



Association of Chief Audit Executives of Banks in Nigeria

Design+printbyProwess08039221516

ACAEBIN

Plot 1398B, Tiameyi Savage Street, Victoria Island, Lagos.
Office Line: +234-1-3424805
E-mail: info@acaebin.org
website: www.acaebin.org



Eagle Eye

A Quarterly Publication of the Association of Chief Audit Executives of Banks in Nigeria (ACAEBIN) Q2, 2023



Auditing the Internal Auditors, Helping to Measure the Internal Audit Effectiveness and Efficiency

Fraud Control And Prevention As An Investment ...
Page 25

Wellness
7 Natural ways to reduce your blood sugar level.
Page 17

PCI DSS Certified
Page 27
What Auditors Should Know About The Payment Card ...

ACAEBIN EXCO MEMBERS



Felix Igbinosa
Chairman



Prince Akamadu
1st Vice Chairman



Aina Amah
2nd Vice Chairperson



Gboyega Sadiq
Treasurer



Adekunle Onitiri
Auditor



Ugochi Osinigwe
Chairperson Research & Publication



Mogbitse Atsagbede
Chairman Payment & Systems



Olusegun Famoriyo
Ex-officio I



Femi Fatobi
Ex-officio II

CONTENT

4	Auditing the Internal Auditors, Helping to Measure the Internal Audit Effectiveness ...	21	Investigating Money Laundering Schemes and Techniques
10	The Future of Auditing: How Technology is Changing the Audit Profession	25	Fraud Control And Prevention As An Investment In The Long Run
13	How Internal Audit Can Help Improve Bank's Profitability	27	What Auditors Should Know About The Payment Card ...
16	7 reasons you should drink warm water daily.	30	Cybersecurity and its Impact on Financial Institutionsmitigating Fraud Risks



Editorial

It is with great pleasure that I welcome you to the 2nd quarter 2023 edition of your flagship professional publication, the Eagle Eye, especially as we step into the third quarter of the year. In keeping faith with our standard and tradition, this edition presents a collection of articles that will not only educate you but enlighten and entertain you. Our cover article 'Auditing the Internal Auditors, Helping to Measure the Internal Audit Effectiveness And Efficiency', highlights the need for the review of the Internal Audit Function as a performance enabler for business growth, cost savings and long-term sustainability by identifying gaps, optimizing resources and maximizing service delivery quality against the recommended standards by the global Body of Knowledge, the Institute of Internal Auditors namely: IIA International Professional Practice Framework (IIA IPPF Standard), IIA Internal Audit Capability Maturity Model (IIA IC-MM) and IIA Audit Intelligent Suite (Formerly Gains Benchmarking Survey Study).

The article, the Future of Auditing: How Technology is Changing the Audit Profession discusses how internal audit is leveraging on technology and the future of audit with emphasis on financial auditing. Also, there is a piece on how internal auditors can help improve the bottom line of banks titled 'How Internal Auditors can help improve bank's profitability'.

Money laundering is a global menace and as governments all over the world continue to grapple with how to address this malaise, our article on 'Investigating

Money Laundering Schemes and Techniques' will offer some insight while the article on 'Fraud Control and Prevention as an Investment in the Long Run', discusses the benefits of continuous investment in fraud prevention tools by banks and other organizations. As cashless policy continues to gather momentum across Africa and globally, driven by the payment card industry, etc., our article on 'What Auditors Should Know About The Payment Card Industry Security Standards Council's (PCI DSS) Evolutions' looks at the security, risks and the features of the PCI DSS version 4.0 as against previous versions. The Financial Services sector is increasingly becoming digitized which was exacerbated by the Covid-19 pandemic, the importance of robust cybersecurity measures by banks cannot be overstated. Our article on 'Cybersecurity and its Impact on Financial Institutions Mitigating Fraud Risks' focuses on the implications of weak cybersecurity systems and suggested 20 practical ways to mitigate cyber-attacks.

Concluding our array of rich and interesting Q2 edition is our usual journey to maintaining a healthy and wealthy lifestyle with two articles titled '7 Reasons Why You Should Drink Warm Water' and '7 Natural Ways to Reduce Your Blood Sugar Level' after all, health, they say, is wealth. More importantly, do not flip past the well-researched keynote address delivered by the President/Chairman of Council, Chartered Institute of Bankers of Nigeria (CIBN), Dr Ken Opara during the Association's 2022 Annual General Meeting held recently in Lagos.

What an interesting Quarter two it has been, sit back and enjoy our ala carte. See you in September.

Ugochi Osinigwe
Editor-in-Chief

Reader's Comments: kindly send your comment/feedback to info@acaebin.org

Members of Research and Publication Committee

Ugochi Osinigwe (Fidelity Bank, Chairperson)	Olusemore Adegbola (Nigeria Mortgage Refinance Company)
Prince Akamadu (Union Bank of Nig. Plc)	Lydia I. Alfa (Central Bank Nigeria, Advisory)
Daniel Olatomide (Bank of Agriculture)	Emeka Owoh (Citibank Nigeria Limited)
Awe Adeola (Coronation Merchant Bank Ltd.)	Aina Amah (ProvidusBank Limited)
Femi Fatobi (Rand Merchant Bank Nig. Ltd)	Rotimi Omotayo (Polaris Bank Plc)
Abiodun Okusami (Keystone Bank Ltd.)	Edward Onwubuya (Sterling Bank Plc)
Ayaghena R. Ozemede (NEXIM Bank)	Joshua Ohioma (Development Bank of Nig)
Musefiu R Olalekan (Jaiz Bank Plc)	Yemi Ogunfeyimi (Bank of Industry Limited)
Dare Akinnoye (FSDH Merchant Bank Ltd.)	Dr. Romeo Savage (FBNQuest Merchant Bank Limited)
Sadiku O. Kanabe (The Infrastructural Bank Plc)	Rasaq Alawode (Greenwich Merchant Bank Ltd)
Soridei Akene (Heritage Bank Plc)	Dumebi Okwor (Premium Trust Bank Limited)
Olusegun Famoriyo (Unity Bank Plc)	



Auditing the Internal Auditors, Helping to Measure the Internal Audit Effectiveness and Efficiency

Every organization hires for expertise and the expertise comes into play in the quality of work products, impacts and contributions to the achievement of the overall corporate goals and objectives. The Internal Audit function is a performance enabler for business growth, cost savings and long-term sustainability by identifying gaps, optimizing resources and maximizing service delivery quality.

The performance of the internal audit function in carrying out this job function needs to be periodically measured against best practices, standards and the specific criteria established by the organization. The primary goals for the measurements are to identify areas of strengths, weaknesses, improvement opportunities and proactively take appropriate actions towards addressing the weaknesses, reinforcing the strengths and optimizing the improvement opportunities.

The three different standards recommended by the Institute of Internal Auditors (IIA) to be applied to conduct the assessment are:

- IIA International Professional Practice Framework (IIA IPPF) Standard). Please note that the current IIA IPPF 2017 is undergoing transformation. The public comments to the draft exposures were closed at the end of May 2023. Once the final release copy has been published, this my blog post will be updated to reflect the changes.
- IIA Internal Audit Capability Maturity Model (IIA IC-MM).
- IIA Audit Intelligent Suite (Formerly Gains Benchmarking Survey Study).

Each of these quality measurement standards and tools provides specific focus areas to be reviewed and analyzed, about the internal audit function, so as to gain robust insight into what the internal audit service delivery is at each of the focus areas and provide at the aggregate level, the bigger picture of the overall performance. The focus areas covered by the reviews are generally grouped under five key elements namely: Structure, Strategy, System, Staffing and Style.

These elements are reviewed to establish the value protection, addition, impacts and contributions of the internal audit function. The key performance indicators assessed are:

- Extent of alignment of the internal audit function with the overall corporate goals and objectives
- Quality of Risk management a
- Quality of Staff optimization and development
- Quality of Stakeholders engagement, relationship management, general perceptions of the internal audit function and perspectives for the future.
- Quality of Cost management and savings
- Extent of leveraging digital technologies for innovations and creativity
- Quality of customer service delivery
- Quality of reporting and communication across all levels of the organization
- Quality of continuous improvement programs for business continuity

IIA recommended the reviews to be done in three stages namely Continuous assessment. Periodic internal assessment and Five-year Cycle Independent External Assessment.

The **Continuous assessment** is done on an ongoing basis through self-and peer reviews done by the internal audit staff and regular feedbacks received from auditees on the completion of audit engagements.

The **Periodic internal assessment** is done regularly based on the cycle determined by the business or the internal audit function for example annually. Internal assessments are done by a dedicated in-house quality assurance team outside the internal audit function.

The **Independent external assessment** is done every five years and should be done by a qualified external assessor from outside the organization. Most external independent assessments come with big surprises of findings about the internal audit operations and lots of pushback from the internal audit function. The internal assessment is critical because it helps the internal audit function to avoid or minimize big surprises and conserve the energies and efforts expended in pushbacks. The internal assessment helps the internal audit function to achieve the following:

- be well prepared for their job with the required knowledge, skills and experiences,
- proactively identify the gaps, strengths and improvement opportunities within the internal audit operations and take appropriate actions to address the issues quickly,
- have constructive engagement with the senior management, executives, board committees and independent external assessors.

Experience has shown that most of the external quality assessments come with big surprises to the internal audit function, because of the failure of the internal audit to conduct internal self-assessment of its activities. The major contributing factor is knowledge gap of the right standard best practices, methodology and reporting styles. To avoid these surprises, the internal audit function should ensure that the internal assessment is done on a more regular basis to help them achieve.

