



Association of Chief Audit Executives of Banks in Nigeria

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

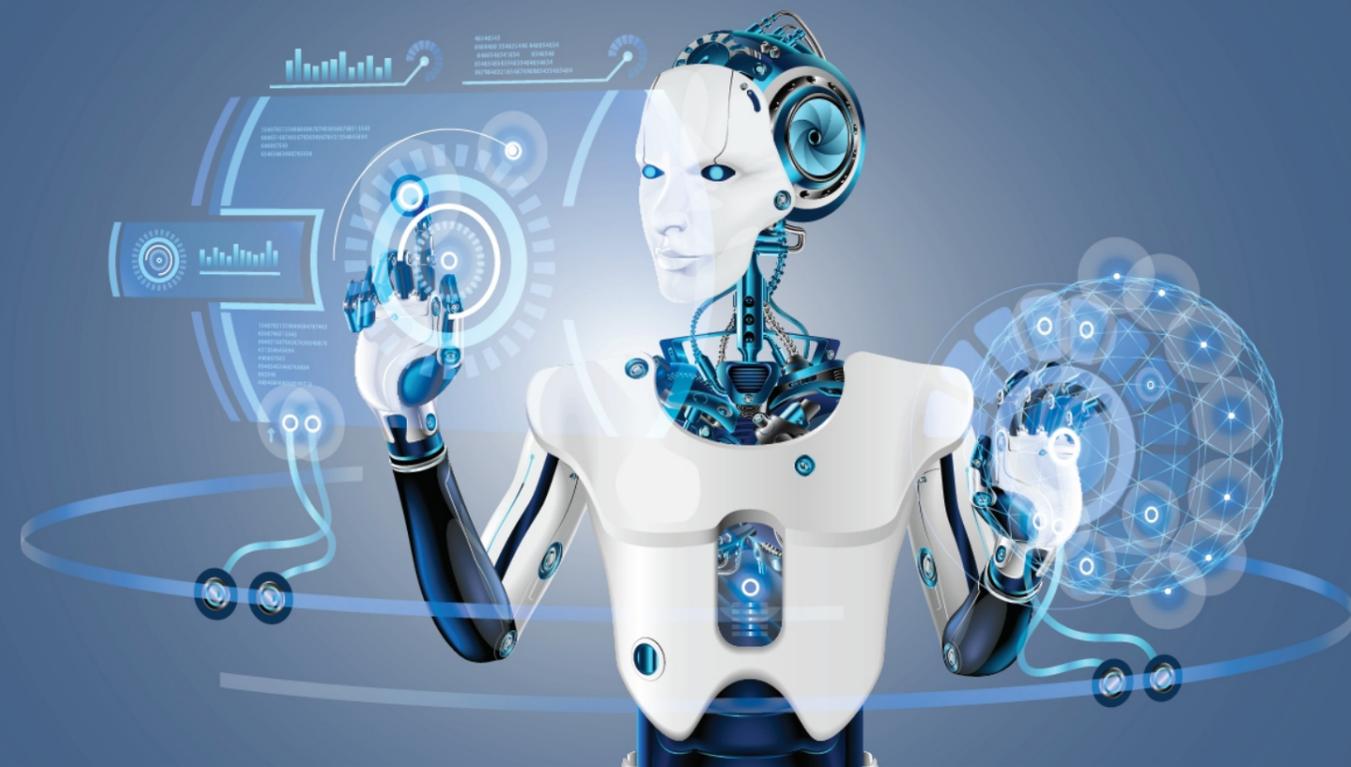
Design+printbyProwess08039221516



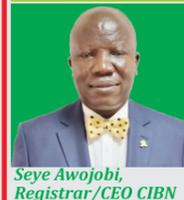
Eagle Eye

A Quarterly Publication of the Association of Chief Audit Executives of Banks in Nigeria (ACAEBIN) Q1, 2022

Disruptive Technology and its Impact on the Accounting Profession: The Nigerian Case.



Personality Interview:



Seye Awojobi,
Registrar/CEO CIBN

Collaboration Key to Achieving a Truly Independent Internal Audit Function...

Page 26

Wellness

Dealing with Anxiety



Page 44

Internal Audit Charter as a Bedrock for Effective Performance of Audit Functions... (Sample of Audit Charter)



Page 15

ACAEBIN EXCO MEMBERS



Yinka Tihamiyu
(Chairman)



Uduak Nelson Udoh
(1st Vice Chairman)



Felix Igbinosa
(2nd Vice Chairman)



Gboyega Sadiq
(Treasurer)



Aina Amah
(Auditor)



Prince Akamadu
(Chairman Research & Publication)



Adekunle Onitiri
(Chairman Payment & Systems)



Olusegun Famoriyo
(Ex-officio I)



Cyril Osheku
(Ex-officio II)

CONTENT

| | | | |
|----|--|----|--|
| 4 | Disruptive Technology and its Impact on the Accounting Profession: The Nigerian Case. | 31 | Understanding the Spread of Fintechs' Offerings within Banking Applications and the Internal Auditors' Checklist |
| 8 | Review of Internal Capital Adequacy Assessment Process (ICAAP) in banks - Special Focus on ... | 37 | Advancing the Auditing Techniques in the Pandemic and Post Pandemic era |
| 12 | Effective Time Management Skills for Productivity | 39 | Reasons for the Recent Spike in Fraud on Digital Banking Platforms and how to Mitigate ... |
| 19 | Artificial Intelligence (AI) Auditing Framework to Encourage Accountability | 43 | The 4-Dimensional Leadership Development |



Editorial

Welcome to the first edition of your flagship quarterly professional publication, 'Eagle Eye' in 2022.

We begin with the concerns expressed in certain quarters that Accounting profession may be going extinct by the combined influence of disruptive technologies such as robotic process automation (RPA), artificial intelligence (AI), blockchain, smart contracts, and advanced analytics. We have an article wherein the author rather argues that the profession should ignore such dark prophecies as the profession is far away from an inglorious ending. Instead, the profession should take advantage of the emerging technologies and enhance its pride of place.

We have included a scholastic article on the internal auditor's responsibilities as it pertains to Internal Capital Adequacy Assessment Process in Banks. Also in this edition is an article 'auditing the spread of fintech offerings' where the author posits that auditors should position to identify inherent risks on the e-payment platforms for banks especially as Fintech companies integrates into the banks' applications.

The writer of an article "Artificial Intelligence (AI) Auditing Framework to Encourage Accountability" is of the opinion that while protecting an organization against a diverse and ever-expanding range of risks may be daunting; avoiding AI and the risks it presents is not a viable option in today's highly digitized business environment.

You will find our article on 'the 4-Dimensional Leadership Development' interesting as it highlights the time honoured fact that the most constant factor in life is change and as such no professional or human being in general should allow him/herself to be left behind in the race of excellence. As a leader, you need to read.

Of course, we also have a sizzling interview with the Registrar of the Chartered Institute of Bankers in Nigeria, Dr. Seye Awojobi. He was at his cerebral best as he fielded questions from the editorial team. These and more we serve in this bumper edition.

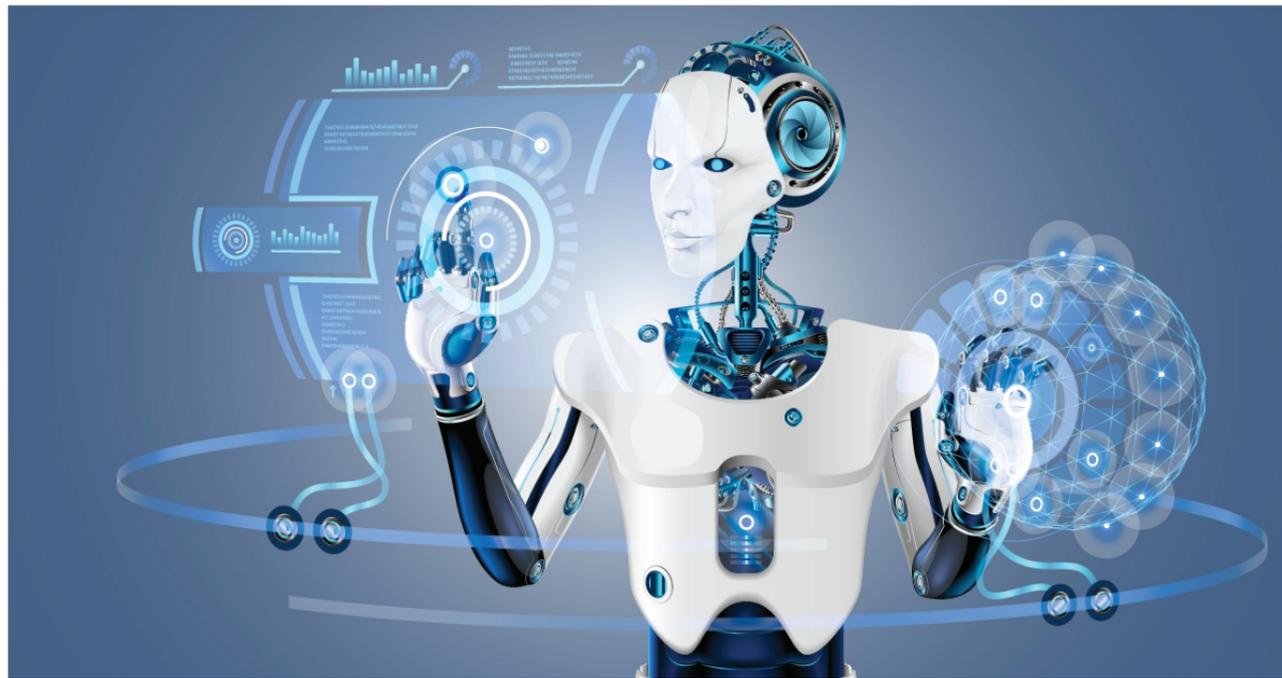
Finally, it is always difficult to say goodbye from people you love or an assignment that you are committed to. It has been an honour to serve as the editorial chairman of the *Eagle Eye* magazine for the last four eventful years. Over the course of the two tenures, we have made impactful changes, introduced innovations and generally enhanced the look and feel of the magazine even as we continued to publish through the Covid-19 pandemic against odds. Today, the *Eagle Eye* ranks very high amongst its peers in the industry. In fact, it is the reference point. None of these could have been possible without the unrelenting support of the Research and Publications Sub Committee and the article contributors. A very big 'thank you' to you all even as I wish the Association a successful Annual General Meeting in the ancient city of now cosmopolitan Uyo. To the newly minted ACAEBIN EXCO, I wish a successful tenure in office.

