watch, safeguard and protect the organizational resources so that stakeholders could benefit overall. It is argued that from the 1940s till present, there has been a shift of audit paradigm as compounded by recent financial statement frauds, such as those at Societe Generale, Satyam, Ahold, Enron, etc (Egbunike & Egbunike 2017), consequently there is an increasing debate on the responsibility of the auditor both at the internal and external level to detect and disclose fraud, thus the auditor must Police the organizations at all times.

Policeman theory was the most widely used concept of auditing until the 1940s (Hayes et al., 2000). According to this theory, an auditor carries out the duties of a police officer, focusing on arithmetic accuracy, prevention and detection of fraud. Due to its failure to explain the shift from the audit to the verification of the truth and fairness of the financial statement, however, the theory seems to have lost much of its explanatory value. According to the police theory, the auditor is responsible for the research, discovery, identification and prevention of fraud. The main focus of the auditors was recently to ensure the accuracy and fairness of the financial statements. Fraud control – both prevention and detection is a hot topic in the debate on auditor responsibility, on the other hand, and the pressure on auditors to detect fraud often intensifies as cases of financial statements fraud are revealed (Hayes et al., 2005). According to the audit literature the company is responsible for the detection of fraud and irregularities which can obtain reasonable assurances that such liability has been carried out through an internal control system. It is not the responsibility of an auditor to seek fraud unless he is required to do soon a specific basis. The hypothesis presupposes that fraud occurs in an organization or agency and that an effective technique used by the auditor should enable the auditor to detect and prevent fraud, as the auditor cannot prevent or discover fraud.

## Review of Empirical Literature

Ogwiji and Lasisi (2022) study investigated internal control system and fraud prevention of quoted financial services firms in Nigeria: A smart PLS-SEM approach. The study sought to examine the effect of internal control system on fraud prevention of financial services firms in Nigeria. The population was 284 respondents from the listed financial services firms in Nigeria. A cluster sampling technique was adopted for the study. The data was sourced through the primary sources and a structured questionnaire were administered to the respondents through the use of five-point Liker scale system, and the SMART-PLS-3-SEM was used to analyze the fitness of the data and test the research hypothesis. Findings from the study revealed that control environment and monitoring were found to have a positive and significant effect on fraud prevention, while the information and communication has a negative and significant effect on fraud prevention. Risk assessment showed an insignificant positive effect on fraud prevention while control activities has negative and insignificant effect on fraud prevention of the listed financial services firms in Nigeria. The study found that internal control system has a significant influence on fraud prevention. It was recommended among others that the management of financial services firms should maintain the used in control environment, monitoring system because they play a greater in effect on fraud prevention. Also, regulator agency such as CBN, EFCC and ICPC should develop an internal control framework and policy that will guide the financial services firm in Nigeria.

Ordu and Abowei (2021) study focused on critical analysis of the link that exists between the use of forensic accounting, and electronic accounting in checkmating fraud. Its objectives were: 1) to provide conceptual definitions, origin and applications of forensic accounting, 2) electronic accounting evolutions, importance and challenges associated with its evolution, 3) the connection between electronic accounting, forensic accounting and internet fraud detection and minimization by finance professional. Extensive literature review methodology was adopted for the study. The study discovered that forensic accounting is an evolving concept that is so important in tackling of fraud given the

multidimensional nature of frauds – including internet fraud in contemporary times. In addition, the evolution of E-Accounting has simplified and made the work of forensic accounting easy in detecting fraud. However, this is achieved only when there is its embrace and right environment created for it to work. Internet fraud has taken many dimensions-some appear to be legal why some are obvious including the Yahoo Yahoo (the Nigerian Prince). The cost is huge – both globally and local to Nigerian economy and to many Nigerian individuals. It recommended amongst others, that regarding forensic accounting development in Nigeria, government must provide the favorable environment to enable forensic accounting profession to thrive in the country by strengthening the legal, educational and political frame work in the country (Nigeria).

Nyakarimi et al., (2020) examined the effect of internal control system on fraud prevention as proxy of risk management in banking sector in Kenya. The study involved all the banks where branch managers, operations managers and cash supervisors were sought for the study. The study analysed 117 questionnaires from respondents. Factor analysis was used to reduce the number of variables for analysis purposes. Correlation research study and structural equation model were applied in the study to establish the relationship between variables and in analysis of hypotheses. The study found that control environment has no statistically significant and a negative effect on fraud prevention.