Completing the internal and external independent assessments requires completing the following eight specific activities:

- Phase 1 - Engagement planning
- Phase 2 - Validation of the business needs and stakeholders' expectations.
- Phase 3 - Current state/AsIs status assessment
- Phase 4 - Root Cause Analysis
- Phase 5 - Reporting and stakeholders' presentation
- Phase 6 - Development of Implementation Road Map
- Phase 7 - Implementation support
- Phase 8 - Post implementation support

The key deliverables from the internal audit quality assessment reviews are generally driven by the primary objectives for the reviews, the business needs and expectations of the stakeholders. Listed below are some of the most common key deliverables in the industry:

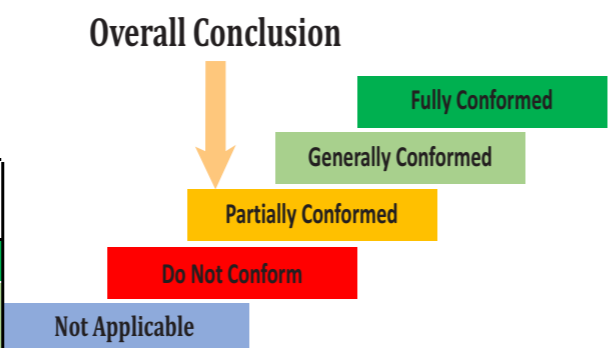
- Project plans and communication protocols
- Business Needs Analysis and Stakeholder expectations.

Detailed findings and executive summary reports aligned with the review focus areas prescribed by the different quality measurement standards and tools deployed in the reviews. Generally, the report should highlight the Stakeholder's perceptions of the internal audit function and perspectives for the future, Conformance to the IIA IPPF, Current and target maturity levels in the IIA Internal Audit Capability Maturity Model and Comparison positions with the IIA Audit Intelligence Suite/GAINS Benchmarking Survey Study).

Presented below are the specific focus areas to be reviews within each of the standards and nature of assessment results					
Institute of Internal Auditors International Professional Practice Framework (IPPF) - 2017 (Standards) Assessment Criteria					
Sections of IIA IPPF 2017 Standards	Total Number Per Compliance Status				
	Fully conformed	Generally Conformed	Partially Conformed	Do Not Conform	Not Applicable
1000 – Purpose, Authority, and Responsibility					
1200 – Proficiency and Due Professional Care					
1300 – Quality Assurance and Improvement Program					
2000 – Managing the Internal Audit Activity					
2100 – Nature of Work					
2200 – Engagement Planning					
2300 – Performing the Engagement					
2400 – Communicating Results					
2500 – Monitoring Progress					
2600 – Communicating the Acceptance of Risks					

Assessment Results

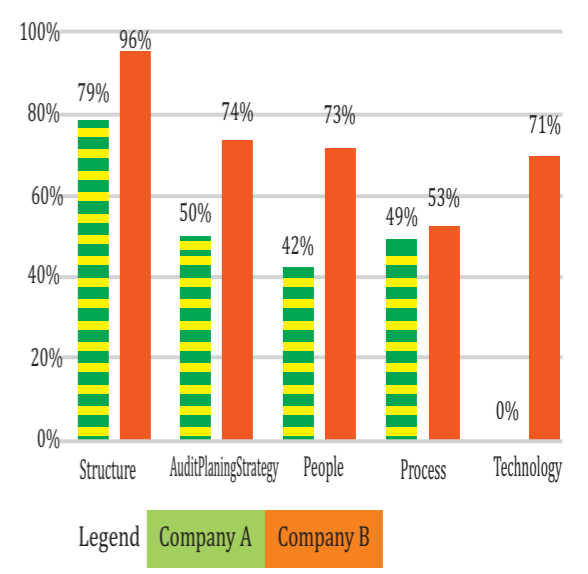
Conformance Status	Number of Standards Tested
Fully Conform (FC)	
Generally Conform (GC)	
Partially Conform (PC)	
Do Not Conform (DC)	
Not Applicable (NA)	
Total	



Benchmarking Criteria

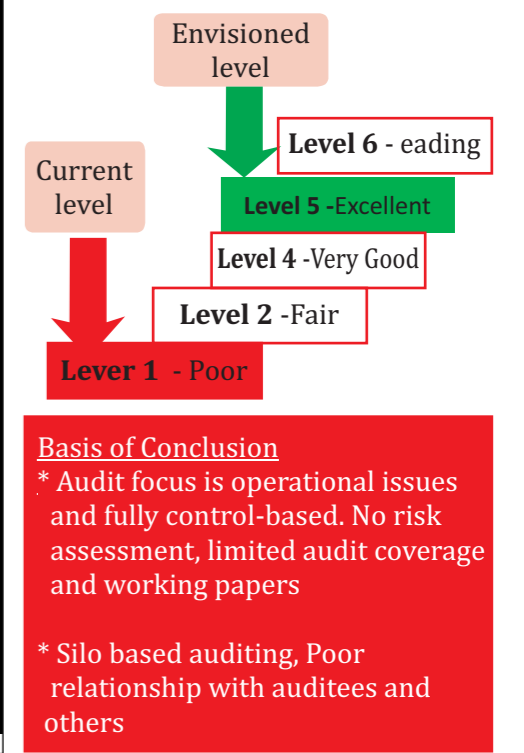
- Structure**
* Roles, Responsibilities, Authority & Independence of IAD
- Strategy**
* IAD Planning Drivers and Horizon
- Process**
* Audit field work execution, reporting, issues monitoring and quality assurance processes
- People**
* Recruitment Strategy and experience of IAD staff
- Technology**
* Existence of use of technology to automate audit management processes end-to-end

Assessment Results



High Level Summary - IIA Internal Audit Capabilities and Performance Levels	
Key Focus Areas	Key elements considered
Services and Role of Internal Auditing	Enablers for the provision of independent and objective assurance and advisory
People Management	Enablers for people management and development to perform to the best of their abilities.
Professional Practices	Audit strategy, processes, policies and practices enabling alignment of internal audit work products with key business risks and overall corporate goals and objectives
Performance Management and Accountability	Financial metrics and other indicators for monitoring and measuring internal audit performance against targets
Organizational Relationships and Culture	Information communication and stakeholders engagements
Governance Structures	Administrative and functional Reporting levels

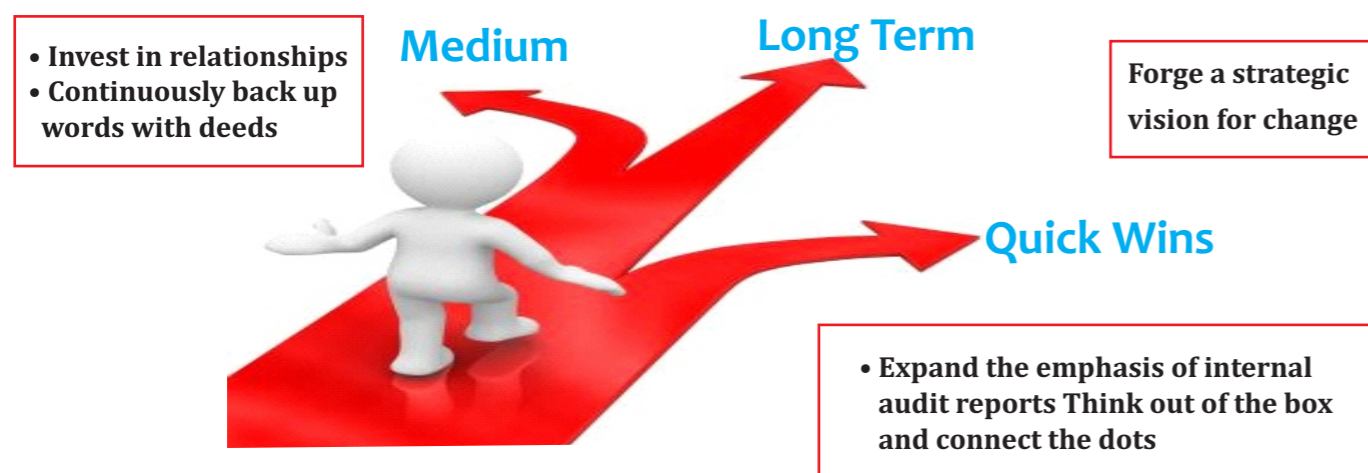
Assessment Results



Stakeholders Perceptions and Perspectives Assessment Criteria	
Focus Areas	Key Elements Assessed
Business Impact (Quality of Service Delivery, Value Protection & Additions)	Focus on Critical Risks & Issues that matter
	Stakeholders Engagement
	Business Continuity
	Cost-Effective Service Delivery/result oriented culture
	Integrity
	Trust
Stakeholder Communication (Stakeholders Engagement & Relationship Management)	Enabling a Client Service Culture -
	Risk Reporting Quality
	Conviction
	Confidence
	Respect, Interpretation & Listening
	Robust mandate, Policies, Processes & Procedures
Strategic Positioning (Knowledge of the Business Leading Practices)	Matching Talent model to value proposition
	Business Acumen,
	Knowledge of the business
	Visibility & Influence & Presence
Visioning (Adaptability to Change)	, Risk Management & Assurance Knowledge
	Robust mandate, Policies, Processes & Procedures
	Use of Technology
	Research oriented - skeptical mindset, thinking out of the box, analytical mindset
	Strategic Planning & Thinking



High Level Summary of the Recommendations for Improvements



Is the quality assessment of the internal audit function mandatory in Nigeria?