Prince Akamadu
Editor-in-Chief

Members of Research and Publication Committee

| | |
|----------------------------|------------------------------------|
| Prince Akamadu | (Union Bank of Nig. Plc), Chairman |
| Ugochi Osinigwe | (Fidelity Bank) |
| Daniel Olatomide | (Bank of Agriculture) |
| Awe Adeola | (Coronation Merchant Bank Ltd.) |
| Femi Fatobi | (Rand Merchant Bank Nig. Ltd) |
| Abiodun Okusami | (Keystone Bank Ltd.) |
| Ayaghena R. Ozemede | (NEXIM Bank) |
| Abdullahi Usman | (Jaiz Bank Plc) |
| Dare Akinnoye | (FSDH Merchant Bank Ltd.) |
| Sadiku O. Kanabe | (The Infrastructural Bank Plc) |

| | |
|---------------------------|--------------------------------------|
| Olusemore Adegbola | (Nigeria Mortgage Refinance Company) |
| Lydia I. Alfa | (Central Bank Nigeria) |
| Emeka Owoh | (Standard Chartered Bank Nig. Ltd.) |
| Aina Amah | (ProvidusBank Limited) |
| Rotimi Omotayo | (Polaris Bank Plc) |
| Cyril Osheku | (Sterling Bank Plc) |
| Joshua Ohioma | (Development Bank of Nig) |
| Yemi Ogunfeyimi | (Bank of Industry Limited) |
| Dr. Romeo Savage | FBNQuest Merchant Bank Limited |
| Rasaq Alawode | Greenwich Merchant Bank Ltd |



Disruptive Technology and its Impact on the Accounting Profession: The Nigerian Case.

Introduction

Technology is altering all aspects of business life and compelling adaptation in processes and product utilization. Disruptive technologies usually bring in cheaper and simpler products with features valued by new customers and often cause radical industry changes. In the era of disruptive technologies, accounting will inevitably change and be progressively automated in order to continue to be of great importance to the enterprises and stakeholders (Christensen & Raynor, 2013). The world driven by technology is filled with potentials and challenges - Cars that drive themselves, machines that read X-rays and algorithms that respond to customer-service inquires etc. are all manifestations of powerful new forms of automation. These technologies increase productivity and improve our lives as their use will substitute for some work activities humans currently perform.

The fast pace of technological innovation continues to interrupt traditional processes in all spheres, the accounting profession inclusive. Consequently, the author examined the likely effects that disruptive technologies will have on both the profession at large and accounting education specifically (Chanyuan, Jun & Mikkos, 2018). They provide suggestions for

educators and universities on how to shape their curricula to meet the needs of the new environment. It is predicted that the traditional mix of jobs in accounting firms will change substantially, and accountants will need to learn new skills when the more traditional tasks become automated and the technical maintenance and analytic needs of the work increase substantively. A major wave of educational change is also emerging with the advent of distance education, various forms of unorthodox training, and a large set of new learning needs. Given these disruptive information technologies, business measurement (accounting) and assurance (audit) will inevitably change and be progressively automated in order to continue to be of great importance to the enterprises and stakeholders (Li, Duo & Mikkos, 2017)

Concept of Disruptive Technology

The term "disruptive technology" as coined by Christensen (1997) refers to a new technology having lower cost of performance measured by traditional criteria but having higher ancillary performance. Christensen finds that disruptive technologies may enter and expand emerging market niches, improving with time and ultimately attacking established products in their traditional markets. This conception,

while useful, is also limiting in several important ways. By emphasizing only "attack from below" Christensen ignores other discontinuous patterns of change, which may be of equal or greater importance (Utterback, 1994; Acee, 2001). Further, the true importance of disruptive technology, even in Christensen's conception is not that it may displace established products, rather, it is a powerful means for enlarging and broadening markets and providing new functionality. In Christensen's theory of disruptive technology, the establishment of a new market segment acts to channel the new product to the leading edge of the market or the early adopters. Once the innovation reaches the early to late majority of users, it begins to compete with the established product in its traditional market.

Robotic Process Automation

Robotic Process Automation (RPA) automates repetitive tasks via the use of software robots that mimic human motions on a screen and extends automation to interfaces that are complicated or lack an Application Programming Interface (API). That is why RPA is excellent for automating activities that are typically performed by humans or need human interaction. Responsive robots adapt to changes in the display and maintain process flow in the case of a change. When RPA robots are powered by Artificial Intelligence-based machine learning, they are capable of recognizing screen objects (even the ones they have never seen before) and mimicking human intuition in understanding their function. They read text (for example, text boxes and links) using optical character recognition (OCR) and visual components using computer vision (for example, shopping cart icons and login buttons).

Artificial Intelligence (AI)

According to John McCarthy "the father of Artificial Intelligence", It is "The science and engineering of making intelligent machines, especially intelligent computer programs". Artificial Intelligence is a way of making a computer, a computer-controlled robot, or a software to think intelligently, the way intelligent humans think. AI is accomplished by studying how human brain thinks, learn, decide, and work while trying to solve a problem, and then use the outcomes of the study as a basis of developing intelligent software and systems. While exploiting the power of the computer systems, the curiosity of human lead to wonder, "Can a machine think and behave like humans?" Thus, the development of AI started with the intention of creating similar intelligence in machines that we find and regard high in humans.

Artificial intelligence (AI) is the ability of a machine or computer to replicate the attributes of human brain. AI makes use of a range of technologies to empower computers with human-like intelligence in terms of preparation, acting, perceiving, and detecting (Cozac, 2021). Artificial intelligence systems are sensitive enough to detect their surroundings, recognize objects, make decisions, settle conflicts, learn from experience, and simulate daily situations. These abilities are combined to accomplish activities that are usually undertaken by professionals.

According to Cozac (2021), artificial intelligent systems adhere to specific principles. It is founded on the reverse engineering of human abilities and traits transferred to a computer. The system utilizes computer power to perform tasks that are beyond the capability of average human. The machine must be trained to recognize and respond to certain behaviours. It uses historical data and algorithms to build propensity model. Through experience, machines gain the capacity to perform cognitive functions usually reserved for the human brain. The system self-learns from the features or patterns in the data.

Concept of Accounting Profession

A common international definition of the term professional accountant that could be widely understood, faithfully translated, and effectively applied would have utility to all stakeholders. It would support the International Federation of Accountants (IFAC) mission to serve the public interest by contributing to the development, adoption and implementation of high-quality international standards and guidance. It would acknowledge the applicability of the international standards to professional accountants is not limited to those who have membership in IFAC member organizations. Further, while it may not be possible to achieve a common definition that satisfies all conceivable objectives, a common international definition, descriptive in nature, could serve as a universal foundation from which further adjustments could be made on different national levels and in different professional contexts - acting as a focal point of consideration for the diverse functions of professional accountants.

The term professional accountant describes a person who has expertise in the field of accountancy, achieved through formal education and practical experience, and who: Demonstrates and maintains competence; complies with a code of ethics; is held to a high professional standard; and, is subject to enforcement by a professional accountancy



Review of Internal Capital Adequacy Assessment Process (ICAAP) in banks - Special Focus on Revised ICAAP Reporting (Internal Auditors' Responsibilities)

1.0 INTRODUCTION

Internal Capital Adequacy Assessment Process (ICAAP) is a process of planning a firm's appropriate level of capital via the combination of capital management activities and enterprise risks management in a way that support business strategies and decision making.

ICAAP thus allows entities to assess the capital adequacy and appropriateness of the risk management techniques or strategies that enables an entity to harness and document such processes. **The CBN's 2013 cum 2017 revised ICAAP guidance notes requires** ICAAP report to be submitted on an annual basis to the apex regulatory authority (Central Bank of Nigeria) taking into consideration the attributable sectoral cum industry risks where such entity plays.

2.0 CBN GUIDANCE NOTES REQUIREMENTS FROM BANKS

The 2013 guidance notes on **'Revised Guidance On Supervisory Review Process of ICAAP (SRP/ICAAP)'** provides a clear position on what banks are expected to do with respect to maintaining healthy capital structure in banks, The revised 2021 CBN guidance notes on ICAAP stated as excerpted below:

- All banks are required to develop an ICAAP to maintain adequate capital levels consistent

with their strategies, business plans, risk profiles and operating environment on a going concern basis.

- The ICAAP should be based on appropriate risk management systems that require adequate corporate governance mechanisms, an organisational framework with clear lines of responsibility, and effective internal control systems. This is because capital should not be regarded as a substitute for addressing fundamentally inadequate control or risk management processes.
- The ICAAP should be documented, understood, and shared by all bank structures and should be subject to independent internal review.
- The respective banks' boards are entirely responsible for the ICAAP. They are expected to independently establish the design and organisation of the ICAAP in accordance with the risk appetite of the bank. They are also responsible for the implementation and the annual update of the ICAAP and the calculation of internal capital that takes into consideration the banks' activities and operating environment.
- Banks should, on an annual basis (30th of April), submit to the CBN an ICAAP report

detailing, amongst others: the key features of the ICAAP, their risk exposures and the level of capital deemed adequate to support those risks. The report should also contain a self-assessment of the ICAAP, areas for improvement, any deficiencies in the process and any corrective measures to be taken.

2.1 IMPACT OF ECONOMIC CAPITAL ON ICAAP

ECONOMIC CAPITAL refers to the amount of risk capital that a bank estimates it will need in order to remain solvent at a given confidence level and time horizon. Regulatory capital on the other hand, reflects the amount of capital that a bank needs, given regulatory guidance and roles.

- Banks and other financial institutions must account for longer-term uncertainties.
- Economic capital is the amount of risk capital that a bank needs for a given confidence level and time period.
- EC is essential to support business decisions, while regulatory capital attempts to set minimum capital requirements to deal with all risks.
- A bank can use EC estimates to allocate capital across business segments.
- Economic capital could one day supersede regulatory capital requirements, as EC frameworks continue to grow thereby largely increasing the number of stress scenarios an entity needs to perform.

The loss absorption capacities of entities differ, wholly depending on the category of tier capital available to such bank or entity. These capital structures are designated into tiers I, II, III capital as highlighted below:

(I) Tier One Capital

Capital broadly includes elements such as:

- ✓ Common stock;
- ✓ Qualifying preferred stock;
- ✓ Surplus and retained earnings

3.0 REGULATORY REPORTING COMPONENTS OF ICAAP REPORT

- **Tier 1 (core) capital** broadly includes elements such as common stock, qualifying preferred stock, and surplus and retained earnings.
- **Tier II** Includes short-term subordinated debt and net trading book profits that have not been externally verified.
- **Tier III Capital** includes short-term subordinated debt and net trading book profits that have not been externally verified.

Note that these tiers may be constituted in various ways according to legal and accounting regimes in Bank for International Settlement (BIS) member countries. Additionally, the capital tiers differ in their ability to absorb losses;

Tier 1 capital has the best abilities to absorb losses. It is necessary for a bank to calculate the bank's minimum capital requirement for credit, operational, market risk, and other risks to establish how much Tier 1, Tier 2, and Tier 3 capital is available to support all risks.