Agyemang (2020) study within the Ghanaian context investigated internal control and fraud prevention. The main objective of the study was to assess the effect of internal controls on fraud prevention. The questionnaire was used to obtain data for the study. A combination of purposive sampling and random sampling techniques were used to select the sample elements. A sample of ten (35) management staff including the internal auditor was selected for the study. Descriptive statistics using frequency tables and charts were used for data analysis using SPSS. The study revealed that, the internal control measures put in place by management have helped the bank in preventing fraud. It was again revealed that majority of the respondents agreed that management ensure that all necessary measures needed to prevent and detect fraud are provided. Also, majority of the respondents (91.4%) revealed that there is an effective supervision and implementation of internal control system capable of revealing fraudster's mode of operations in the bank. The study recommended that a well-established internal audit department must be created with its staff fully equipped; Management should institute incentive packages in place in order to prevent employees from engaging themselves in fraudulent activities.

Shah et al. (2020) study investigated Cybersecurity readiness of E- Retail Organisations: A technical perspective. This study investigates cybersecurity readiness from the technical perspective in some UK online retailers. This research adopted a qualitative case study approach with semi-structured interviews for collecting data. A total of 15 interviews were conducted with an online retail company's staff and management who had responsibility for managing cybersecurity. A thematic analysis method was used to analyse the qualitative data. The research findings showed that the company is facing internal and external threats to their information systems and their technical defences are not very effective at present. The study recommended that the company should consider investing more resources in the technical controls to prevent these attacks.

Jezovita et al (2018) study focused on the state of analytical procedures in the internal auditing as a corporate governance mechanism within the Croatian context. The study argued that internal auditors are facing today's fast-paced business conditions that challenge them to implement adequate information technology and use analytical procedures as key audit techniques. Continuous technology improvement enables the development and application of analytical procedures that were unimaginable in the time of 'paper-based auditing. Consequently, the study aimed at investigating the level and improvements of analytical procedures by internal auditors working in contemporary business conditions in Croatia. Specifically, the study examined the coherence between available technology and applied analytical procedures; an investigation of the level, differences and complexity of analytical procedures used in internal audit in order to determine the current state of and prospects for improving the effectiveness and efficiency of internal audit activity in Croatia as well as examined the extent to which, measured by the analytical procedures application level, internal audit functions in Croatia are adapting to contemporary business conditions and changing professional processes. The research issues were analyzed by using the theoretical overview, guidance provided by professional institutions, and the importance that internal auditing has as a corporate governance mechanism.

Appelbaum et al. (2018) in their study stated that analytics prevail over traditional audit procedures. The authors concluded that in certain cases analytical procedures may be more effective and efficient than substantive tests of details, especially in cases when the data set is large and varied.

Tan et al. (2017) state that the use of data analytics should be a priority for future internal auditing. Advanced analytics are newly introduced to internal auditing, which is supported by Li et al. (2018) who concluded that most companies do not use full audit analytics. Changing from a traditional to contemporary approach of internal auditing usually implies its developmental role by focusing on policies, transactions and compliance to risk-based approach that focuses on goals, strategies and risk management processes.

Saleh (2016) study investigated effect of internal control on fraud prevention in Maiduguri manufacturing industries Nigeria. The objective of the study was to critically appraise the effect of internal control on fraud prevention in

manufacturing industry using flourmills Maiduguri as a case study with the intention of finding out the extent to which fraud is actually prevented in manufacturing industries. The required data for this research work was obtained through questionnaire, oral interview conducted among respondents, text books, journals etc. from the data analysis carried out, (chi-square and ANOVA used for data analysis ) the major findings were; inefficient management composition and policies have led to the increase in the level of fraud witnessed in the manufacturing industries. Lack of proper supervision has led to most of the fraud witnessed in the industry. Lack of training, nepotism and poor operations staff, poor segregation of duties, all have effect on numbers of fraud in the manufacturing industries. The study found out that manufacturing industries have put all necessary control measures required to prevent fraud and that each successful fraud in the industry always go through with the help of insiders. The recommendation suggested was that manufacturing industries should ensure that their management composition and policies is efficient enough to control and check fraud. Staff remuneration should be reviewed to meet up with the present standard of living in the country. Recruitment of staff should be based on merit and achievement but not on nepotism. Very importantly, proper system of internal control must be put in place to check fraudulent members of staff.