Yes, the quality assessment of the internal audit function is mandatory for all the Public Limited Liability Companies (PLC) and Public Interest Entities in Nigeria as prescribed by the Nigerian National Code of Corporate Governance (NCCG) 2018 principle 18.6 and the NGX (formerly Nigerian Stock Exchange/NSE) Corporate Governance Guidelines (NGX CCG). The NCCG (2018) and NGX CCG require that the Internal Audit Functions

should adhere to the IIA standards and that the independent external assessment should be done every three years and reports submitted to the NGX and Financial Reporting Council of Nigeria (FRC).

Other categories of companies regardless of size can benefit from the internal audit quality assessments as it enables them to embed internal audit best practices in their operations.

Do the other Assurance functions such as Internal Control, Risk Management and Compliance need quality assessment to be performed on their functions?



Yes, all assurance providers from the first line to the third lines of defense need to be measured based on the same quality measurement principles adopted for the internal audit function. The second and third lines of assurance functions are already covering the performance assessment of the first line of defense through continuous risk and control monitoring and periodic audit activities. However, the second line and third lines are the most neglected, particularly in the area of internal and external assessments. External assessments are mostly driven by mandatory regulatory compliance requirements and when done, they are mostly by ticking the box approach. The major difference between the conduct of quality assessment on the internal audit function and that of the other assurance functions in the second and third lines is the applicable quality measurement standards and tools deployed.

The quality measurement principles, standards and tools for assessing the performance of the internal control function have been prescribed by the COSO

Internal Control) (COSO IC) Integrated Framework while for conducting the Enterprise Risk Management Function is the COSO Enterprise Risk Management Framework (COSO ERM) or COSO Enterprise Risk Management Framework Integrated with Strategy (COSO Strategy). The ISO 31000 Enterprise Risk Management Standard (ISO 31000) is another quality measurement standard that can be deployed to conduct ERM function performance assessment. The COSO ERM framework was introduced in 2014 and updated in 2017 as COSO Strategy. Although the use of COSO Strategy appears better since it is an upgrade of the COSO ERM, organizations have a choice to choose what they use but articulate the business case for the decision.

The ISO 37301 (previously ISO 19600:2014) is the common standard that is globally used for conducting quality assessments of the Ethics and Regulatory Compliance function. The performance assessment of the Compliance function is more demanding and wider in scope due to the many different legal and regulatory frameworks and standards required to cover a typical good compliance universe such as the Anti-Money Laundering, Counter Terrorism Financing (AML/CT), Anti-Bribery and Corruption (ABC) standards.

The ISO 3701 is applicable only to assess the performance of the Compliance function at the enterprise level and during the review, the quality assessor will obtain high-level information on how the Compliance function is managing the organization's regulatory exposures such as money laundering, terrorism, bribery and corruption risks, reviewing certain reports and asking questions. A separate comprehensive performance assessment can be done specifically for each of the legal and regulatory compliance areas contained in the Compliance Universe such as the AML/CTF or ABC using the specific standards for the area. The frequency of the external assessment reviews for the compliance function and the specific industry focus areas are driven by regulations while the internal assessment is driven by the company's preferences and priorities.

Sally Ogwo Okey-Umahi (MlD, Author, Speaker)
Executive Director, Platinum Edge Consulting



The Future of Auditing: How Technology is Changing the Audit Profession

Auditing is a vital function in the world of finance and accounting.

The auditing process has been around for centuries, and it has evolved significantly over the years. Technology has played a significant role in the evolution of auditing and will continue to shape the future of the audit profession. This article will discuss how technology is changing the audit profession, the benefits and challenges of technology, and the future of auditing with emphasis on financial auditing.

Overview of the Audit Profession:

The audit profession is responsible for ensuring the accuracy and reliability of financial information presented by companies. The audit process involves examining a company's financial statements and systems of internal control, risk management and governance to identify misstatements, errors, or the risks of fraud with material impact on the organization. The audit profession is highly regulated,

and auditors must follow strict guidelines and standards. Auditors must ensure their integrity is not in doubt, apply professional competency in carrying out their job, abide to the principle of confidentiality and maintain independence to ensure that their objectivity is not impaired.

The Role of Technology in Auditing:

Technology has significantly impacted the audit profession over the years. In the past, auditors used manual methods to review financial statements, which were time-consuming and prone to errors. With the advancement of technology, auditors can now use software to automate the audit process and identify potential issues more efficiently.

Audit software can perform various functions, including data analysis, fraud detection, and risk assessment. It can also help auditors track and manage their work, making the audit process more efficient. Audit software can also be used to identify

trends and patterns in financial data, which can help auditors identify potential issues before they become significant problems.

Benefits of Technology in Auditing:

Technology has several benefits for auditors and companies. Some of these benefits include:

1. **Increased Efficiency:** Technology has made the audit process more efficient by automating many manual tasks. This saves time and reduces the risk of errors.
2. **Improved Accuracy:** Audit software is more accurate than manual methods, reducing the risk of errors and ensuring that financial statements are reliable.

manually, such as data entry, account reconciliation, and financial statement analysis. This automation has not only reduced the risk of errors but has also made the auditing process faster and more efficient.

6. **Enhancing Data Analysis:** Another significant impact of technology on the auditing profession is the ability to analyze large amounts of data quickly. Auditors can now use data analytics tools to examine data sets, identify trends and patterns, and perform more in-depth analysis than was previously possible. This enhanced data analysis has made it easier for auditors to identify potential issues and irregularities in financial statements.
7. **Increasing Collaboration:** Technology has also made it easier for auditors to collaborate with



3. **Increased Transparency:** Technology has made it easier for auditors to communicate with clients, increasing transparency and ensuring everyone is on the same page.
4. **Enhanced Fraud Detection:** Audit software can identify potential fraudulent activities, helping auditors detect and prevent fraud.
5. **Automating Manual Tasks:** One of the most significant impacts of technology on the auditing profession is the automation of manual tasks. With the use of advanced software applications and data analytics, auditors can now automate several tasks that were once performed

each other and with their clients. With the use of cloud-based applications, auditors can share documents and data in real-time, regardless of location. This has made it easier for audit teams to work together, even when they are located in different parts of the world.

8. **Enhancing Audit Quality:** Finally, technology has also significantly impacted the quality of audits. With advanced software applications and data analytics, auditors can now perform more in-depth analysis, identify potential issues and irregularities in financial statements, and provide more comprehensive audit reports. This enhanced audit quality has improved the

reliability and credibility of audits.

Challenges of Technology in Auditing:

While technology has several benefits, it also presents some challenges. Some of these challenges include:

1. **Dependence on Technology:** Auditors may become too reliant on technology, which can lead to errors if the software is not used correctly.
2. **Cost:** Audit software can be expensive, making it challenging for smaller firms to invest in the technology.

role in auditing. AI can be used to automate tasks such as data entry and analysis, reducing the risk of errors and increasing efficiency. AI is also transforming the audit profession, enabling auditors to leverage machine learning algorithms to identify patterns in financial data and make more accurate predictions. AI-powered tools can also help auditors to identify areas of risk and suggest ways to mitigate them.

4. **Greater Focus on Cybersecurity:** As technology becomes more prevalent in auditing, firms will need to invest more in cybersecurity measures to protect their data from cyber threats.



3. **Security:** Audit software contains sensitive financial information, making it a target for hackers. Firms must invest in robust cybersecurity measures to protect the data.

The Future of Auditing:

Technology will continue to shape the future of the audit profession. Some of the potential changes include:

1. **Increased Automation:** As technology advances, auditors will rely more on automation to perform routine tasks. This will free up auditors to focus on higher-level tasks such as analysing financial data and identifying potential issues.
2. **Greater use of Data Analytics:** Data analytics will become increasingly crucial in auditing. Auditors will use software to analyse large sets of financial data and thus help identify patterns and trends that will provide evidence for forming an opinion.
3. **Integration of Artificial Intelligence (AI):** Artificial intelligence will play a more significant

5. **Blockchain:** Blockchain technology is making it possible to create more secure and transparent financial systems. Auditors can use blockchain technology to verify the accuracy and integrity of financial data and to ensure that transactions are recorded accurately and securely.

6. **Cloud computing:** Cloud computing enables auditors to work more collaboratively and efficiently, regardless of their physical location. Cloud-based audit tools allow auditors to work together in real-time, share documents and information securely, and access data from anywhere in the world.

Conclusion:

Technology is transforming the audit profession, making it more efficient, effective, and collaborative. While technology cannot replace the human judgment and expertise of auditors, it can help auditors to work more effectively and provide better insights into the financial health of the companies they are auditing.

*Onwuemele Sunday Emeke CFE
Team Member Head Office Audit
United Bank for Africa Plc*



How Internal Audit Can Help Improve Bank's Profitability

An internal audit is an independent assessment of a bank's internal controls, policies, and procedures. The primary objective of an internal audit is to evaluate and improve the effectiveness of the bank's operations, risk management, and governance processes. An internal audit function is a critical component of a bank's corporate governance framework, which ensures that the bank operates in compliance with applicable laws, regulations, and ethical standards.

An effective internal audit function helps banks to enhance their profitability in several ways. Internal audit can play a critical role in improving bank profitability by identifying and addressing potential risks and inefficiencies in the bank's operations. Here are some specific ways internal audit can contribute to improving bank profitability:

- **Identifying revenue opportunities:** Internal audit can review the bank's products and services, identifying areas where the bank can generate additional revenue. By identifying revenue opportunities, the bank can increase its revenue streams, which can improve profitability.
- **Ensuring regulatory compliance:** Internal audit can ensure that the bank is complying with all relevant regulations, avoiding fines and penalties that can impact profitability.
- **Identifying and mitigating operational risks:** Internal audit can help identify potential risks in the bank's operations and make recommendations for mitigating those risks. By reducing operational risks, the bank can avoid costly errors and losses, which can improve profitability.
- **Enhancing internal controls:** Internal audit can review and assess the bank's internal control systems, ensuring that they are effective in mitigating risks and preventing fraud. By enhancing internal controls, the bank can reduce the likelihood of losses due to fraud or error, which can also improve profitability.