4.0 COMPREHENSIVE IDENTIFICATION OF ENTERPRISE RISKS

In building the ICAAP model, the CBN revised guidance notes on Supervisory Review Process (SRP) requires that all duly identified activities within an enterprise should uphold certain percentages of risks to be dimensioned for the purpose of identifying its impact on bank's capital planning process. These risks attributable to these activities are listed below:

- ▣ Model risk
- ▣ Liquidity risk
- ▣ Interest rate risk in the banking book
- ▣ Legal risk
- ▣ Reputational risk
- ▣ Concentration risk
- ▣ Cyber risk
- ▣ Fraud risk
- ▣ Operational risk

■ Credit risk

5.0 RISK ASSESSMENT BASIS/LIQUIDITY RISK FRAMEWORK



Risk assessments are categorised into likelihoods – i.e. probability of an event happening in order to determine the level of significance as well as impact and ultimately determining the capital charges on the entity's overall business operations.

These risks are streamlined into:

■ *INHERENT RISKS*

■ *RESIDUAL RISKS*

INHERENT RISK connotes the level of risk on ground, before actions are taken to alter the risk's impact or likelihood. While **RESIDUAL** risk entails the outstanding or remaining level of risk following the development and implementation of entity's response.

5.1 CAPITAL CHARGES COMPUTATIONS

For assessing internal capital requirements, processes are stress-tested to ascertain the ability to withstand sudden decline arising from unexpected variables, externalities and perhaps force majeure. Losses arising from such scenarios or stress-tested results are estimated and charged or added to regulatory capital.

Thus, making all risks enabling charges to be tied to the entity's capital structure. Thereby making entities to seek for internal cum external funding in the form of capital buffers. This is done annually in line with CBN strong directives on sounding capital planning across banks and other financial institutions in Nigeria.

5.2 LIQUIDITY RISK FRAMEWORK

Bank's reputations are built on sound liquidity stability; to have a sound capital management plan, the liquidity risk framework needs to be managed and monitored effectively. Entities are endangered when they pay lip services to the liquidity framework. Key risk monitoring strategies for liquidity stress scenarios for banks underpinned the graphical illustration below:



- Contingency funding plan (CFP)
- Liquidity risk appetite
- Risk strategy formulation
- Daily funding management
- Stress testing
- Early warnings and monitoring.

5.3 ICAAP - SOUND CAPITAL ASSESSMENT

Risk registers are to be maintained for the purpose of assessing risks associated with banks' operations as well as duly monitored by Market Risk Management Team.

Historical, current and emerging risks are all considered for the purpose of understanding the degree of threats capital inadequacies pose to banks operations.

As part of the capital assessments, the CBN in its guidance notes stated the twelve items (12) which should embody the ICAAP annual reports for which oversight functions of the Internal Auditor remained imperatives. They are:

- Executive summary
- Structure and operations
- Governance and structure
- Risk assessment and capital adequacy
- Stress testing
- Capital planning

- Design, approval, review and use of ICAAP
- Challenges and further steps
- Summary of Internal Capital Adequacy Assessment Process
- Risk appetite statement
- Use of Internal Model for Capital Assessment
- Review of ICAAP (evidence of line item indicating that Internal/External Auditors have reviewed the ICAAP reports as issued.

6.0 RESPONSIBILITIES OF THE INTERNAL AUDITORS IN VIEW OF THE REVISED ICAAP REPORTING



- ◆ Confirm the ICAAP document and the results (including stress test results) were submitted to senior management and board and approved by the board prior to submission to CBN as evidence of board and senior management oversight.
- ◆ Confirm that the steering committee held and discussed the ICAAP report prior to rendition of the document as evidence of management review. (implore the CAE to ascertain evidence of such in the board minutes of meeting(s) reports)
- ◆ Obtain queries/comments raised by the CBN on the ICAAP documents and confirm management resolutions.
- ◆ Check and ensure that there is an executed ICAAP policy with the bank
- ◆ Confirm through calculations that the figures captured in the ICAAP document leading to capital charges for various identified risks, stress test results, and the underlying

assumptions are consistent with the different models or template used.

- ◆ Confirm that the ICAAP (12) items document is prepared following the sequence as stated in section 2.4.1 and annex B(7) of the CBN guidance notes on supervisory review process.
- ◆ Confirm that forward looking stress test scenarios and the underlying assumptions were approved by the bank's board and are in line with the bank's risk appetites.
- ◆ Verify the accuracy of the figures used in the computations of the stress tests outcomes.
- ◆ Confirm that forwarding lookig stress test scenarios and the underlying assumptions were approved by the Bank's board and are in line with the bank's risk appetite.

◆ Verify accuracy of the figures used in the computations of the stress test outcomes with bank audited financials, policies and other relevant documents.

◆ Verify with adequate evidences that the bank's projections of its pre-and-post stress test regulatory capital position, and the likely impact of the proposed management actions for at least three (3) years going forward, as stipulated in section 3.1 (15) of the CBN guidelines on stress testing for Nigeria banks.

- ◆ Verify that the responsibilities of the board and senior management are defined in the bank's ICAAP policy.

7.0 CONCLUSION

Internal Audit Teams in banks should align with the various checklists and fully understand the steps needed in the ICAAP computations. The impact of comprehensive identification of enterprise risks, sound capital assessment, stress testing, corporate governance roles as the body responsible for the ICAAP reports, monitoring and reporting, internal control systems and external cum internal audit roles in validating and providing assurances to those charged with governance of the banks.

*Julius Oreye
Head Office Audit, Heritage Bank Plc*



Effective Time Management Skills for Productivity

Time is one of the most important and valuable resources we have, yet many people do not make use of it wisely. This is usually due to a lack of understanding of the importance of effective time management and how it can improve the performance of every profession and life in general.

To most of us, it seems as if there's never enough time in the day. However, we all have 24 hours in a day to accomplish our tasks, and some people are exceptionally good at it, while others struggle to meet deadlines.

Why is it that some people utilize their time more efficiently than others? The answer lies in effective time management.

What is Effective Time Management?

Effective time management is the utilization of your time to plan your days so that you can do your work with less effort and make the most of the time you have. It involves planning and managing your time to work smarter rather than harder.

It allows individuals to make the best use of available time by prioritizing tasks according to their importance and estimated time taken to complete them. On the other hand, failing to manage time can negatively affect both your professional and personal

life. The quality of your work will improve, your performance will increase, and you will achieve your intended goals with less effort if you master time management.

Importance of Effective Time Management for Productivity

With effective time management, you can accomplish more within a shorter period, which offers you more time freedom, improves focus, reduces your stress, allows you to be more productive, and more time to devote to the people who mean most to you.

There are several reasons why time management is important in the workplace and even in life generally. It is, without a doubt, one of the most desired qualities for employees to have. Let's have a look at why time management is so important in the workplace.

- ◆ Better Performance
- ◆ Deliver Work on Time
- ◆ High Work Quality
- ◆ Improve Efficiency and Productivity
- ◆ Less Procrastination

- ◆ Better Work and Life Balance

1. Better Performance

One of the best benefits of being good at managing time is that you perform better at work. You will better understand what you must accomplish and how much time each task will take if you schedule a block of time during your day for your most important tasks.

Making a perfect schedule helps with time management and sticking to a strict schedule decreases the possibility of procrastination. When you have a schedule to stick to, you will spend less time deciding what to work on and more time accomplishing important tasks.

2. Deliver Work on Time

If you effectively manage your time, you can deliver work on time. To effectively manage your time, you must allocate each task on your list to a unique time slot.

3. High Work Quality

In any workplace, high-quality work is valued. Increased productivity naturally translates into better quality work. Your responsibilities as an employee include delivering work with a certain level of quality and standard. By proper utilization of time and prioritization of tasks, it is easy to achieve higher quality work.

4. Improve Efficiency and Productivity

Effective time management skills make you a more efficient and productive professional. This is because you are not spending time on insignificant activities and are completing your task as quickly as possible without compromising on the quality of work.

That does not mean you rush your work and sacrifice quality; it just means you make the most of the time you have. When you are occupied with unimportant tasks, your overall productivity suffers, but time management skills let you take care of tasks that are both urgent and important.

5. Less Procrastination

Procrastination happens due to poor time management. It is easy to get distracted and procrastinate if your goals aren't clear and focused. If you have a defined schedule that you know you must follow, you can reduce procrastination and focus on the work.

You won't procrastinate if you build effective time management skills and manage your time, and you will feel more in control of your workload. Therefore, this helps in the reduction of procrastination.

6. Better Work and Life Balance

Better work-life balance is the most important benefit of time management. Work-life balance means creating a balance between your professional and personal life.

Steps to Effective Time Management for Productivity

It's not so hard to learn how to manage your time; it just takes some practice and learning. Anyone can be good at time management. Here are some steps to that guarantee effective time management:

1. Plan

Planning is the most important aspect of effective time management. With proper planning, you can manage your time effectively and become more organized and productive. Many people find it helpful to take a few minutes every night before bed and put together their schedule for the next day.

For planning, you don't necessarily have to follow a strict routine. You should know what task to take and when to take it. The idea behind time management is to work smarter rather than harder and create space for other things as well.

It is important to recognize when you're most productive and save your most essential and challenging tasks for the time when your productivity is at its peak.

2. Prioritize Tasks

Prioritizing tasks involves listing tasks in order of their urgency and importance. One of the best ways to get started is by making a long list of every single task or duty you have in your job and prioritize them by their order of importance and urgency.

It is important to focus on your priorities to be successful at work. When you prioritize your tasks, you will realize how many unimportant things you do each day. You can delete these tasks from your list or assign them the lowest priority so that you can devote more time to those tasks that are essential and time-consuming.

3. Do not Multitask

Multitasking may seem to be a fantastic method to get more work done, and we often take pride in our ability to multitask, but it is the one you should not do. Research has shown that multitasking can lower your comprehension and intelligence level by 11%.

It is one of the most time-consuming activities and decreases your productivity. When you take on too many tasks, you end up achieving nothing. So, it's better to concentrate entirely on one task at a time rather than juggling multiple activities at the same time.

If you are working on just one project with full attention, the possibilities of making mistakes are lower, and you will produce a better quality of work.

4. Use Time Management Tools

One of the best things you can do to manage your time more wisely is by using as many tools as necessary to support your workload. There are millions of computer programmes and smart phone apps out there waiting to make your life easier with a simple download. Even adding a single time management tool to your repertoire can save you hours of work each week.

Time management tools helps you become more organized and efficient. It helps you to keep track of every minute and manage your work better. It can be helpful when you have many tasks to tackle at once.