Onoja and Usman (2015) study investigated internal audit techniques and fraud prevention: A case study of selected local government councils in Bauch State. This study analyzed the Internal Audit Techniques and Fraud Prevention in Bauchi State Local Government Councils. The data for the study were collected from both the primary and secondary sources. The primary sources data were collected from the thirteen (13) local governments internal audit units through self-administered questionnaires to the sample size of the study. The secondary sources were documents from Bauchi state ministry for local government affairs. Several statistical tools were used including tables, simple percentages, Chi-square and Pearson Product Moment Correlation Coefficient to analyze the data and test the null hypotheses formulated. The study revealed that the internal audit unit at local government put necessary measures to prevent fraud but lack total independent freedom to carry out their function effectively. The study concluded that the internal audit units at local government level in Bauchi state are performing the function of fraud prevention and the internal audit techniques/procedures capable to prevent any type of fraud was effective. It was discovered that internal audit unit at local governments' level in Bauchi state are not independent, and this affected their functions. The study recommended among other things that, Bauchi state government through House of Assembly should enact laws/legislation that will grant internal audit unit autonomy to discharge their functions. Effective internal audit techniques/procedures capable of preventing fraud should be installed by the councils and that adequate measures and control should be put in place.

## 3. METHODOLOGY

Nomothetic (quantitative) Philosophy was adopted while the cross-sectional survey research design was adopted. The population of the study was twenty-one (21) listed consumers' goods companies on the Exchange as at June, 2022. Using purposive sampling technique 11 of the companies was selected for the study and one hundred and sixty-five (165) copies of questionnaire were used for data gathering. Primary data was used for the study. Construct and face validity were used to establish the validity of the instrument, while Cronbach's alpha coefficient was used to ascertain reliability of instruments. A value of 0.984 was obtained for all constructs hence the reliability was ascertained. Univariate and Bivariate analysis were done. Pearson's Product moment correlation coefficient (PPMC) Statistics was used for data analysis with the aid of SPSS.

## 4. RESULTS AND ANALYSIS

### 4.1 Univariate Analysis

**Table 4.1: Analytical Technique**

| | ANALYTICAL TECHNIQUE (AT) | 0=UD | 1=SD | 2=DA | 3=A | 4=SA | TOTAL |
|---|---|---|---|---|---|---|---|
| **1** | Adopting the use of technologies for compliance testing by the auditor could enhance fraud control practice in the company | 0 | 4 | 5 | 70 | 40 | 119 |
| **2** | The use of computer programs and statistics by the auditor for conducting compliance test can enhance fraud control practice in the companies | 0 | 0 | 0 | 60 | 59 | 119 |
| **3** | Using skills sets, and processes to conduct substantive tests by the auditor could enhance fraud control practices in the firms | 0 | 0 | 0 | 80 | 39 | 119 |
| | Total | **0** | **4** | **5** | **210** | **138** | **357** |
| | Total Weighting | **0** | **4** | **10** | **630** | **552** | **1196** |
| | Percentage (%) | **0** | **0.3** | **0.8** | **52.7** | **46.2** | **100** |

**Source: Survey Data, 2022**

From the table 4.1 above, of the total weighting of 1196 of all respondents obtained on the issue of Analytical technique internal audit technique for effective fraud control, 46.2 % of the respondents indicated strongly agreed to the questions asked, 52.7 % indicated agreed, 0.8% indicated disagreed and 0.3% strongly disagreed while there were no responses on other criteria. Again, the mean values (3.35014) greater than the criterion mean (Table 4.10) indicating that the respondents considers analytical technique of internal audit technique as key to fraud control in the firms.

**Table 4.2: Descriptive statistics of independent variable**

| | | AT |
|---|---|---|
| N | Valid | 119 |
| | Missing | 0 |
| Mean | | 3.35014 |
| Std. Deviation | | .498300 |
| Skewness | | .191 |
| Std. Error of Skewness | | .222 |
| Kurtosis | | -1.183 |
| Std. Error of Kurtosis | | .440 |
| Sum | | 398.667 |

**Source (SPSS output of data, 2022)**

From the descriptive statistics table above, Analytical technique dimension has a standard variation of 0. 498300 and mean value of 3.35014, and mean score is greater than 3, indicating that there are evenly distributed.