Improving efficiency: Internal audit can identify inefficiencies in the bank's processes and operations, recommending changes to improve efficiency and reduce costs. By streamlining processes and reducing costs, the bank can improve profitability.

- **Identifying revenue opportunities:** Internal audit can review the bank's products and services, identifying areas where the bank can generate additional revenue. By identifying revenue opportunities, the bank can increase its revenue streams, which can improve profitability.
- **Ensuring regulatory compliance:** Internal audit can ensure that the bank is complying with all relevant regulations, avoiding fines and penalties that can impact profitability.

Bank profitability and internal audit are two interconnected aspects that are vital for the success of any financial institution. In today's ever-changing and competitive business environment, banks face numerous challenges that can affect their profitability. Therefore, it is essential for banks to adopt an effective and efficient internal audit function to enhance safety and improve profitability.

Profitability is a critical measure of a bank's financial performance. Banks must generate sufficient profits to cover their operating costs and provide a return on their shareholders' investment. However, banks face several challenges that can impact their profitability, such as interest rate fluctuations, market volatility, credit risks, operational risk issues and regulatory compliance.

In summary, internal audit can help banks improve profitability by reducing risks, enhancing internal controls, improving efficiency, identifying revenue opportunities, and ensuring regulatory compliance.

*Onwuemele Sunday Emeke CFE
Team Member Head Office Audit
United Bank for Africa Plc*

Keynote Address

Keynote Address delivered by the President/ Chairman of Council, the Chartered Institute of Bankers of Nigeria, Ken Opara, Ph.d., FCIB, during the 2022 Annual Retreat and Conference of the Association of Chief Audit Executives of Banks in Nigeria (ACAEBIN) held on Wednesday March 22, 2023, at Movenpick Hotel Ikoyi, Lagos.



Distinguished ladies and gentlemen, it gives me a great honour and pleasure to deliver this keynote address on this auspicious occasion of the 2023 Annual Retreat of the Association of Chief Audit Executives of Banks in Nigeria (ACAEBIN). I am glad to be here with you today and I must say that I always look forward to opportunities such as this, to contribute to conversations especially when it relates to strengthening the performance and stability of the banking industry.

Let me use this medium to commend the Association ably led by Mr. Felix Igbiosa, HCIB, Chairman, Association of Chief Audit Executives of Banks in Nigeria, for the good work you and your team are doing to foster competence, cooperation, collaboration, ethical standards, and professionalism among Chief Audit Executives (CAEs) of banks.

I salute you for your choice of the theme of this engagement, which is “**Keeping up with the NextGen in Internal Audit**”. The theme, I must remark, is apt and timely. As we all know, the business world is rapidly changing as a result of digitization. The Covid-19 Pandemic which ravaged the world in the year 2020 had significant impact on the global economy which led to the accelerated adoption of technological innovation which would have otherwise taken businesses decades to implement. Given this development, all aspects of businesses were subjected to disruptive innovation, including the internal audit function. Furthermore, the emergence of new technologies, changing behaviors of bank customers, changing regulatory requirements, and evolving business models mean that the traditional methods of internal audit may no longer be adequate. Consequently, it is imperative for the twenty-first century Internal Audit professional to continuously stay ahead of the curve to deliver on his/her mandate effectively and efficiently.

So, what does it mean to keep up with NextGen in internal audit?

First and foremost, it means embracing technological advancements. The use of technology in internal audit is no longer controversial, it is the way to go. There are many factors driving the adoption of tech in internal audit including an increase in the volume of data. According to a 2019 report by the ACCA, it is estimated that over 90% of the world's data has been generated since 2016, and significant amounts of it are financial data. Other drivers include a shift towards automation and a change in business models as a result of innovation in technology.

With the increasing use of data analytics, artificial intelligence, automation tools, internal audit professionals must be able to utilize these tools to identify risks and essentially add value to their respective organizations.

In addition, with increased adoption of technological innovations, businesses should in particular be wary of increased cyber threats which has significantly increased since the outbreak of Covid-19 pandemic. For example, according to Businesswire, 81% of global organizations experienced increased cyber threats during COVID-19 and 79% of organizations experienced downtime due to cybersecurity risk during peak season.

Secondly, keeping up with the NextGen in Internal Audit means, having a deeper understanding of the business domain within which a professional auditor operates. To be effective, internal auditors must have a thorough understanding of their organization's strategy, operations, and risk landscape. This means working closely with other functions within the organization, such as Finance, ICT, Risk Management, Compliance and Operations, to gain a holistic view of the business. With this understanding, internal auditors can identify emerging risks and ensure that they are adequately addressed. This puts them at an advantage compared to professionals who have not

invested time to understand the domain within which they operate.

Thirdly, keeping up with the NextGen in Internal Audit means, being adaptable and agile. The ability to respond quickly to changing circumstances is becoming increasingly important in the internal audit profession. Internal auditors must be able to respond quickly to changes in business operations, emerging risks, or changes in regulatory requirements. The ability to work in an agile manner, with a focus on continuous improvement, is becoming an essential skill for NextGen internal auditors. According to PWC, 2018 Tangible results from Agile Auditing have included a 20% time saving on regulatory audits and a 10% time saving on less standard audits.

Recommendations for Internal Audit Professionals

To keep up with the NextGen, the Chief Audit Executive must take note of the following:

- 1. Thorough understanding of the next-generation workforce:** The entrance of the Millennials and Gen”Z”s into the industry requires the Industry and Chief Audit Executive to understand the attitudes, values, and preferences of the workforce of the next generation. This also includes understanding their expectations around technology, collaboration, work life balance, etc. This understanding will help to get the best from them.
- 2. Adoption of emerging technologies:** Technologies like artificial intelligence, robotic process automation, and blockchain are rapidly transforming the business landscape. Internal auditors need to be familiar with these technologies and understand how they can be used to improve audit efficiency and effectiveness. They should be able to analyze large amounts of data, identify patterns and trends, and use data for robust reporting and decision making.
- 3. Staying agile:** Internal auditors need to be agile and able to adapt quickly to changing business needs. This means being flexible and open to new ideas, and willing to learn and develop new skills. It also includes embracing digital transformation and incorporating advanced technologies to automate routine tasks, identify anomalies and patterns, and provide more accurate and timely insights to stakeholders.
- 4. Focus on risk management:** The next generation of internal audit will need to focus more on risk management rather than compliance. With the increased complexity and interconnectedness of business processes, the focus should shift towards pre-mortem analysis, identifying emerging risks, evaluating their potential impact on the

organization, and developing strategies to mitigate them.

- 5. Collaboration:** The next-generation auditors would need to work closely with other units such as IT, Risk Management, Legal department etc. within the organization, to identify and mitigate risks especially cybercrimes. This collaboration should be extended to business stakeholder to understand their priorities and goals, and jointly come up with solutions to global issues that may affect the practice of Internal Audit.
- 6. Training, Upskilling & Continuous Learning:** The internal audit function must have a continuous learning culture. It is important for internal auditors to attend training and developmental programs. As the business landscape is changing digitally and, in all ramifications, the NextGen Auditor must be ahead of the development. This can only be possible through continuous learning.

Ultimately, next generation internal auditing practices should be adopted because while internal controls and risk management practices can help prevent fraud, audits are critical to detecting fraud that may have gone unnoticed by other internal processes. Furthermore, with the increasing complexity of financial transactions and the evolving nature of fraud schemes, traditional audit approaches are no longer sufficient to identify fraud.

Essentially, next generation auditing practices are the last line of defense against fraud in a bank and technological advancements are needed to protect organisations against such fraud. Therefore, banks should adopt technological advancements in their audit processes which would make tasks such as analyzing vast amounts of data, real-time monitoring, reduced human error and bias more efficient. By doing so, banks can enhance their ability to detect and prevent fraud, ultimately protecting their customers and shareholders.

Conclusion

In conclusion, beyond the interventions I have proposed which include adopting an innovative mindset, embracing emerging technologies, and collaborating with other functions, internal auditors must deliberately and personally identify initiatives that will make them remain relevant and add value to their organizations as well as the practice of Audit.

Distinguished Ladies and Gentlemen, on this note, I declare this 2023 Annual Retreat and Conference of the Association of Chief Audit Executives of Banks in Nigeria formally open.

I wish you all a successful deliberation.

Thank you and God bless.

7 Reasons you should drink warm Water daily.



Drinking warm water every day on a regular basis can help the body to break down fat deposits, relax muscles, and increase blood flow.

Here are 7 well-researched benefits of warm water;

Helps with digestion: Drinking warm water can help to stimulate digestion by increasing blood flow to the digestive tract. It can also help to break down food particles and make them easier to digest, which can reduce the risk of constipation and bloating.

Boosts metabolism: Drinking warm water can increase your metabolic rate, which can help you to burn more calories throughout the day. This can be especially beneficial for weight loss and weight management.

Reduces pain: Warm water can help to reduce pain and inflammation in the body. It can also help to soothe sore muscles and joints, which can be especially beneficial for people with arthritis or other inflammatory conditions.

Improves circulation: Drinking warm water can help to improve blood flow and circulation throughout the body. This can help to deliver oxygen and nutrients to the cells more efficiently, which can improve overall health and vitality.