5. Cut off Distraction

Distractions are caused by our poor time management skills and are one of the primary productivity killers. Some of the common distractions at the workplace are mobile phones, social media, and chatty co-workers.

Most of the time, notifications from mobile and laptops add to the distraction. If productivity is being affected by social media and mobile phones, set a time during the day to check social media, lock the smartphone in a desk drawer or use a browser extension to block the websites that are the most distracting.

6. Introduce Time Blocking

Time blocking is a time management method that asks you to divide your day into blocks of time. Each block is dedicated to accomplishing a specific task, or group of tasks, and only those specific tasks.

The key to this method is prioritizing your task list in advance. With days that are time blocked in advance, you won't have to constantly make choices about what to focus on. All you need to do is follow your time blocked schedule. If you get off-task or distracted, simply look at your schedule and get back to whichever task you blocked off time for.



Other variants of time blocking include task batching (grouping similar tasks together for a specific time block), day theming (dedicating each day to a single theme or type of activity) and time boxing (imposing a limit to how much time you will dedicate to a specific task).

Conclusion

Effective time management helps you become more focused and productive. The right time management strategy reduces stress, allows you to prioritize, and helps you work smarter, faster, and more efficiently.

Effective time management skills can have a positive impact on both your career and your personal life. Once you learn the art of time management, you can control your life and will have more power and freedom.

Jennifer Nwofor
ProvidusBank Limited



Internal Audit Charter as a Bedrock for Effective Performance of Audit Functions... (Sample of Audit Charter)

Introduction

Internal Auditing is an independent, objective assurance and consulting activity that is guided by a philosophy of adding value to improve the internal controls and operations of organizations. It assists the organization in accomplishing its objectives by bringing a systematic and disciplined approach to evaluate and improve the effectiveness of the organization's risk management, control and governance processes.

The Internal Audit function is established by the Board of Directors and oversight of the Internal Audit activities is delegated to the Audit Committee of the Board of Directors.

Purpose of the Charter

The purpose of this document is to define the role and responsibilities of the Internal Audit function and to set guidelines and standards for its operations. The Charter also records the reporting and oversight responsibilities for the function and the standards of independence and objectivity expected of the function in its operations. The Charter should be regularly updated and amended to reflect best

practices in the profession and changes in circumstances of organizations.

Mission

To provide independent, objective appraisal of all the activities of organizations and advise with a view to add value, improve operational efficiency, risk management and internal control systems.

The objectives of the internal audit function is to assist Management and the Board of Directors, through the Audit Committee in the effective discharge of their responsibilities through:

- Adopting a systematic and disciplined approach to examining and evaluating whether the Organization's framework of risk management, control and governance processes are adequate and functioning properly;
- Advising and recommending to the Board and Senior Management areas of improvements in the internal controls and risk management systems of the organization.

Scope of Work

The scope of work of the Internal Audit function is to develop, maintain and sustain a robust internal controls framework to provide assurance to Senior Management and Board Members with regard to the adequacy of internal controls and the effectiveness and efficiency of compliance within the Company. In order to fulfill its mission and objectives, the Internal Audit function scope of work may includes:

- ✦ Examination and evaluation of the adequacy and effectiveness of the internal control systems at various operations and activities of the Organization;



- ✦ Review of the application and effectiveness of risk management procedures and risk assessment methodologies at various operations and activities of the Organization;
- ✦ Review of management and financial information systems, including the electronic

- information system;
- ✦ Review of the accuracy and reliability of the Organization's accounting records and financial reports;
- ✦ Testing of both transactions and functioning of specific internal control procedures at various departments, offices or processes
- ✦ Evaluation of adherence to legal and regulatory requirements and approved policies and procedures;
- ✦ Evaluation of effectiveness of existing policies and procedures and provision of recommendations for improvement;
 - ✦ Identifying opportunities for cost savings and making recommendations for improving cost efficiencies;
 - ✦ Examining that resources are acquired economically, used efficiently and safeguarded adequately;
 - ✦ Carrying-out of special investigations.

Every activity, department and office of the Organization fall within the scope of internal audit for independent appraisal. The Head of Department (HOD) and staff of internal audit department are, however, not allowed to:

- Perform any operational duties for the Organization outside audit department functions;
- Initiate or approve accounting transactions external to audit department;
- Direct the activities of any employee not employed by the audit department, except to the extent such an employee has been appropriately assigned to work with or assist the auditing team in carrying out a specific engagement. Such directive(s) must be restricted to the extent of such an engagement.

- Engages in activities which will pairs the auditors objectivity and independence.

Authority

The HOD and staff of Internal Audit Department are authorized to:

- ✦ Have unrestricted access to all departments, offices, activities, records, information, properties and personnel, relevant to the performance of their audit function;



- ✦ Require all members of staff and management to supply such information and explanations as may be needed within a reasonable period of time;
- ✦ Determine scope of work and apply the techniques required to accomplish the audit objectives;
- ✦ Obtain the necessary assistance/cooperation of personnel in various departments/offices of the Organization where they perform audits;
- ✦ Obtain assistance of specialists/

professionals where considered necessary from within or outside the Organization.

Senior Management should inform Internal Audit immediately on any occurrence of any significant incident concerning security and/or compliance with regulations and procedures, without delay.

Responsibility

The Internal Audit function will comply with the *Standards for the Professional Practice of Internal Auditing* by the Institute of Internal Auditors (the

“Standards”) and accordingly, shall have responsibility to:

- ✦ Assessment of the reliability and integrity of financial and other management information and the systems and operations (in-house or outsourced) that produce such information;
- ✦ Upon request of the Audit Committee, perform consulting and advisory services related to governance, risk management, and control as appropriate for the Organization.
- ✦ Maintain requisite professional audit staff strength with sufficient knowledge, skills, experience, and relevant professional

certifications to meet the requirements of this Charter

- ✦ Issue periodic reports on a timely basis to the Committee and Managing Director summarizing results of audit activities.
- ✦ Maintain and administer a rigorous follow-up process to ensure that necessary measures to address the concerns have been taken by Management;
- ✦ Evaluate the means of safeguarding assets of the Organization,, its appropriateness as well as, verifying the existence of such assets.
- ✦ Continuous review of existing procedures and systems for adequacy and propose improvements where necessary.
- ✦ Keep the Audit Committee informed of emerging trends and developments in internal auditing practices and give recommendations for necessary revisions in Internal Audit Charter and Internal Audit Manual. Provide a list of significant measurement goals and results to the Audit Committee;
- ✦ Assist in the investigation of significant violations of the Organization's code of conduct and notify the Audit Committee and Managing Director of the results.
- ✦ Work collaboratively with the Organization's external auditors and other Assessors to ensure appropriate risk coverage.
- ✦ Ensure that the department complies with sound internal auditing principles and best practices; seek guidance from the standards issued by the Institute of Internal Auditors and Information Systems Audit & Control Association, (USA) and other relevant professional bodies.

The HOD and staff of audit department have responsibility to:

- ✦ Follow the guidelines and methodology given in the Internal Audit Manual;
- ✦ Exercise due professional care in carrying out audit assignments.
- ✦ Maintain integrity and objectivity.

The internal audit process, however, does not relieve

departmental Heads/Managers of their responsibility for the maintenance and improvement of controls in their respective areas.

1 Internal Audit Plan

The HOD, Internal Audit Department will submit to the Audit Committee an annual audit plan and other activities for review and approval.

The internal audit plan is part of a cycle, which starts with the external auditors of the Organization delivering their report on the Organization's previous year and highlighting key issues requiring management's attention. These issues will be considered by the HOD, Internal Audit Department when preparing the plan.

The internal audit plan will include for every assignment

- A project title and proposed work plan;
- A list of risks already identified at the planning stage;
- Project administration: location, expected timing and resources required.

The internal audit plan will also include monitoring and follow up on prior year open issues.

The internal audit plan will be supported with a budget and other resource requirements for the next 12 months. The HOD, Internal Audit Department will communicate the impact of resources limitations and significant interim changes to the Audit Committee.

The internal audit plan will be developed based on prioritization of the audits using a risk-based methodology, including input of the Audit Committee and senior management (when appropriate). The internal audit plan may also include surprise audits. This plan may be modified, as appropriate for changing or emerging business risks or issues. Modifications that significantly alter the nature of collective audit and risk coverage provided under the plan must be reviewed and approved by the Audit Committee

TO BE CONTINUED...

Rasaq A Ozemede
CAE of NEXIM Bank



Artificial Intelligence (AI) Auditing Framework to Encourage Accountability

Artificial intelligence is a type of computer technology which is concerned with making machines work in an intelligent way, similar to the way that the human mind works.

The term is frequently applied to the project of developing systems endowed with the intellectual processes characteristic of humans, such as the ability to reason, discover meaning, generalize, or learn from past experience.

Artificial Intelligence (AI) is proliferating across industries and deepening its impact on many aspects of our personal lives — from voice recognition software like Apple's Siri or Amazon's Alexa to driver assist systems like Tesla Autopilot. While AI's growing ubiquity delivers competitive advantages and other beneficial outcomes, it also brings a commensurate number of potential risks and pitfalls.

ICT-based decision aids are currently making waves in the modern business world simultaneously with increased pressure on auditors to play a more effective role in the governance and control of corporate entities, to boost the value they bring to their organizations.

To position banks or organizations to reap the benefits of AI, internal audit functions need to consider how to incorporate control monitoring to prevent and mitigate potential risks. Failing to effectively provide assurance over AI initiatives may have far-reaching impacts. Regulators have signalled that they will be watching and may hold organization accountable for discrimination and bias in their AI algorithms.

This article will provide a quick overview of the stages in the AI life cycle where internal audit could provide assurance and highlight five potential AI auditing frameworks that internal audit functions can leverage to take advantage of AI, while protecting organizational assets and reputation.

Potential Impact of Artificial Intelligence on Organizations

There are many truths and half-truths out there concerning the impact that AI will have across a range of industries and professions. Some industries have adopted elements of the technology faster than others, with varying degrees of success and challenges. Given the hype surrounding AI we can be certain that there will be a significant impact on many

areas in the business world for the foreseeable future. AI will have far-reaching impact on the audit profession as well, given auditors' need to provide assurance around it. The purpose of this paper is to prepare auditors for what to expect and how to approach AI in a real-world audit scenario.