## Table 4.3 Cyber security Scans

| | CYBERSECURITY SCANS (CS) | 0=UD | 1=SD | 2=DA | 3=A | 4=SA | TOTAL |
|---|---|---|---|---|---|---|---|
| **4** | Internal audit technique that involves regular checking and review of the IT systems can enhance fraud control in the company | 0 | 0 | 0 | 54 | 65 | 119 |
| **5** | Regular review of servers and other ICT to ensure that controls are in place can help to reduce fraud in the companies | 7 | 0 | 5 | 35 | 72 | 119 |
| **6** | Adopting the right audit technique for systems audits and other audit activities can help check the incidences of cyber fraud in the company | 0 | 0 | 19 | 40 | 60 | 119 |
| | Total | **7** | **0** | **24** | **129** | **197** | **357** |
| | Total Weighting | **0** | **0** | **48** | **387** | **788** | **1223** |
| | Percentage (%) | **0** | **0.5** | **0.4** | **37.4** | **61.7** | **100** |

**Source: Survey Data, 2022**

From table 4.3 above, of the total weighting of 1223 of all respondents obtained on the issue of cybersecurity scans means of fraud control through the use of internal audit technique, 61.7% of the respondents indicated strongly agreed to the questions asked, 37.4% indicated agreed, 0.4% disagreed on their responses, while 0.5% indicated strongly disagreed on their responses. O% however was undecided.

**Table 4.4 Descriptive Statistics of dependent variable**

| | | CS |
|---|---|---|
| N | Valid | 119 |
| | Missing | 0 |
| Mean | | 3.42577 |
| Std. Deviation | | .694238 |
| Skewness | | -.990 |
| Std. Error of Skewness | | .222 |
| Kurtosis | | .144 |
| Std. Error of Kurtosis | | .440 |
| Sum | | 392.667 |

**Source (SPSS output of data, 2022)**

From the descriptive result analysis as shown on the table above, Cyber security scan (CS) has a variation of 0. 694238 and a mean value of (3.42577). Again with the dependent variable scoring a mean score of greater than 3 also indicates that they are evenly distributed.

## 4.2 Bivariate Analysis and Test of Hypothesis

**Decision Rule**: Accept null hypothesis if Sign F is greater (2 tailed) than 5% (0.05) (Sign F>0.05), otherwise, reject the null hypothesis.

- **HO1:** There is no significant relationship between Analytical technique and Cybersecurity scans of listed consumer goods manufacturing companies in Nigeria.

**Table 4.5: PPMC Correlations Result for Hypothesis one**

| | | AT | CS |
|---|---|---|---|
| AT | Pearson Correlation | 1 | .823** |
| | Sig. (2-tailed) | | .000 |
| | N | 119 | 119 |
| CS | Pearson Correlation | .823** | 1 |
| | Sig. (2-tailed) | .000 | |
| | N | 119 | 119 |

**. Correlation is significant at the 0.01 level (2-tailed).

**Source: (SPSS output of Data, 2022)**

From the table above, the positive and very large value of PPMC (0.823**) indicates that there is a very strong correlation between Analytical technique and Cybersecurity scans of listed consumer goods manufacturing companies in Nigeria, and correlation is significant at 0.01 level. Since the p – value (= 0.000) is less than the level of significance (alpha) (0.05), we therefore reject the null hypothesis and conclude that: there is a significant relationship between Analytical technique and Cybersecurity scans of listed consumer goods manufacturing companies in Nigeria. "

## Discussion of Findings

From the result obtained it shows that Analytical technique has a strong, positive and significant relationship with Cybersecurity scans of listed consumer goods manufacturing companies in Nigeria. This is evident in the correlation value of 0.823** (82.3%). The null hypothesis was therefore rejected and the alternative hypothesis accepted. The result shows that 82.3% of the changes in fraud control in terms of cybersecurity scans is accounted for by analytical technique aspect of internal audit technique of listed consumer goods manufacturing companies in Nigeria. The implications of this result is that when the audit technique involves the use of certain technologies, skill sets, and processes, computer programs, statistics etc. for the exploration, evaluation, and investigation of business operations by the internal auditor is in place, Implementation of strategies to prevent and detect fraudulent transactions and activities in the organization would be effectively achieved. This would be seen in terms of cybersecurity scans to ensure that fraud factors are reduced. The findings here are in consonance with earlier studies of (Lillard, 2021; Agymang, 2020; Jezovita et al., 2018; Onoja & Usman, 2015) whose study results indicated that internal audit practices have significant effect on fraud prevention across different firms in different nations.