Promotes relaxation: Drinking warm water can have a calming effect on the body and mind. It can help to reduce stress and anxiety and promote feelings of relaxation and well-being.

Detoxifies the body: Drinking warm water can help to flush out toxins and impurities from the body. It can also help to improve kidney function and prevent the formation of kidney stones.

Enhances skin health: Drinking warm water can help to improve skin health by promoting hydration and increasing blood flow to the skin. This can help to reduce the appearance of fine lines and wrinkles and promote a healthy, radiant complexion.

allure.vanguardngr.com

7 Natural ways to reduce your Blood Sugar level.



EAT RIGHT: Having a balanced Meal of (Protein, Fat and Carbs) will naturally balance your blood sugar level as it all boils down to nourishing your metabolism so that it can function optimally.

AVOID PROCESSED FOODS: Eating foods high in sugar contributes to blood sugar spikes. When you have that block of chocolate or sugary snack, you push your body to burn sugar for energy, rather than fat, leading to an increase in insulin.

EAT YOUR GREENS: As always, the star of the show is an abundance of leafy green vegetables. B vitamins are especially important for glucose metabolism, so making sure you have enough of these in your diet will help.

LIMIT CAFFEINE & SUGAR: Not overdoing caffeine will not only help regulate your blood

sugar but will also help keep your anxiety in check.

STICK TO A REGULAR EATING SCHEDULE: Eating a well-balanced meal at regular intervals is one of the best and easiest ways to feel better this time.

MANAGE STRESS & GET ENOUGH SLEEP: As much as we know our daily activities can be overwhelming, it is important to try as much to manage stress as well as get sufficient sleep

INCLUDE STRETCHES & WALKS: I understand that we might not have all the time in but it's still important to take time to talk and walk often.

allure.vanguardngr.com

2022 Annual General Meeting of the Association held on March 22, 2023 at Movenpick Hotel, Ikoyi, Lagos



2022 Annual General Meeting of the Association held on March 22, 2023 at Movenpick Hotel, Ikoyi, Lagos



Training on Retirement Plan for Chief Audit Executives held on June 24, 2023 at Federal Palace Hotel, Victoria Island, Lagos



Investigating Money Laundering Schemes and Techniques

Investigating Money Laundering Schemes and Techniques: Unveiling the Veil of Illicit Finance

Money laundering remains a persistent and pervasive global issue, enabling criminals to legitimize and conceal the origins of illicitly obtained funds. The ability to launder money effectively allows criminals to enjoy the proceeds of their illegal activities while evading detection and prosecution. Investigating and understanding the various money laundering schemes and techniques is crucial for combating this illicit practice. This article explores the world of money laundering, its impact on economies and societies, and the methods employed by criminals to launder their ill-gotten gains.

Understanding Money Laundering

Money laundering is the process of transforming "dirty" money acquired through criminal activities into "clean" money that appears legitimate. It involves three key stages: placement, layering, and integration. Placement involves introducing illicit funds into the financial system, often through cash deposits or other means to obfuscate their origins. Layering involves disguising the source of funds through complex transactions, making it difficult to trace their origins.

Finally, integration involves merging the laundered funds with legitimate assets, thereby legitimizing their existence.

Money laundering refers to the illegal process of making illegally obtained or "dirty" money appear legal or "clean" by disguising its true origin, ownership, or purpose. It involves a series of transactions and activities that aim to obscure the illicit nature of funds and make them appear legitimate.

The primary objective of money laundering is to integrate the illicit funds into the legitimate financial system without raising suspicion. This process allows individuals or criminal organizations to enjoy the profits generated from illegal activities while distancing themselves from any association with criminal behaviour.

Stages of Money Laundering

Money laundering typically involves three main stages: placement, layering, and integration.

1. Placement: This is the initial stage where the illegally obtained funds are introduced into the

financial system. It often involves activities such as depositing cash into bank accounts, purchasing assets, or using it for gambling. The aim is to break down large sums of money into smaller, less suspicious amounts that can be easily handled.

2. Layering: In this stage, the launderers create complex layers of transactions to further obscure the origin of the funds. They may engage in multiple transfers between accounts, conduct transactions across different countries or financial institutions, and employ various techniques to make it difficult to trace the money back to its illegal source. This process aims to create a convoluted paper trail that confuses



investigators and hides the illicit origin of the funds.

3. Integration: The final stage involves reintroducing the laundered money back into the legitimate economy. At this point, the funds appear to be clean and can be freely used without arousing suspicion. The launderers may invest the money in legitimate businesses, purchase real estate or other assets, or engage in legal financial transactions. By integrating the funds into the legal economy, the individuals or organizations can enjoy the illicit profits and legitimize their wealth.

Money laundering is a serious crime that enables the perpetuation of various illegal activities, such as drug trafficking, corruption, fraud, and organized crime. It undermines the integrity of the financial system, hampers efforts to combat crime, and can have significant negative effects on economies and

societies. To combat money laundering, governments and financial institutions have implemented strict regulations, monitoring systems, and international cooperation efforts to detect and prevent these illicit activities.

Common Money Laundering Schemes

Shell Companies and Offshore Accounts: Criminals frequently employ shell companies and offshore accounts to launder money. These entities, often established in tax havens, serve as conduits for transferring funds, creating complexity and obscurity in financial transactions.

1. Trade-Based Money Laundering: Criminals manipulate trade transactions to facilitate money laundering. Over or under-invoicing of goods, multiple invoicing, and false descriptions of goods are common techniques used to obscure the illicit origin of funds.

2. Virtual Currencies: The rise of cryptocurrencies has opened new avenues for money laundering. Criminals exploit the decentralized nature of virtual currencies to move and convert funds anonymously, making detection and tracking challenging for law enforcement agencies.

3. Real Estate Investments: Money laundering through real estate involves purchasing properties using illicit funds and then selling or renting them to create a seemingly legitimate source of income. This scheme helps criminals integrate their illicit funds

into the legal economy.

4. Shell companies: Setting up fictitious businesses to commingle illicit funds with legitimate ones.

5. Smurfing: Breaking large sums of money into smaller, less suspicious transactions.

6. Trade-based laundering: Manipulating invoices and over/under-invoicing in international trade transactions.

7. Offshore accounts: Transferring money to banks in countries with lax financial regulations.

8. Structuring deposits: Making multiple small deposits to avoid reporting thresholds.

9. Black market peso exchange: Converting illicit funds into another currency through a network of currency dealers.

10. Cash-intensive businesses: Using cash-based businesses to blend illegal funds with legitimate revenues.

11. Gambling: Placing illicit funds as bets and later claiming winnings as legitimate income.

12. Cryptocurrency conversion: Using digital currencies to convert illicit funds into seemingly legitimate assets.

13. Loan-back schemes: Lending illegally obtained money to oneself through offshore entities.

14. Hawala system: An informal money transfer system that bypasses traditional banking channels.

15. Art and antique sales: Purchasing high-value items with illicit funds and reselling them at legitimate auctions.

16. Charitable organizations: Donating illicit funds to charities and claiming tax deductions.

17. Front companies: Using legitimate businesses to mix illicit funds with legal revenues.

18. Prepaid cards: Loading illicit funds onto prepaid cards for withdrawal or transfer.

19. Underground banking: Operating unregulated financial institutions for money movement.

20. Stock market manipulation: Buying and selling stocks to obscure the origin of funds.

21. Cash smuggling: Physically transporting large

amounts of cash across borders.

22. Loan repayment schemes: Repaying loans using illicit funds, making the money appear as legitimate debt payments.

Investigative Techniques

Law enforcement agencies and financial institutions employ various investigative techniques to detect and combat money laundering. Here are common investigative techniques used in the fight against money laundering:

1. Financial Intelligence Units (FIUs): Governments establish FIUs to collect, analyse, and disseminate financial information to combat money laundering. By monitoring suspicious transactions and sharing information with law enforcement agencies, FIUs play a vital role in detecting and investigating money laundering activities.

2. Know Your Customer (KYC) Regulations: Banks and financial institutions adhere to KYC regulations, requiring them to verify the identities of their clients and monitor their transactions. Strict KYC protocols help identify and prevent money laundering attempts by establishing transparency and accountability in financial transactions.

3. Enhanced Due Diligence (EDD): Conducting thorough due diligence on high-risk customers or transactions allows financial institutions to identify potential money laundering activities. By scrutinizing the source of funds, beneficial ownership, and transaction patterns, EDD helps to detect suspicious activities that may warrant further investigation.

4. Collaboration and Information Sharing: Effective combating of money laundering requires cooperation between financial institutions, regulatory bodies, and law enforcement agencies. Sharing information, intelligence, and expertise facilitates the identification and tracking of money laundering networks and enhances the overall investigative efforts.

5. Transaction monitoring: Tracking and analysing financial transactions for suspicious patterns or behaviour.

6. Know Your Customer (KYC): Verifying the identity of customers and assessing their risk level before conducting business.

7. Suspicious Activity Reports (SARs): Reporting unusual or suspicious transactions to regulatory

authorities.

8. Source of Funds/Wealth: Investigating and verifying the origin of funds used in transactions.

9. Financial intelligence units (FIUs): Specialized agencies that collect, analyze, and disseminate financial information to combat money laundering.

10. Due diligence: Conducting thorough investigations and background checks on individuals, businesses, and financial transactions.

11. Data analysis: Utilizing data analytics to identify anomalies and patterns indicative of money laundering.



12. Collaboration and information sharing: Exchanging information and cooperating with other agencies, both domestically and internationally.

13. Undercover operations: Deploying undercover agents to infiltrate criminal networks involved in money laundering.

14. Asset tracking and forfeiture: Tracing and seizing assets acquired through illegal activities.

15. Sting operations: Setting up scenarios to catch individuals engaging in money laundering activities.

16. Whistle-blower reports: Encouraging individuals with insider knowledge to report suspected money laundering activities.