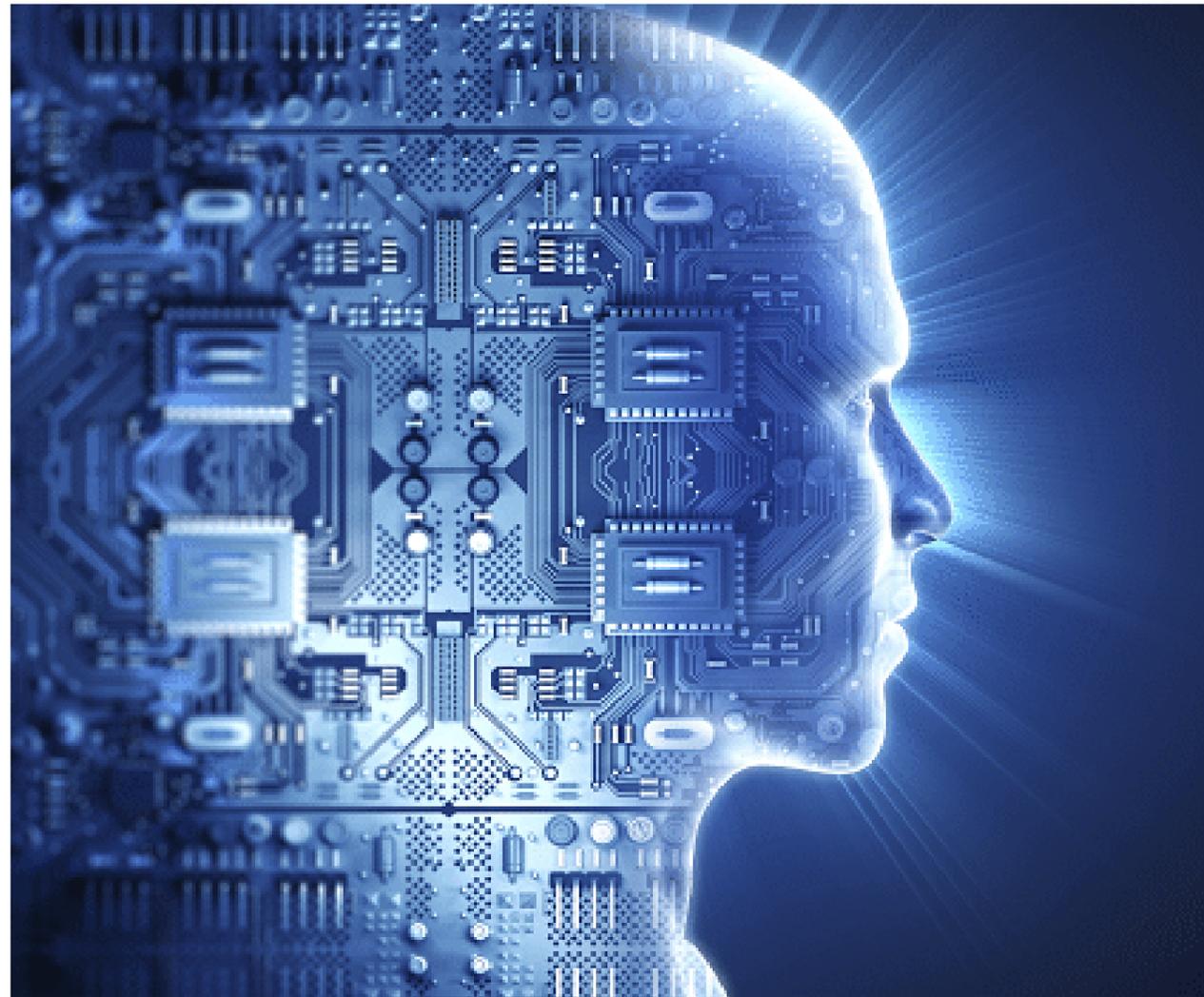
When should Internal Audit get Involved with Artificial Intelligence?

Oftentimes questions only get asked about an AI-enabled system after it has been designed, developed,

What AI Auditing frameworks can Internal Audit Leverage?

Protecting an organization against a diverse and ever-expanding range of risks may be daunting but avoiding AI and the risks it presents is not a viable option in today's highly digitized business environment.

With guidance on how to audit AI initiatives becoming more commonplace — even if it remains in its relative infancy — several AI auditing frameworks have been



and deployed but waiting introduces unnecessary risk. A best practice is to ask questions as the team moves through each of the various stages of the AI life cycle- design, development, deployment, and monitoring.

By conducting assessments throughout the entire AI life cycle not just solely at ad-hoc “points-in-time” system-wide issues become more apparent to internal audit and not unknowingly overlooked.

published by a mix of international organizations and governments that can aid the internal audit function.

- A. Control Objectives for Information and Related Technologies (COBIT) Framework
- B. Committee of Sponsoring Organizations (COSO) Enterprise Risk Management Framework
- C. US Government Accountability Office (GAO)

AI Framework

- D. Institute of Internal Auditors (IIA) Artificial Intelligence Auditing Framework
- E. Singapore Personal Data Protection Commission (PDPC) Model AI Governance Framework

We will look at each of these potential Artificial Intelligence framework and as we explore them you may be able to adopt a particular framework for auditing an Artificial Intelligence enabled initiative.

1. COBIT Framework

The most recent version of the COBIT framework, COBIT 2019, was released by the ISACA (Information Systems Audit and Control Association) in 2018 to replace its predecessor COBIT 5. Considered an “umbrella” framework and recognized internationally for the governance and management of enterprise information and technology it includes process descriptions, desired outcomes, base practices, and work products across nearly all IT domains. This broad IT applicability makes it well-positioned to serve as the initial starting point for the internal audit function when auditing AI-enabled initiatives. COBIT 2019 can be used to create an audit plan for AI, along with an enumeration of the nine main challenges to an effective AI audit that ISACA has identified, with similar best practice approaches to tackle these challenges.

2. COSO ERM Framework

Updated by the Committee of Sponsoring Organizations in 2017, the COSO ERM framework's five components governance and culture, strategy and objective-setting, performance, review and revision, and information communication and reporting and 20 principles provide internal audit functions with an integrated and comprehensive approach to risk management. COSO ERM's risk management approach can offer guidance to provide governance over AI and effectively manage its associated risks for the benefit of the organization.

Additionally, COSO and Deloitte's white paper, “Realize the Full Potential of Artificial Intelligence,” sets out a helpful five-step framework to follow when establishing an AI audit program:

- a. Establish a governance structure and identify a senior executive to lead the AI program and

provide risk and performance oversight.

- b. Collaborate with stakeholders throughout the organization to draft an AI risk strategy that defines roles, responsibilities, controls, and mitigation procedures.
- c. Complete an AI risk assessment for each AI model in use, understanding how it uses data and whether it introduces any unintended bias.
- d. Develop a view of risks and opportunities such as those pertaining to model malfunction.
- e. Specify an approach to manage risks and the associated risk-reward trade offs.

3. U.S. Government Accountability Office AI Framework

Developed by the U.S Government's Accountability Office (GAO), and published in June 2021, the Artificial Intelligence Accountability Framework for Federal Agencies and Other Entities was created to “help managers ensure accountability and responsible use of AI in government programs and processes.” Although this AI auditing framework has a focus on accountability for the government's use of AI, because it is anchored in existing control and government auditing standards, internal audit functions can easily adapt it to their organization's needs.

Defining the basic conditions for accountability in all respects of the AI life cycle, the GAO AI framework is organized around four complementary principles:

- **Governance** Promote accountability by establishing processes to manage, operate, and oversee the implementation.
- **Data** Ensure quality, reliability, and representativeness of data sources, origins, and processing.
- **Performance** Produce results that are consistent with program objectives.
- **Monitoring** Ensure reliability and relevance over time.

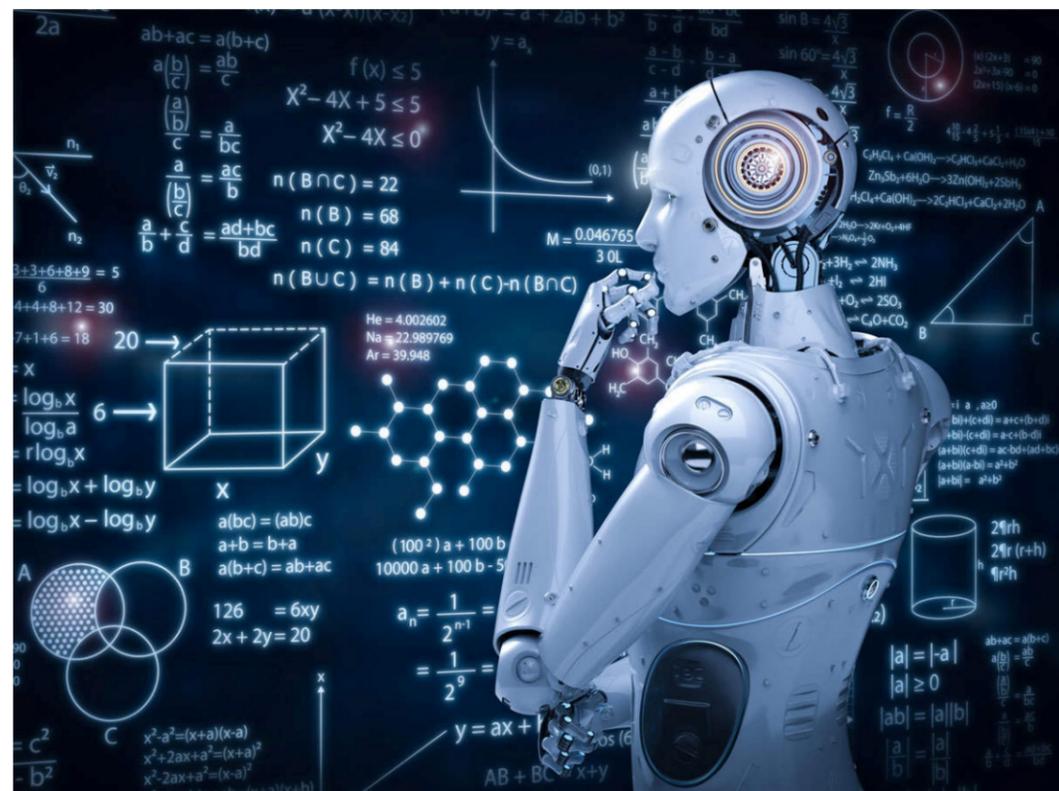
Specific questions, and audit procedures for each of the four framework principles expanded upon governance, data, performance, monitoring- are

available.

4. IIA Artificial Intelligence Auditing Framework

Comprising three overarching components Strategy, Governance, and the Human Factor and seven elements Cyber Resilience, AI Competencies, Data Quality, Data Architecture & Infrastructure, Measuring Performance, Ethics, and The Black Box

Commission (PDPC) in conjunction with the World Economic Forum Centre (WEF) for the Fourth Industrial Revolution (4IR), the Model Artificial Intelligence Governance Framework second Edition focuses on four broad areas internal governance and measures, human involvement in AI-augmented decision-making, operations management, and stakeholder interaction and communication as a baseline set of considerations and measures for organizations to adopt as they roll out AI initiatives.