## 5. CONCLUSION AND RECOMMENDATIONS

This study was carried out to assess the relationship between Analytical internal audit technique and cyber security scan of fraud control in listed consumer goods firms in Nigeria. Based on the findings made, the study concludes that Analytical technique has a strong, positive and significant relationship with Cybersecurity scans method of fraud control in listed consumer goods firms in Nigeria. The study thus recommended that:

(i) Management of listed consumer goods firms should adopt the analytical internal audit technique in addition to their traditional audit technique so that fraud control measures would be effective in tackling fraud
(ii) Fraud control measures such as cybersecurity scans among others should be adopted by the firms as a way of fraud prevention
(iii) There should be regular review and checking of IT systems, servers and other ICT to ensure that controls are in place and vulnerability to use as means of fraud are controlled
(iv) Management should ensure that the internal auditors acquire the requisite techniques and skills in computer operations and electronic data and other digital systems that enhances audit exercise specially to enable them able to carry out analytical procedures.

## Contribution to Knowledge

This research has contributed to knowledge in the following: It provided understanding on the importance of adequate and effective use of Analytical internal audit technique for audit activities towards fraud control within the private sector firms as can be seen in terms of conducting cybersecurity scans, This is novel to the developing nation's context, thus corroborating the calls by international communities that developing nations should embrace contemporary audit techniques including the use of ICT for audit practice that could ensure effectiveness of audit activities that could enhance controls and thus checkmate fraudulent activities in firms and businesses.

# REFERENCES


1. Adeleke, O. K., Segun, Ilugbusi B., & Olaoye, A. C. (2020). Impact of internal control on fraud prevention in deposit money banks. Nigerian Studies in Economics and Management Sciences, 2(1), 42–51.
2. Agwor, T.C. (2017). Fraud prevention and business performance in quoted manufacturing companies in Nigeria. European Journal of Accounting Auditing and Finance Research,5(9), 71-80.
3. Agyemang, K..J. (2020). Internal control and fraud prevention. International Journal of Scientific Research & Management Studies, 1-11
4. Appelbaum, D., & Kogan, A. (2017). Big data and analytics in the modern audit engagement: Research needs. Auditing: A Journal Of Practice & Theory, 36(4),1-27.
5. Clark, M., & Harrell, C.E. (2013). Unlike chess, everyone must continue playing after a cyber-attack. Journal of Investment Compliance, 14(4), 5–12.
6. Da Veiga, A (2016). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. Paper Presented at the Science and Information (SAI) Computing Conference, London, UK, July 13–15, 1006–1015.
7. Da Veiga, A. (2016). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. Paper Presented at the Science and Information (SAI) Computing Conference, London, UK, July 13–15, 1006–1015.
8. Egbunike, P. A. & Egbunike, F.C. (2017). An empirical examination of challenges faced by internal auditors in public sector audit in south-eastern Nigeria. Asian Journal of Economics, Business and Accounting, 3(2), 1-13.
9. Gallagher, B. (2022, April 27). The five types of testing methods used during audit procedures. Online at https://www.ispartnersllc.com/blog/five-types-testing-methods-used-audits/
10. Hamilton, D., & Gabriel, J. (2012). Dimensions of fraud in Nigeria quoted firms. Am J Soc Mgmt Sci 3(3), 112-120.
11. Hayes, R., Schilder, A., Dassen, R.,& Wallage, P. (2000). Principles of auditing: An international perspective. McGraw-Hill Publishing Co.
12. Hayes, R., Schilder, A., Dassen, R.,& Wallage, P. (2005). Principles of auditing: An international perspective. Revised edition. McGraw-Hill Publishing Co.
13. Hui, K., Kim, S.H., & Wang, Q (2017). Cybercrime deterrence and international legislation: Evidence from distributed denial of service attacks. MIS Q. 41(2), 497–572.
14. Humaidi, N., & Balakrishnan, V. (2018). Indirect effect of management support on users' compliance behaviour towards information security policies. Health Information Management Journal, 47(1), 17–27.
15. Institute of Internal Auditors (2009). Definition of internal auditing code of ethics international standard for professional practice of internal auditing. Institute of Internal Audit Publications, 233-240.
16. International Standards for Professional Practice of Internal Auditing (2002). Report of International Standards for Professional Practice of Internal Auditing Florida: The Institute of Internal Auditors.
17. Ježovita, A., Tušek, B., & Žager, L. (2018). The state of analytical procedures in the internal auditing as a corporate governance mechanism. Journal of Contemporary Management Issues, 23(2),15-46
18. Kent, C., Tanner, M., & Kabanda, S. (2016). How South African SMEs address cyber security: the case of web server logs and intrusion detection. Paper Presented at the IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech), Balaclava, Mauritius, August 3–6, 100–105.
19. Klimburg, A. (2012). National cyber security framework manual. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn
20. Li, H., Dai, J., Gershberg, T., & Vasarhelyi, M. A. (2018). Understanding usage and value of audit analytics for internal auditors: An organizational approach. International Journal of Accounting Information Systems, 28, 59-76.
21. Lillard, M. (2021, October 5). Fraud control and prevention: Mastering the basics. Manager, risk & advisory services, GRF, online at https://www.grfcpa.com/2021/10/fraud-control-and-prevention-mastering-the-basics/
22. Manhart, M., & Thalmann, S. (2015). Protecting organizational knowledge: A structured literature review. Journal of Knowledge Management, 19(2), 190–211.