17. Parallel financial investigations: Simultaneously investigating the financial aspects of a crime along with other criminal elements.

18. Cryptocurrency analysis: Tracking and

analyzing cryptocurrency transactions for money laundering activities.

19. Enhanced due diligence: Applying more rigorous scrutiny and monitoring to high-risk customers or transactions.

20. Financial audits: Conducting thorough reviews of financial records and statements to detect irregularities.

21. International cooperation: Collaborating with foreign jurisdictions to investigate cross-border money laundering activities.

22. Forensic accounting: Employing accounting techniques to analyze financial records and detect discrepancies or hidden transactions.

23. Watchlists and sanctions screening: Checking individuals and entities against watchlists and sanctions lists to identify suspicious connections.

24. Training and awareness programs: Educating financial professionals, law enforcement, and the public about money laundering risks and prevention measures.

These techniques, combined with legal frameworks and regulations, play a crucial role in identifying and combating money laundering activities.

Conclusion

Investigating money laundering schemes and techniques is a multifaceted task that demands a combination of legal frameworks, technological advancements, and international cooperation. By understanding the various money laundering methods and continuously adapting investigative techniques, authorities can improve their ability to detect, prevent, and disrupt money laundering operations. Strengthening regulatory frameworks, enhancing international cooperation, and promoting awareness among financial institutions and the public are essential steps toward combating this illicit practice and safeguarding the integrity of financial systems worldwide.

*Onwumele Sunday Emeke CFE
Team Member Head Office Audit
United Bank for Africa Plc*



Fraud Control And Prevention As An Investment In The Long Run

Fraud prevention is an investment in the long-term health and sustainability of an organisation.

Fraud control and prevention is an important investment for any organization in the long run. Fraud can have severe consequences on a business, including financial losses, damage to reputation, and loss of customer trust. It is therefore important for organizations to take proactive measures to prevent fraud from occurring and to detect it early if it does occur.

Investing in fraud control and prevention can involve several measures, such as implementing strong internal controls, conducting regular audits, and providing training to employees on fraud awareness and prevention. These measures can help prevent fraudulent activities from taking place within the organization and can also help detect fraud early, minimizing its impact.

While investing in fraud control and prevention may require some initial costs, the benefits of doing so can far outweigh the costs in the long run. By preventing fraud, organizations can avoid financial losses,

damage to reputation, and legal consequences. Additionally, investing in fraud control and prevention can help build trust with customers and stakeholders, which can lead to increased business opportunities and profitability.

Fraud control and prevention is indeed an investment in the long-term health and sustainability of an organization. Here's why:

Financial Protection: Fraud can have severe financial consequences for an organization. It can result in monetary losses, damaged reputation, legal liabilities, and increased insurance premiums. By implementing robust fraud prevention measures, an organization can minimize these risks and protect its financial resources.

Preserving Trust and Reputation: Fraud incidents can erode the trust and confidence that customers, investors, and partners have in an organization. Maintaining a strong reputation is crucial for long-term success. By demonstrating a commitment to fraud prevention, an organization signals its dedication to integrity, transparency, and ethical

business practices, thereby safeguarding its reputation.

Operational Efficiency: Fraudulent activities can disrupt business operations, divert resources, and hinder productivity. Implementing preventive measures, such as internal controls, employee training, and monitoring systems, helps streamline operations by reducing the likelihood of fraud occurrences. This, in turn, improves efficiency, productivity, and overall organizational performance.

Legal and Regulatory Compliance: Many industries are subject to specific laws and regulations governing fraud prevention. Non-compliance can lead to penalties, fines, and legal consequences. By investing in fraud prevention, an organization ensures adherence to legal and regulatory requirements, mitigating the risk of legal complications and associated costs.

Enhanced Employee Morale: Fraud incidents can harm employee morale and trust within the organization. When employees witness fraudulent activities, it can lead to a toxic work environment, decreased job satisfaction, and increased turnover. By proactively addressing fraud risks, an organization fosters a culture of transparency and integrity, promoting employee morale and loyalty.

Investor Confidence: Investors and stakeholders are more likely to support organizations that prioritize fraud prevention. By demonstrating a strong commitment to maintaining a fraud-free environment, organizations attract investment and gain the confidence of shareholders, leading to increased financial stability and long-term sustainability.

Competitive Advantage: Organizations that proactively invest in fraud prevention differentiate themselves from competitors. Customers, partners, and investors value organizations with robust anti-fraud measures in place, as it demonstrates a commitment to ethical practices and risk management. This can provide a competitive edge and contribute to long-term growth and sustainability.

Practical Ways of Investing in Fraud Control and Prevention

Investing in fraud control and prevention is important for both individuals and businesses to safeguard their assets, reputation, and credibility. Here are some practical ways to invest in fraud control and prevention:

1. Implement strong internal Controls:

Businesses can implement strong internal controls to prevent fraud. This includes segregating duties, regular audits, and implementing checks and balances in financial transactions.

2. Conduct Background Checks: When hiring employees, conducting thorough background checks can help prevent fraud. This includes verifying educational and employment history, as well as conducting criminal background checks.

3. Invest in fraud detection software: Businesses can invest in fraud detection software that can identify patterns and anomalies in financial transactions, helping to detect fraud before it occurs.

4. Provide fraud awareness training: Educating employees about the risks of fraud and how to identify and report suspicious behaviour can help prevent fraud.

5. Work with a fraud prevention specialist: Businesses can work with a fraud prevention specialist who can help identify potential risks and develop a comprehensive fraud prevention program.

6. Use secure payment systems: Individuals and businesses should use secure payment systems to protect against fraudulent transactions. This includes using credit cards with fraud protection and avoiding sharing personal or financial information over unsecured networks.

7. Stay vigilant: It is important to stay vigilant and monitor financial transactions regularly to detect and report any suspicious activity. This includes reviewing bank statements, credit reports, and monitoring social media and online accounts for signs of identity theft or fraud.

Investing in fraud control and prevention can save individuals and businesses from significant financial losses and reputational damage. By implementing these practical measures, individuals and businesses can protect themselves against fraud and mitigate potential risks.

In conclusion, fraud control and prevention is an important investment for any organization in the long run. By taking proactive measures to prevent and detect fraud, organizations can avoid the negative consequences associated with fraudulent activities and build a reputation for integrity and trustworthiness

*Onwuemele Sunday Emeke CFE
Team Member Head Office Audit
United Bank for Africa Plc*



What Auditors Should Know About The Payment Card Industry Security Standards Council's Evolutions.

1.0 INTRODUCTION

Today's businesses cannot get wider acceptance without a digitalized mode of settlement (that is debit and credit). Businesses that accept credit and debit card payments face a high risk of malicious attacks from cyber-crimes of various degrees. Malicious attackers target the sensitive personal information cardholder data (CHD) and sensitive authentication data (SAD) of cardholders.

The Payment Card Industry Data Security Standard (PCI DSS) aims to enhance security for consumers by setting guidelines for any company that accepts, stores, processes, or transmits credit card information irrespective of the volume of transactions or the size of the transactions.

These risks also extend to merchants, processors, and service providers (in this case deposit money banks, FINTECH entities and others) involved in payment transactions. This article will examine the evolution of payment card industry security standards released by the Council with a special focus on PCI DSS V.4.

2.0 SECURITY CONTROLS TO PROTECT BUSINESSES AND CUSTOMERS.

The Payment Card Industry Security Standard Council created security controls to protect businesses and

customers. One such standard is the payment card industry security standards; having been very acceptable amongst major card brands, it highlights the policies and practices to secure transactions and prevent identity theft of all kinds.

All organizations involved in payment card transactions, as well as those handling sensitive authentication data, are subject to PDI DSS. The Council thus also ensure that it does not fall short of its change management configuration as fraudsters also increase their searches to break through programming codes and firewalls built to protect the global payment systems.

2.1 PCI DSS V4.0 FOCUS HIGHLIGHTS

- PCI DSS V4.0 High-Level Changes
- Understanding new requirements of PCI DSS V4.0
- How to prepare for PCI DSS 4.0 Implementation
- Goals of PCI DSS V4.0
- What changes are required to do for the existing entities holding PCI DSS 3.2.1
- Defined Approach Vs Customized Approach.

- V3.2.1 to V4.0 Transition & Timelines
- Compliance Requirements for Merchants and Service Providers.

2.2 THE PCI DSS EVOLUTION AND OBJECTIVES

Taking a retrospective look at the changes that have emanated from the PCI SSC (Council) in a way to foster safe havens for entities and individuals either as merchants or users on web transactions or one-time present payments, the evolution timelines have taken into cognizance the intelligence of fraudulent actors who manipulate and execute rigorous research to break through coded scripts at all hours of day and night to reap where they did not sow.

S/N	HISTORICAL MILESTONES	EVOLUTION TIMELINES	OBJECTIVES OF PCI VERSIONS
1	2004	PCI 1.0	Data standard security was created
2	2006	PCI 1.1	Enhanced to address evolving web application security.
3	2008	PCI 1.2	Enhanced to address evolving wireless security.
4	2009	PCI 1.2.1	Enhanced with inputs from industry contributors.
5	2020	PCI 2.0	<ul style="list-style-type: none"> ■ No major changes. ■ Designed to promote greater clarity and flexibility to facilitate improved understanding of the requirements and eased implementation for merchants.
6	2013	PCI 3.0	Focuses on helping business integrate payment security into daily business practices.
7	2015	PCI 3.2	Addressed growing threats to customers payment information.
8.	2018	PCI 3.2.1	Minor update to address customer migration to enhance datagram transport layer security (DTLS).
9	2022	PCI V4.0	<ul style="list-style-type: none"> ■ Continuous enhancement of the standard to meet today's payment security needs ■ Add flexibility and support via additional methodologies to achieve security. ■ Promote Security as a continuous process ■ Enhance validation methods and procedures, via assessments of adhering to validation requirements as a consistence experience across the industry.