Though not created specifically with the internal audit function in mind, the framework and its related Implementation and Self-Assessment Guide for Organizations (ISAGO) provides auditors with useful information when setting up or analysing their organization's AI program. Additionally, their Compendium of Use Cases contains detailed

illustrations of the framework in action across varying sectors, including specific examples of how organizations have effectively put in place accountable AI governance.

the Institute of Internal Auditors' (IIA) AI auditing framework aids the internal audit function in fulfilling the role of "helping an organization evaluate, understand, and communicate the degree to which artificial intelligence will have an effect (negative or positive) on the organization's ability to create value in the short, medium, or long term".

In their three-part series entitled "Artificial Intelligence – Considerations for the Profession of Internal Auditing" (Part I, Part II, Part III) The IIA provides detailed recommendations for each of these overarching components including engagement objectives and procedures internal audit can use as it formulates an AI program in accordance with their organization's risk profile and strategic objectives.

5. Singapore PDPC Model AI Governance Framework

Created by Singapore's Personal Data Protection

Getting AI Auditing right for your organization

Whether starting an AI program from ground to up or are seeking to add an auditing structure to an existing one, these AI auditing frameworks can be used as a starting point or more generally as a point of reference. Note that each framework does not necessarily need to be used in isolation or in its entirety it is recommended that the auditor takes the pertinent component parts and ideas from each to build an AI auditing framework that is best suited to their respective bank and its needs.

*Augustine Okochukwu
(ProvidusBank Limited)*

Welcome address by the Managing Director / Chief Executive Officer Keystone Bank Limited. Mr Olaniran Olayinka at the 51st Quarterly General Meeting of the Association of Chief Audit Executive of Banks in Nigeria (ACAEBIN) held on 16th December, 2021 at BWC, Victoria Island Lagos with the theme: "The Role of Internal Audit in Combating the Growing Menace of Electronic Fraud"



The Chairman at today's event (Mr Yinka Tihamiyu), Executive committee and member of the Association of Chief Audit Executive of Banks in Nigeria, the guest speaker (Mr. Lawrence Amadi) and all the other distinguished guest. It is my pleasure to deliver the welcome address on your 51st Quarterly General Meeting on this 16th day of December 2021 which we at Keystone Bank Ltd. are delighted to host.

Let me start by wishing all of us, Merry Christmas and Happy New Year in advance, as we gradually come to the end of year 2021 and the beginning of a more promising and prosperous 2022.

Theme for this Quarterly General Meeting which is, "The Role of Internal Audit in Combating the Growing Menace of Electronic Fraud", should serve as a clarion call for Internal Auditors to reappraise their current and more importantly, their emerging roles in combating the growing menace of electronic fraud. I am very sure that you were deliberate in the choice of three key words used in this theme combating, menace and fraud. Fraud can be defined as "wrongful or criminal deception intended to result in financial or personal gain", while menace is a threat or danger. To combat is to fight or take action against. Putting it simple, the theme is asking all of us gathered here today, just one question:

"How do we intend to fight or take action against, the growing danger or threat of wrongful deception by criminals, using electronic means, to steal other people's money, kept in our care"?

As we know today, bulk of the money in the world has since became electronic or digital and in no time, we will have a world with less than 1% physical money. This therefore underscores the need, to devote significant resources to protecting our electronic money.

As you deliberate today, I want you to consider three (3) key issues that may be relevant to how we answer

the very important question that this theme demands:

1. How do we get our regulatory guidelines and legislative acts and laws to keep pace with, and be reflective of, the growing threats from electronic frauds?
2. How can new technologies such as Artificial Intelligence (AI) and Machine Learning (ML), provide real-time and accurate insight to internal auditors and other law enforcement agencies, during fraud investigations and forensic audits
3. How do we ensure that Fintechs and other non-bank players who interact with our customers' data comply with data privacy and other security practices

Let me conclude by acknowledging your collective efforts so far, in curtailing the negative financial impacts, of these electronic fraud in the industry, majority of which, the losses were prevented, and the bad actors arrested and handed over to the law enforcement agencies for prosecution.

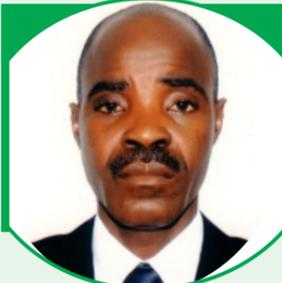
Once again, I wish you fruitful and enjoyable deliberations.

Thankyou.

ACAEBIN meeting with the Chief Judge of Lagos State, Hon. Kazeem Atogba and the Management Team of the Lagos State Judicial Service Commission at the State High Court, Ikeja Lagos.



Happy Birthday Distinguished CAEs

| | |
|---|--|
|  <p>Abiodun Okusami Keystone Bank January 01</p> |  <p>Abdullahi Usman Jaiz Bank January 29</p> |
|  <p>Ugoada Chikelu NOVA February 09</p> |  <p>Adebowale Odunola FCMB February 27</p> |
|  <p>Emeka Owoh Standard Chartered February 27</p> |  <p>Soridei Akene Heritage Bank March 03</p> |
|  <p>Rotimi Omotayo POLARIS BANK March 05</p> |  <p>Femi Fatobi RMB March 07</p> |
|  <p>Gboyega Sadiq UBA March 21</p> |  <p>Sadiku Kanabe THE INFRASTRUCTURE BANK PLC March 23</p> |



Dr. Seye Awojobi,
Registrar/CEO CIBN

Collaboration Key to Achieving a Truly Independent Internal Audit Function...

The notice for this interview though short and coming at a time the Registrar/CEO was in the thick of the recently concluded Annual Conference of the Chartered Institute of Bankers of Nigeria (CIBN) which he superintends, Seye Awojobi braced all the odds to ensure he kept faith to his commitment. Adorning a bow tie on a sparkling white shirt, this Ago Iwoye-born knowledge advocate and

administrator quickly settled into his executive chair, ready to field questions from the editorial crew of the Eagle Eye Magazine after the initial meet and greet. This Agric Education graduate-turned Banker and Administrator has steered the ship of the CIBN, introducing policies and programmes that has made the Institute, the number one hub for financial knowledge education and a critical stakeholder in the

Nigerian financial industry and the economy as a whole. In this interview, Dr Awojobi said that he couldn't have found a better fulfilment in life than combining his love for education and passion for the banking industry. Excerpts:

Sir, kindly take our esteemed readers through who Dr. Seye Awojobi is? – your upbringing and journey to becoming the Registrar of CIBN?

Seye Awojobi is professional banker who started his career about 35 years with National Bank in 1986. From there I moved to Afribank, People's Bank and a couple of Mortgage Banks before joining the Chartered Institute of Bankers' of Nigeria (CIBN), Lagos Branch as an Administrative Manager and later to the National Secretariat from 2000 till date. I was born 59 years ago to a humble family in Ago Iwoye, Ogun State, Nigeria. I progressed through the various stages of educational cadre from primary to secondary, Teachers College, College of education and the University. In fact, it has been a gradual journey for me, doing what I know best proffering banking education.

Looking at your profile, one would notice that you have been with the Institute for over two decades. How would you describe your experience so far, especially as the head of the Institute?

You see between 1986 and 1996, I was shuttling between banks, starting with the National Bank. There is this saying that the sky is your limit if you are honest and hardworking. Despite the fact that I had a higher degree, I joined the banking industry as a Clerk because of my love for the banking profession and it was deliberate because it was a deviation from the course I studied which was Agricultural Education. So because of that passion for banking, I qualified as a professional banker within my four years in the industry as such, natural instinct will want to make you grow and achieve higher. However, there were industry challenges at that time and in between moving to 4 different banks within a spate of ten years, I did introspection and decided to retrace my steps having answered some critical personal questions. So, in search of personal fulfilment, I decided to combine my love for education and banking. I was employed by the Institute as Branch Administrative Manager in 1996, having sought the counsel of some of my mentors. Within four years of working at the Lagos branch office, the national secretariat saw the potential in me and deemed it appropriate to move me from the branch to the national level as Assistant

Manager – a position lower than the full manager I was at the branch. But I was not discouraged because rather than lose that banker in me, I converted the energy to providing banking education. So, it was a deliberate preparation by me to become a banking capacity builder rather than a practising banker. Let me also mention that while I was at the national secretariat of CIBN, offers were coming my way to head the training centres of some banks but I resisted the urge to move. Anytime I look back and see the number and calibre of persons within and across the industry, regionally, and internationally that have passed through me in the Institute, I feel fulfilled. Lest I forget, I had a stint with Amicable Insurance during the days of universal banking just to have an all-round financial industry experience. So in summary, my experience here at the Institute has been a fulfilling one to the glory of God.

How would you best describe what the Institute does to a layman on the street?

The Institute is a Self-Regulatory Organization (SRO) and statutorily, it was established through a federal legislative Act 5, 2007, which was a repeal of Decree 12 of 1990 that made it a Chartered Institute. However, historically, the Institute was established in 1967 as Nigeria Institute of Bankers and it was then a body or branch of the London Institute of Bankers. By the Institute's establishment, it is expected to regulate the conduct of professional bankers, it has the mandate to regulate, supervise, provide the skills and knowledge to any person that aspires to or called a banker. It is equally an institute that is expected to enhance and ensure that people live by the ethics and professionalism of the banking profession. It also had the mandate to conduct research and espouse through advocacy, to its teeming stakeholders, which cuts across the entire spectrum of the economy namely; banks, employees, government, banking public, academia, and international institutions. So the institute focuses majorly on capacity building, behaviour, conduct, ethics and professionalism, skills and competencies required of a banker are the issues the Institute is addressing through several channels.

What has been the biggest challenge for you in the course of your career, especially in CIBN and how have you been able to overcome them?

I can situate the challenges into three; personal, institutional and industry. Personal challenges were those values required from one as a banker; however, there are conflicts between this value and societal expectation that a 'banker must

have money.' Also the challenge of desire for career progression and upliftment is another one, however, not all strive to achieve that in terms seeking the right knowledge. A whole lot of us are comfortable when we work as employees and because the society appreciates us, sometimes we are driven to a certain level that pressure comes on us. So we must imbibe the values of honesty, trust and confidence and if you are not able to control yourself through these values, the tendency for one to want to live up to that societal pressure is high irrespective of the position you occupy in the bank. Some of us have been able to surmount



these challenges because of the above mentioned traits we imbibe.