23. Nyakarimi, S. N., Kariuki, S. N., & Kariuki, P. W. (2020). Application of internal control system in fraud prevention in banking sector. International Journal of Scientific and Technology Research, 9(3), 6524–6536.
24. Ogundana, O., Okere, W., Ogunleye, O., & Oladapo, I. (2018). Forensic Accounting and fraud prevention and detection in Nigerian banking industry. Reviews & Research, 1(1), 34-55
25. Ogwiji, J., & Lasisi, I.O. (2022). Internal control system and fraud prevention of quoted financial services, firms in Nigeria: A Smart PLS-SEM Approach, European Journal of Accounting, Auditing and Finance Research, 10(4), 1-13
26. Okoye, E. I., & Gbegi, D. O. (2013). Forensic accounting: A tool for fraud detection and prevention in the public sector: a study of selected ministries in Kogi state Nigeria, International Journal of Academic Research in Business and Social Sciences, 3(3), 34-57.
27. Okoye, E., & Ndah, E.W. (2019). Forensic accounting and fraud prevention in manufacturing companies in Nigeria. International Journal of Innovative Finance and Economics Research, 7(1), 107-116.
28. Onespan (2021). What is Fraud? Online at https://www.onespan.com/topics/fraud-prevention
29. Onoja, E., & Usman, H. (2015). Internal Audit Techniques and Fraud Prevention: A case study of selected local government councils in Bauch State Mediterranean Journal of Social Sciences MCSER Publishing, Rome-Italy, 6(4), 232-244
30. Ordu, P.A., & Abowei, U.N. (2021). Forensic accounting, electronic accounting and fraud checkmating by financial professionals: A critical review. Journal of Forensic Accounting & Fraud Investigation (JFAFI),6(1), 104 – 120. A publication of the Association of Forensic Accounting Researchers (AFAR) A member of International Association of Accounting Education and Research (IAAER).
31. Ordu, P.A., Chukwu, G.J., Namapele, A., & Barigbon, M. (2019). Audit planning in contemporary organisation: Issues of great importance. International Journal of Business & Law Research 7(3), 37-41, July-Sept.,.
32. Osazefua, I.J. (2019). Operational efficiency and financial sustainability of listed manufacturing companies in Nigeria. Journal of Accounting and Taxation, 11(1), 17-31.
33. Pereira, T., & Santos, H. (2010). A security audit framework to manage information system security. In Tenreiro de Magalhães, S., Jahankhani, H., Hessami, Ali G. (eds.) ICGS3 2010. CCIS, 92, 9–18. Springer, Heidelberg . https://doi.org/10.1007/978-3-642-15717-2_2
34. Pieters, W., Hadžiosmanović, D., & Dechesne, F. (2016). Security-by-experiment: lessons from responsible deployment in cyberspace. Sci. Eng. Ethics 22(3), 831–850.
35. PricewaterhouseCoopers Risk Services Ltd. (2018). State of the Internal Audit Profession. online at https://www.pwc.com/sg/en/publications/assets/state-of-the-internal-audit-2018.pdf
36. PWC (2018). Revitalizing privacy and trust in a data-driven world: Key findings from the global state of information security, survey 2018. https://www.pwc.com/us/en/cyber security/assets/revitalizing-privacy-trust-in-data-driven-world.pdf.
37. Ramamoorti, S., & Olsen, W. (2007). Fraud: The human factor. Financial Executive, 53-55.
38. Ramaswamy, V. (2007). New frontiers: Training forensic accountants within the accounting program. Journal of College Teaching & Learning, 4(4), 31-38.
39. Reason, J. (2016). Managing the risks of organizational accidents. Routledge.
40. Safa, N.S., & Von Solms, R. (2016). An information security knowledge-sharing model in organizations. Computer. Hum. Behaviour. 57(4), 442–451.
41. Saleh, M. (2016). Effect of internal control on fraud prevention of the manufacturing industries in Maiduguri Nigeria: https://www.researchgate.net/publication/320434522
42. Shah, M.H., Muhammad, R., & Ameen, N. (2020). Cybersecurity readiness of E-tail organisations: A technical perspective. Published by Springer Nature Switzerland AG, LNCS 12066, 153–160. https://doi.org/10.1007/978-3-030-44999-5_13
43. Sharma, A., Kansal, V., & Tomar, R. (2015). Location based services in M-commerce: Customer trust and transaction security issues. Int. J. Comput. Sci. Secur. (IJCSS) 9(2), 11–21.
44. Shinde, P.S., & Ardhapurkar, S.B. (2016). Cyber security analysis using vulnerability assessment and penetration testing. Paper Presented at the World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), Coimbatore, India, 29 February–1 March, 1–5.
45. Silverstone, H., & Sheetz, M. (2007). Forensic accounting and fraud investigation for non-experts, Second edition. Wiley.
46. Tang, F., Strand Norman, C., & Vendrzyk, V. P. (2017). Exploring perceptions of data analytics in the internal audit function. Behaviour & Information Technology, 36(11), 1125-1136.
47. Tang, F.T.C., Guo, Z., Cahalane, M., & Cheng, D. (2016).: Developing business analytic capabilities for combating e-commerce identity fraud: A study of Trustev's digital verification solution. Information Management, 53(7), 878–891
48. Taylor, E. (2016). Mobile payment technologies in retail: A review of potential benefits and risks. Int. J. Retail Distrib. Manag. 44(2), 159–177.