These timelines brought about changes that could mitigate nefarious acts of unauthorized cards users, thus leading to the PCI version designated as "V4.0".

The objectives are shown in the schedule below:

2.3 **Prior to the emergence of PCI V4.0, PCI 3.2.1** laid emphasis on DTLS, which stands for Datagram Transport Layer Security. It connotes a communication protocol which provides security to datagram-based applications by enabling them to communicate in a way required to prevent eavesdropping, text or message

forgeries, tampering or dilution, and avoidance of discrete theft of the data being streamed.

The DTLS protocol however based on the stream-oriented transport layer security (SO_TLS) – protocol and is intended to provide similar security guarantees. The DTLS protocol datagram preserves the semantics of the underlying transport – the application does not suffer any delay associated with

- PCI DSS requirements (listed in the form of a schedule to be holistically followed)
- Protect stored cardholder data
- Use and regularly update anti-virus software or programs
- Restrict access to cardholder data by business



stream protocols, but because it uses 'user datagram protocol' (UDP) or 'stream control transmission protocol' (SCTP). The application deals with packet re-ordering, loss of datagram and data larger than the size of the datagram network packet. DTLS uses UDP and SCTP rather than transmission control protocol (TCP), this is to avoid "TCP meltdown problem" when being used to create a VPN tunnel.

3.0 PRINCIPLES TO AID FORTIFY THE CONTROL ENVIRONMENT BY BANKS

- Secure network requirements
- Security policies requirements must be in place
- Cardholder data requirements
- Vulnerability management requirements
- Assess control requirements
- Monitoring and testing requirements

3.1 **Payment Card Industry Data Security Standard Council thus requires entities to ensure the following:**

"need-to-know" (NTK) basis.

- Track and monitor all access to network resources and cardholder data.

4.0 CONCLUSION

The PCI DSS (Payment Card Industry Data Security Standard) is an information security standard designed to reduce payment card fraud by increasing security controls around card-holders data. The standard is a result of collaboration between the major payment brands and is administered by the Payment Card Industry Security Standards Council (PCI SSC).

The latest iteration of the PCI DSS – version 4.0 was released at the end of March 2022. Merchants and service providers have a two-year transition period to update their security controls to conform to the new version of the standard (V4.0) while version 3.2.1 would be retired on the 31st March 2024.

*Julius Oreye A.
internal Control
Heritage Bank Plc*



Cybersecurity and its Impact on Financial Institutions Mitigating Fraud Risks

Meaning of Cybersecurity

Cybersecurity refers to the practice of protecting computer systems, networks, and digital data from unauthorized access, theft, damage, or disruption. It involves implementing measures and employing techniques to safeguard information technology (IT) infrastructure, including computers, servers, mobile devices, electronic systems, and the data they store or transmit.

The primary objective of cybersecurity is to ensure the confidentiality, integrity, and availability of digital assets. Confidentiality means that sensitive information remains accessible only to authorized individuals or entities. Integrity ensures that data remains unaltered and accurate throughout its lifecycle. Availability means that authorized users can access information and services when needed, without disruption or denial of service.

Cybersecurity involves various practices and technologies to protect against cyber threats, such as hacking, data breaches, malware, ransomware, phishing, social engineering, and other malicious activities. It encompasses the implementation of security controls, encryption, access management, intrusion detection systems, firewalls, antivirus software, and regular security assessments.

Given the ever-evolving nature of cyber threats, cybersecurity also includes proactive measures such as threat intelligence, vulnerability scanning, security awareness training, incident response planning, and continuous monitoring of systems and networks to identify and mitigate potential risks.

Overall, cybersecurity aims to create a secure digital environment to safeguard sensitive information, maintain user privacy, prevent financial losses, protect critical infrastructure, and ensure the smooth operation of organizations and individuals in an increasingly connected world.

In today's digital age, the significance of cybersecurity cannot be overstated, especially for financial institutions. With the increasing reliance on technology and the rapid growth of online banking and financial transactions, the risk of cyber threats and fraud has become a major concern for both financial institutions and their customers. It is crucial for these institutions to understand the impact of cybersecurity on their operations and take proactive measures to mitigate fraud risks. This article explores the importance of cybersecurity for financial institutions and provides insights into effective strategies for combating fraud.

The Impact of Cybersecurity on Financial Institutions

Financial institutions, such as banks, credit unions, and investment firms, store and process vast amounts of sensitive customer information, including personal identification details, financial records, and transaction data. This makes them prime targets for cybercriminals who seek to exploit vulnerabilities and gain unauthorized access to valuable financial resources.

A successful cyber attack can have severe consequences for financial institutions. It can lead to the loss of sensitive data, financial theft, reputational damage, and legal liabilities. Moreover, the financial losses resulting from fraud incidents can be substantial and negatively impact the institution's bottom line.



20 Practical Measures of Mitigating Fraud Risks through Cybersecurity Measures:

Mitigating fraud risks in cybersecurity is essential to protect organizations and individuals from various threats. Here are 20 practical ways to mitigate fraud risks:

- 1. Implement Multi-Factor Authentication (MFA):** Require users to provide multiple authentication factors to access sensitive systems and data, making it harder for attackers to gain unauthorized access. To effectively mitigate fraud risks, financial institutions need to adopt a multi-layered approach to cybersecurity. Here are some key strategies that can help in this regard.
- 2. Regularly Update and Patch Systems:** Keep all software and systems up to date with the latest security patches to address vulnerabilities that fraudsters could exploit.
- 3. Conduct Employee Training and Awareness**

Programs: Educate employees about common fraud risks, phishing techniques, and best practices for secure online behaviour to minimize the likelihood of falling victim to scams.

- 4. Use Strong Password Policies:** Enforce the use of complex passwords and encourage employees to regularly update them to prevent unauthorized access to accounts.
- 5. Implement Access Controls:** Assign user roles and permissions based on the principle of least privilege, ensuring that employees have access only to the systems and data necessary for their roles.
- 6. Monitor and Analyse Network Traffic:** Implement network monitoring tools to identify unusual activities, detect potential intrusions, and mitigate fraud attempts in real-time.
- 7. Encrypt Sensitive Data:** Protect sensitive information by encrypting it both at rest and in transit to prevent unauthorized access or interception.
- 8. Deploy Intrusion Detection and Prevention Systems (IDPS):** Utilize IDPS solutions to detect and block suspicious network traffic and potential cyber-attacks.
- 9. Conduct Regular Security Audits:** Perform routine security assessments to identify vulnerabilities, assess the effectiveness of security controls, and address any weaknesses promptly.
- 10. Implement Fraud Detection Systems:** Utilize advanced fraud detection systems that analyze patterns and anomalies in user behavior, transactional data, and other relevant factors to identify potential fraudulent activities.
- 11. Secure Wireless Networks:** Protect Wi-Fi networks with strong encryption (e.g., WPA2) and unique passwords to prevent unauthorized access.
- 12. Use Secure Payment Systems:** Implement secure payment gateways and protocols to safeguard

customer financial information and prevent payment fraud.

13. **Regularly Backup Data:** Perform regular backups of critical data to ensure its availability and recoverability in the event of a security incident or data loss.

14. **Implement Data Loss Prevention (DLP) Solutions:** Utilize DLP tools to monitor and prevent the unauthorized transfer or leakage of sensitive data.

15. **Establish Incident Response Plans:** Develop and document a clear plan of action to respond to security incidents promptly, minimizing the impact and recovery time.

16. **Employ User Behaviour Analytics (UBA):** Utilize UBA tools to monitor user activity and identify deviations from normal behaviour that may indicate fraudulent actions.

7. **Secure Remote Access:** Use secure remote access methods (e.g., virtual private networks, secure terminal services) and enforce strong authentication for remote employees and contractors.

18. **Implement Web Application Firewalls (WAF):** Deploy WAF solutions to protect web applications from common vulnerabilities and attacks, such as SQL injection and cross-site scripting.

19. **Regularly Test and Assess Security Controls:** Conduct penetration testing and vulnerability assessments to identify weaknesses in systems and infrastructure that fraudsters could exploit.

20. **Establish Vendor Management Controls:** Assess the security practices of third-party vendors and ensure they adhere to robust security standards to minimize the risk of fraud through external connections. Remember, fraud risk mitigation is an ongoing process, and organizations should continuously review and update their cybersecurity practices to stay ahead of evolving threats.

21. **Robust Firewalls and Intrusion Detection Systems:** Implementing strong firewalls and intrusion detection systems is essential to prevent unauthorized access to networks and systems. These technologies act as the first line of defence against cyber threats and help identify and block suspicious activities.

22. **Regular Software Updates and Patch Management:** Keeping all software, including operating systems and applications, up to date is critical. Software vendors frequently release updates and patches that address newly discovered vulnerabilities. Financial institutions must have robust patch management procedures in place to ensure that all systems are promptly updated.

23. **Employee Training and Awareness:** Human error is one of the leading causes of cybersecurity breaches. Providing comprehensive training programs to employees regarding cybersecurity best practices, including phishing awareness and password hygiene, can significantly reduce the risk of successful cyber-attacks.