On institutional, the banking industry changed when new investors came into the industry to upstage 'armchair banking' as such, the economy was opened up and the pressure became high such that you need a lot ingenuity in order not to lose the values of banking which are honesty, trust, confidence. So, the coming in of new investors opened room for a lot of sharp practices to the extent that target setting became the order of the day. Even you, the Chief Audit Executives (CAEs) were required to meet certain targets. So, this birthed institutional pressure which resulted in failed banks because character and value were compromised. People who were supposed to grow with the industry were turned to the streets and that pressure robbed-off on the industry and economy as a whole. However, CIBN and other stakeholders stepped in and stability and confidence was restored through knowledge improvement, guaranty of the required competency and advocacy, such that today, things are a lot better and the banking industry is stronger. These are some the challenges but we have been able to overcome them in a way.

Part of the responsibilities of the Institute is to

ensure ethical standards and professionalism among members? Are there sanctions against erring members and how are such sanctions being enforced?

Yes, there are ethical standards in the industry and 'trust' ranks first in the list. Let me refer you to Creed 5 of the Mac Lords Bankers Creed of 1863 which states; "Pay your officers such salary as to enable them live comfortably and respectfully without stealing and require of them their entire services. If an officer lives beyond his income, dismiss him. Even if the excess of his expenditure can be explained, consistently with his integrity, still dismiss him. Extravagance, if not a crime, very naturally, leads to crime. A man who spends more than he earns cannot be a safe officer of a bank." This is to tell you that as far back as 1863, there are standards. So the Institute has standards for her members and that is why the Act Nos 5(2)(2) of 2007, states that anyone that works in the bank today must be registered as a member of the Institute, though you may not take the exams but subsection 2 further stipulates that Corporate members shall cause their

employees to be registered as members of the Institute. The reason is this; a lot of people come into organization for purposes of what they will get or for visa to travel out of the country or steal money or get rich or rip-off the industry but how can they be controlled ethically? If you register as a member of the Institute, you are under the oath of the Code of Business Conduct as approved by the Bankers' Committee. One of such standard is that anytime you are reported for violating any rule that guides banking, you will face the Investigating Panel of the Institute.

The Institute has two investigative panels namely; Investigative Panel of the Sub-committee on Ethic and Professionalism which deals principally with conflict between Bank(s) and Customer(s) and between banks. There is also another Investigative panel where registered members of the Institute are tried. It is the Disciplinary Tribunal of the Institute which has the status of a high court. If the investigative panel finds a member culpable, it will issue a recommendation to the Disciplinary Panel and such person would be blacklisted. This Tribunal works with the CBN and you cannot get another job in the industry and your membership will be

withdrawn. Such person can even be recommended to a higher disciplinary measure if it is a criminal offence beyond unethical practices. Just recently, some students who cheated during one of our exams have lost their job which was part of the recommendation of the investigative panel. So there are various degrees of penalties to people who violate the standard of the Institute.

As a critical stakeholder in the banking industry, how would you assess Nigerian banks, especially in the area of compliance with global best practices on one hand and business competitiveness on the other hand?

Before I go into the specifics, let me say this unequivocally that Nigerian banks need to be applauded for what they are doing in the economy and by extension, the world. However, I think the contribution of the banking industry in the economic growth of the nation is under reported. Our payment system ranks high within the world banking space. In terms of governance, the banks need to continue to improve; however, this is a global challenge. Our banks have also done well in the area of mitigating cybersecurity. I receive monthly fraud returns and I can categorically state that our banks are doing well.

Let us look at the internal audit function. How would you assess the internal audit function in the delivery of its core mandate and as a valued stakeholder?

Before now, you know we used to have a big unit called the Inspectorate Division but with the emergence of the Basle Accord and risk management activities across the banking world, we now have three major departments namely; Internal Audit, Compliance and the Risk Management. This has really proven to be a good initiative. There is a collaborative cross-cutting level amongst the three and CIBN deals with the three in area of capacity building, operational institution and the level of risk management. ACAEBIN plays a major role in the sub-committee on Ethics and Professionalism. The level of support and collaboration within the Association and other critical stakeholders is quite commendable and has helped to increase your value addition. Internal Audit is sometimes misunderstood or seen as a 'policemen', and that is what it should be. The vigilance of the internal Auditors and your Association's collaboration with the Police, EFCC, NFIU, SFU and other relevant security agencies has helped in no great

measure to secure and protect the asset of banks by mitigating risks and CIBN appreciates this. This however is not to say that there is no room for improvement in the Internal Audit Function and the only way to achieve this is to continue to up skill. I will not want to add metrics to it but the internal audit is doing well.

What area would you advise the internal audit to focus more attention and energy on?

If a SWOT analysis is conducted on the internal audit function with focus on the threats alone, one of such areas of focus is the attempt at violating operational rules and policies thereby exposing the banks to risks. It is the duty of the Internal Audit function to ensure that staff have sufficient information and knowledge to enable them perform their duties bearing in mind that your roles entails being proactive and not reactive. Having said the above, there is this saying that 'you cannot give what you don't have.' So, Auditors must continually train and retrain themselves so as to be able to give the right kind of advice. The Internal Audit must strive to shake-off that public notion of 'a policeman looking for who to catch' to being a valued critical stakeholder collaborating with the other units to ensure the protection of the asset of the shareholders and the banking public. I don't know if you are familiar with the Financial Conduct Authority (FCA) in United Kingdom (UK)? These are authority given to individuals in your capacity that works in other banks to exercise some level of independent, conduct and protection such that the institution cannot make them to compromise. These means that as CAEs, there should be some level of protection by the system that allows you to do your job without interference or threat, however subtle. I think ACAEBIN should collaborate with the CIBN to help her push for some of these things and become the Association voice in issues like this.

The Internal Audit through your Association should also strive to produce more people that occupy executive positions. Also, the need for collaboration cannot be over emphasized especially with the Regulators.

How can the Chartered Institute of Bankers of Nigeria (CIBN) assist in strengthening the independence of Internal Auditors in banks and shield the ethical Chief Audit Executive from vindictive managements?

CIBN is always available and ready to defend professionalism in the industry. We are ready to

support all the affiliate bodies in industry to ensure effectiveness and efficiency of the system. Having said this, CAEs should not see redeployment to other units as victimization but an opportunity to continue to add value into the system. The Financial Conduct Authority of UK started as a result of an anomaly that happened in their system over there and stakeholders came together to find a solution, hence the birth of FCA. So, in the same vein, ACAEBIN should begin to collaborate more with other stakeholders in finding solutions to

describe as the major challenge facing Nigerian banks and what area(s) would you advise banks to concentrate more effort at addressing? What solution would you be proffering?

We have the challenges of cybersecurity or cybercrime. What gives the industry sleepless nights today is the vulnerability to cybercrime. Every bank should ensure that it is protected from this menace.



the issues affecting the internal audit function.

Auditors are sometimes faced with the challenge of conflict of interest in the discharge of their duties. As a stakeholder in the banking industry, what would be your advice to them on how to find a balance without compromising their independence?

The truth is that you cannot run away from conflict of interest but you can overcome such challenge by imbibing the character of integrity. However, any conflict of interest that is antithetical to regulatory guideline and international best practice, either for the CAE or the organization should be avoided. One of the truest tests of integrity is the blunt refusal to be compromised.

On a final note, in your assessment, what would you

Also, there is the need for continuous knowledge education and training, so that we can meet the needs of our customers.

Further to the above is the high level of Non-Performing Loans (NPL) in the industry. Though, the Regulators are making effort at mitigating this through the issuance of Global Standard Instruction (GSI). Like I said earlier, the only way we can achieve efficiency of our operations and systems is through continuous collaboration.

Finally, I want to crave the indulgence of ACAEBIN to take the challenge of ensuring your various organization registers every of her member with the Institute for the benefit of ethics and compliance as such, reduce operational and knowledge risk. Thank you so much for having me on your platform.



Understanding the Spread of Fintechs' Offerings within Banking Applications and the Internal Auditors' Checklist

1.0 BACKGROUND

The Central Bank of Nigeria (CBN) contextual framework on inclusive banking has been enhanced by the multiplicities of FINTECH companies in Nigeria. This expansion will aid increasing expertise in developing electronic solutions and applications to solve the banking needs of all and sundry irrespective of locations. In 2021 the CBN issued licences to mobile network entities including MTN Group; and in the same vein finalized and launched the E-Naira Project. These initiatives, gives indication of the greater roles FINTECH companies will play in the future of financial service delivery.

Given the speed of innovation and the evolving regulatory space for FINTECH companies in Nigeria, financial institutions are collaborating with regulatory technology (Regtech) solutions to enhance greater regulatory compliance across all technological frontiers. Requirements for more rigorous data protection, confidentiality and privacy have led FinTech companies to, as part of their 'Regtech' offerings provide blockchain, cybersecurity

and other technological-enabled services to enable banks and other financial institutions to comply with data protection, risk monitoring, reporting and know your customer (KYC) requirements.

Several classes of Fintech's offerings have emerged amongst which are:

- ✓ Electronic payments
- ✓ Alternative lending and digital credit
- ✓ Public revenue collection
- ✓ Other banking services
- ✓ Investment and financial management
- ✓ Foreign exchange and remittance transaction
- ✓ Blockchain, digital currencies, crowdfunding and alternative financing

2.0 FINTECH SECTOR REGULATORS IN NIGERIA AND OBJECTIVES

The regulators of Fintech Sector in Nigeria are not only the CBN as it is being widely held. Though the CBN has the mandate to issue licences to banks and other financial institutions in line with Bank and Other Financial Institution Act 2020 (BOFIA).

Companies playing in the Fintech space, offering financial services to Nigerian Consumers must obtain the necessary licences and comply with CBN applicable guidelines. Other institutions involved in the regulation of Fintech companies in Nigeria are as listed below:

- ✓ Nigeria Deposit Insurance Corporation (NDIC)
- ✓ The Security and Exchange Commission (SEC)
- ✓ The Security and Capital Market Regulator in Nigeria
- ✓ The Corporate Affairs Commission (CAC)
- ✓ The Nigerian Communication Act
- ✓ NITDA – National Informational Technology Development Agency
- ✓ NAICOM Act 1997
- ✓ FCCPA – Federal Competition & Consumer Protection Agency – this body prohibits anti-competitive practices within the fintech space in Nigeria.

2.1 KEY OBJECTIVES

- ◆ Sustain the confidence of all and sundry in the evolving and growing Fintech sector in Nigeria.
- ◆ Defend the value of the naira via comprehensive regulatory oversight and control
- ◆ To make financial activities visible for regulatory monitoring and control
- ◆ To combat money laundering and corruption
- ◆ To promote accountability, accuracy and transparency

- ◆ To build a strong and well-regulated financial market that would protect consumers
- ◆ To reduce possible capital flight through emerging market
- ◆ Build regulatory certainties in blockchains within the fintech space.

3.0 FINTECH PENETRATION IN NIGERIA AND PROJECTED VIABILITY



CBN projection of growth accruing from Fintech penetration in Nigeria revealed that revenue will reach \$543 million by 2022, driven by increasing smartphone penetration amongst the unbanked populations. In 2019, Nigeria officially recognised its first Fintech unicorn, with Interswitch achieving a valuation of \$1billion based on a \$200 million investment from VISA.