49. The Institute of Internal Auditors. (2016). The International professional practices framework (IPPF). The International Standards for the professional practice of internal auditing. Online at https://na.theiia.org/standardsguidance/Public%20Documents/IPPFStandards-2017.pdf
50. The Institute of Internal Auditors. (2018).The international professional practices framework (IPPF). Implementation Guidance. Online at https://na.theiia.org/standards-guidance/Member%20 Documents/2017-Implementation-Guides-ALL.pdf
51. Udoayang, J., & James, F. (2004). Auditing and investigation. University of Calabar Press, Calabar.
52. Uma, M., & Padmavathi, G. (2013). A survey on various cyber-attacks and their classification. IJ Netw. Secur. 15(5), 390–396.
53. Waly, N., Tassabehji, R., & Kamala, M. (2012). Improving organisational information security management: the impact of training and awareness. Paper Presented at the High Performance Computing and Communication & IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICESS), Liverpool, UK, June 25–27, 1270–1275.

**CITE AS**
Promise Akor ORDU, Prof. Sam A.OTAMIRI, & Cletus O.AMAH. (2023). Analytical Internal Audit Techniques and Cyber security Scans of Fraud Control: Evidence from Nigerian Listed Consumers Goods Firms. Global Journal of Research in Business Management, 3(1), 1–15. https://doi.org/10.5281/zenodo.7555473