24. **Continuous Monitoring and Threat Intelligence:** Implementing real-time monitoring systems that analyse network traffic and detect anomalies can help identify potential cyber threats early on. Financial institutions should also stay up to date with the latest threat intelligence to proactively address emerging risks.

25. **Incident Response and Business Continuity Planning:** Having a well-defined incident response plan in place is crucial to minimize the impact of a cyber attack. This plan should outline the steps to be taken in the event of a breach, including communication strategies, containment measures, and data recovery procedures.

Conclusion

As the financial sector becomes increasingly digital, the importance of robust cybersecurity measures cannot be overstated. Financial institutions must recognize the impact of cyber threats on their operations and take proactive steps to mitigate fraud risks. By implementing a comprehensive cybersecurity framework that encompasses firewalls, regular updates, employee training, strong authentication, data encryption, continuous monitoring, and incident response planning, these institutions can safeguard their assets and protect their customers' sensitive information. A strong commitment to cybersecurity will not only mitigate fraud risks but also enhance the reputation and trust of financial institutions in the eyes of their customers.

*Onwuemele Sunday Emeke CFE
Head Office Audit
United Bank for Africa Plc*

Happy Birthday Distinguished CAEs

	 Prince Akamadu April 06		 Rasaa Alawode April 11
	 Abiodun Gbadamosi April 16		 Mogbitse Atsagbede May 12
	 Isiaka Arowolo May 15		 Omobola Faleye May 30
	 Richard Bello Jun 07		 Yemi Ogunfeyimi Jun 13
	 Lydia I. Alfa June 17		 Mufutau Abiola Jun 19



Access Bank Plc
Omobola Faleye
14/15, Prince Alaba Oniru Street,
Victoria Island, Lagos
Omobola.Faleye@accessbankplc.com
08121913718



Bank of Agriculture Limited
Daniel Olatomide
1 Yakubu Gowon Way Kaduna.
d.olatomidei@boanig.com
08067007183



Bank of Industry Limited
Yemi Ogunfeyimi
23, Marina
Lagos.
yogunfeyimi@boi.ng
08033059361



Central Bank of Nigeria (CBN)
Lydia I. Alfa
Plot 33, Abubakar Tafawa Balewa
Way Central Business District,
Cadastral Zone, Abuja,
Federal Capital Territory, Nigeria
lialfa@cbn.gov.ng
07040092783



Citibank Nigeria Ltd
Emaka Owoh
27 Kofo Abayomi St
Victoria Island, Lagos
Emaka.owoh@citibank.com
08037027452



Coronation Merchant Bank Ltd
Adeola Awe
10, Amodu Ojikutu Street
Victoria Island, Lagos.
Aawe@coronationmb.com
08183745169



Development Bank of Nigeria
Joshua Ohima
The clans place
Plot 1386A Tigris Crescent,
Maitama, Abuja.
johioma@devbankng.com
08129145586



Ecobank Nigeria Ltd
Felix Igbinosia
Ecobank Pan African Centre (EPAC)
270, Ozumba Mbadiwe Street,
Victoria Island, Lagos, Nigeria.
FIGBINOSA@ecobank.com
07068754692 ; 08023633203
D/L: 01 2260449



FBNQuest Merchant Bank Limited
Dr. Romeo Savage
10, Keffi Street, Ikoyi Lagos
Remeo.Savage@fbnquestmb.com
01-270-2290 Ext-1245
08023551492



Federal Mortgage Bank of Nigeria
Rakiya Bello Umar
Plot 266, Cadastral AO, Central
Business District
P.M.B 2273, Abuja
rakiya.umar@fmbn.gov.ng
08180705065



Fidelity Bank Plc
Ugochi Osinigwe
Fidelity Bank Plc.
2, Adeyemo Alakija Street, VII, Lagos.
ugochi.osinigwe@fidelitybank.ng
08023030298, 08092147012.



First Bank of Nigeria Ltd
Mufutau Abiola
9/11, McCarthy Street, Lagos
Mufutau.Abiola@firstbanknigeria.com
081291456605



First City Monument Bank Ltd
Adebawale Oduola
10/12 McCarthy St, Lagos.
Adebawale.Oduola@fcm.com
01-2912276(D/L) 08034468071



FSDH Merchant Bank Limited
Dare Akinnoye
Niger House (6/7 floors)
1/5 Odunlami St, Lagos
dakinnuoye@fsdhgroup.com
08022017090



Greenwich Merchant Bank Ltd
Rasaq Alawode
Plot 1698A Oyin Jolayemi Street,
Victoria Island, Lagos
rasaq.alawode@greenwichbank
group.com
08083248797



Globus Bank Limited
Monday Edwards
6 Adeyemo Alakija Street,
Victoria Island, Lagos
mondayedward@globusbank.com
08023192506



Guaranty Trust Bank Plc
Lanre Kasim
178, Awolowo Road, Ikoyi, Lagos
lanre.kasim@gtbank.com
08023020839



Heritage Bank Ltd
Soridei Seba Akene
130, Ahmadu Bello Way,
Victoria Island, Lagos
Soridei.akene@hbg.com
08037025486



JAIZ BANK PLC
Musefiu Olalekan
No. 73 Ralph Shodeinde Street,
Central Business District,
P.M.B. 31 Garki Abuja, Nigeria.
080




Keystone Bank Limited
Abiodun Okusami
707 Adeola Hopewell Street,
Victoria Island, Lagos
abiodunokusami@yahoo.com
08033534920



Lotusbank
2, Bourdillon Road
Ikoyi Lagos.



NEXIM BANK
Ayaghena R. Ozemede
NEXIM House
Plot 975 Cadastral Zone AO,
Central Business District,
P.M.B. 276, Garki, Abuja, Nigeria.
ozemeder@neximbank.com.ng
08024725055



NIBSS Plc
Richard Bello
Plot 1230, Ahmadu Bello Way
Victoria Island, Lagos
rbello@nibss-plc.com.ng
08028346740



Nigeria Mortgage Refinance Company
Olusemore Adegbola
Plot 17, Sanusi Fafunwa,
Victoria Island, Lagos
oadegbola@nmrc.com.ng
08033769975



Nova Merchant Bank
Isiaka Arowolo
23, Kofo Abayomi Street
Victoria Island, Lagos.
Isiaka.arowolo@novamb.com
08033088681



Optimus Bank
Adeyinka Oladebo
55, Bishop Oluwole Street,
Victoria Island, Lagos
adeyinka.oladebo@optimusbank.com
07035316372



Parallex Bank
Seyi Ogundipe
Plot 1261, Adeola Hopewell, Street,
Victoria Island, Lagos.
Seyi.ogundipe@parallexbank.com
08023014800, 07081876026,
08102853283



Polaris Bank
Olurotimi Omotayo
3 Akin Adesola St
Victoria Island, Lagos
romotayo@polarisbanklimited.com
08023096373



Premium Trust Bank Limited
Dumebi Okwor
Plot 1612 Adeola Hopewell Street,
Victoria Island, Lagos
dumebi.okwor@premiumbank.com
08175500864.



Providus Bank Ltd
Aina Amah
Plot 724, Adetokunbo Ademola Street
Victoria Island, Lagos.
aamah@providusbank.com
08029087442




Rand Merchant Bank
Femi Fatobi
3RD Floor, Wings East Tower,
17A, Ozumba Mbadiwe Street
Victoria Island, Lagos
Femi.fatobi@rmb.com.ng
01-4637960, 08028514983




Stanbic IBTC Bank
Abiodun Gbadamosi
Plot 1712, Idejo Street
Victoria Island, Lagos
Abiodun.Gbadamosi@stanbicibtc.com
07057215563.



Standard Chartered Bank Nig. Ltd.
James Chukwuadi Unaegbe
142, Ahmadu Bello Way
Victoria Island, Lagos
Jameschukwuadi.Unaegbe@sc.com
07062776951



Sterling Bank Plc
Edward Onwubuya
1st Floor,
Sterling Bank Plc Head Office
(Annex), Ilupeju
239/241, Ikorodu Road, Lagos.
Edward.onwubuya@sterling.ng
08068250302



SunTrust Bank Nig. Ltd.
Youseph Edu,
1, Oladele Olashore Street,
Off Sanusi Fafunwa Street,
Victoria Island, Lagos
Yousuph.Edu@Suntrustng.com
0803 727 4559



TajBank Nigeria Limited
Saheed Adeoluola Ekeolere
Plot 72, Ahmadu Bello Way,
Central Business District,
Abuja.
saheed.ekeolere@tajbank.com
08033050015



The Infrastructure Bank Plc
Sadiku Ogbhe Kanabe
Plot 977, Central Business District
(Adjacent National Mosque)
P.M.B 272, Gark
F.C.T, Abuja Nigeria.
skanabe@tibplc.com
08033039481, 08056900079



Union Bank of Nigeria Plc
Prince Akamadu
36 Marina,
Lagos.
Poakamadu@unionbankng.com
08037649757



United Bank for Africa Plc
Gboyega Sadiq
UBA House
57 Marina, Lagos
gboyega.sadiq@ubagroup.com
08025011046



Unity Bank Plc
Olusegun M. Famoriyo
Plot 290A, Akin Olugbade Street,
Off Adeola Odeku Road,
Victoria Island, Lagos
famoriyo@unitybankng.com
08023145535



Wema Bank Plc.
Adekunle Onitiri
Wema Towers
54 Marina, Lagos
adekunle.onitiri@wemabank.com
+234 1 4622364, 08022245818



Zenith Bank Plc.
Mogbitse Atsagbede
Plot 84 Ajose Adeogun St
Victoria Island, Lagos
mogbitse.atsagbede@zenithbank.com
08023270998