Given the increasing smartphones and internet penetration coupled with technology savvy army of youths as well as high number of unbanked populations, the revenue projection would however continue to grow year-on-year. However, the dangers of insecurity, malicious attacks and other fraudulent acts within the dark web would continue to be a global bane. As Internal Auditors, we have a major role to play in identifying potential material misstatements capable of resulting to income leakages for banks and the financial industry in general.

4.0 ARE THERE EMERGING RISKS WITHIN THE E-PAYMENT SYSTEMS WITH FINTECH COMPANIES INVOLVEMENT?

In addition to existing inherent risks on the e-payment platforms for banks and other entities, Fintech companies integrating into the banks' application program interface implies that risks are being onboarded knowingly. However, the risk is moderated in view of the associated benefits of 'purposeful marriages' with Fintech Companies and control mechanism required to keep the risks within appetite. Therefore, Internal Auditors must be ready to identify

these possible risks and other emerging ones ahead of time and take proactive steps to manage them. Some of



4.1 VULNERABILITIES WITHIN E-PAYMENT SYSTEM IN BRIEF

| S/N | RISK TYPES | VULNERABILITIES' CAUSES |
|-----|---------------------------|--|
| 1 | System Risk | <ul style="list-style-type: none"> ■ Repetitive network glitch; ■ Frequent system downtimes; ■ Inadequate security infrastructure to detect and mitigate threats. |
| 2 | Credit Riskk | <ul style="list-style-type: none"> ■ Character of the borrower – borrower reputation (past records of transactions); ■ Conditions – any economic conditions that might affect the borrower; ■ Collateral – After search report has been obtained, using borrower's BVN, financial asset balances < than obligor's exposures. |
| 3 | Liquidity Risk | <ul style="list-style-type: none"> ■ Insufficient funds in customers' accounts; ■ Nil cashflows inflows (zero credit balances). |
| 4 | Operational Risk | <ul style="list-style-type: none"> ■ Frequent System downtimes; ■ Significant human errors (thin line between error and fraud); ■ Substandard workstation or ineffective devices (nil window, android or iPhone operating system – not IOS enabled) or devices without internet features. |
| 5 | Settlement Risk. | <ul style="list-style-type: none"> ■ Unimpacted balances due to delay at the point of settlement; ■ System glitch; |
| 6 | Information Security Risk | <ul style="list-style-type: none"> ■ Nil baseline controls – set of minimum-security controls defined for a low-impact, moderate-impact or high-impact information system; |
| 7 | Compliance, Legal | <ul style="list-style-type: none"> ■ Breach to customers' confidentiality, integrity and availability (CIA); |

5.0 OUTLOOK OF FRAUD HISTORY WITHIN THE FINTECH SPACE IN NIGERIA

Fig 1.

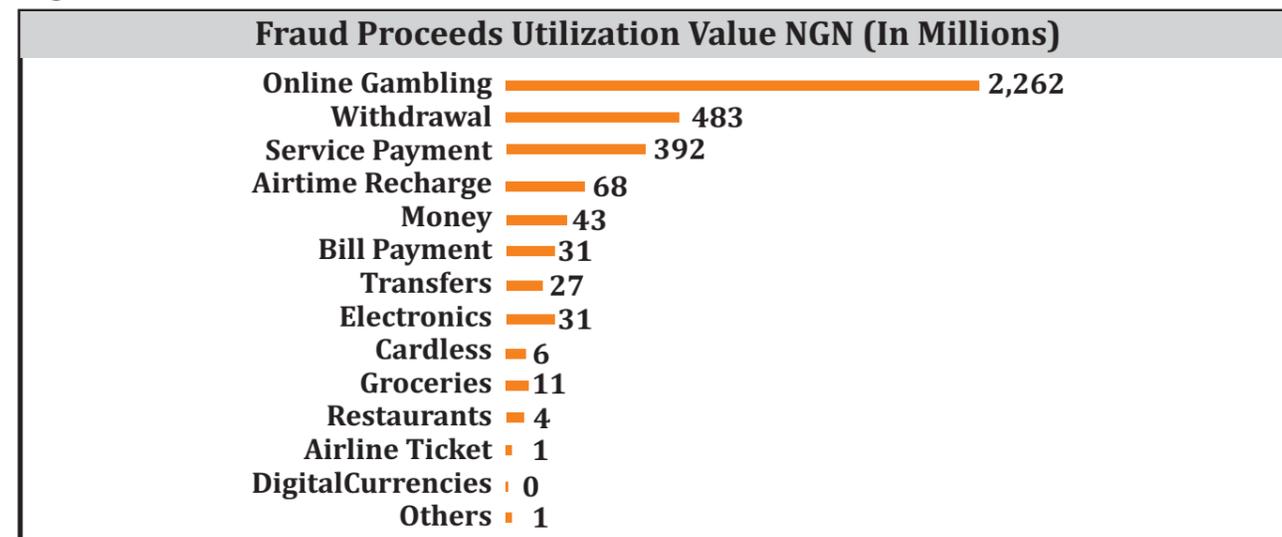


Fig II.

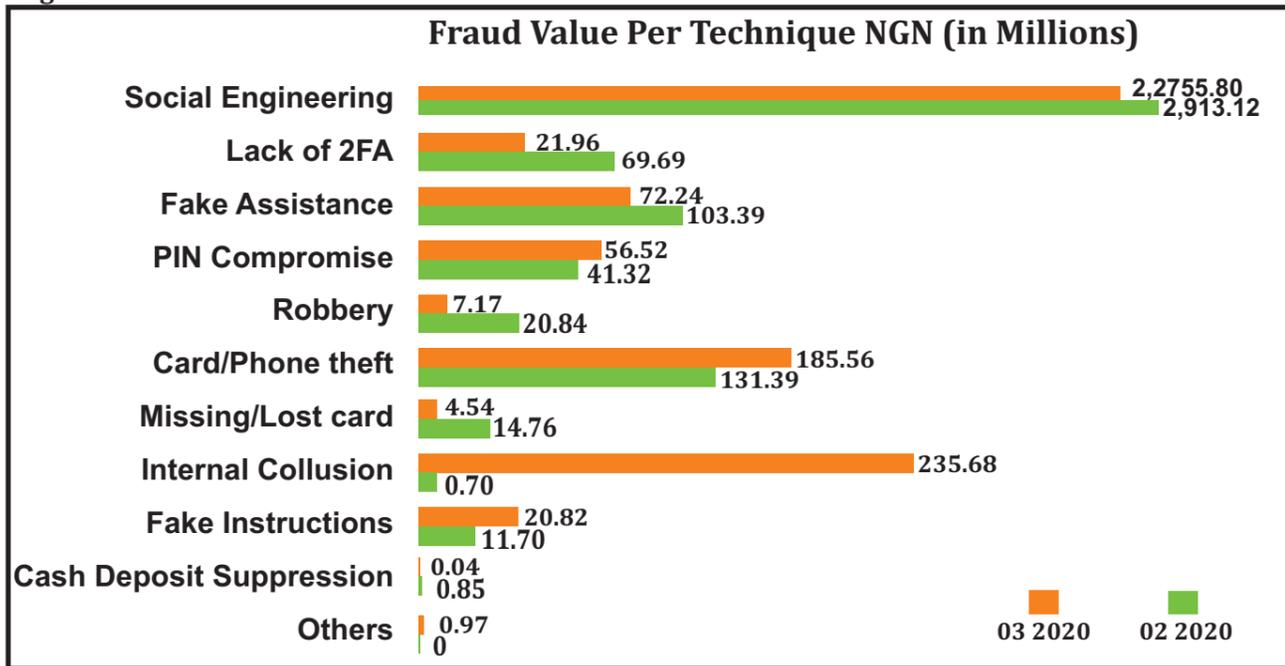


Fig III.

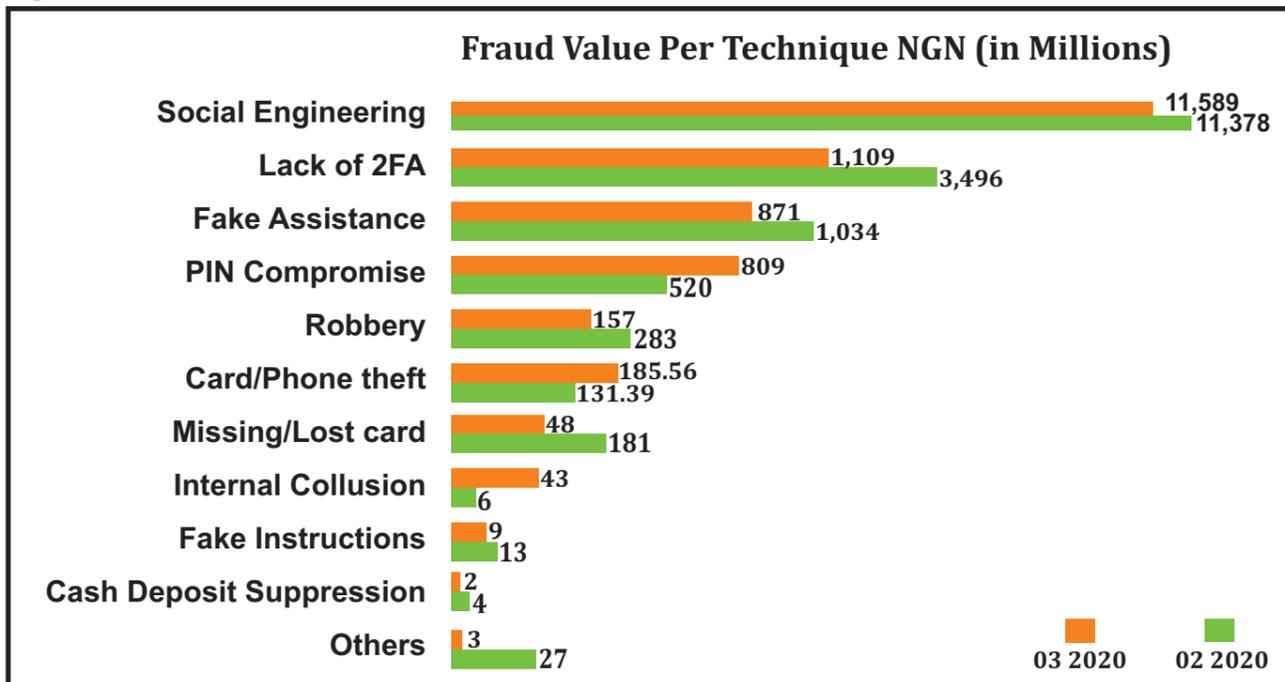


Fig IV.

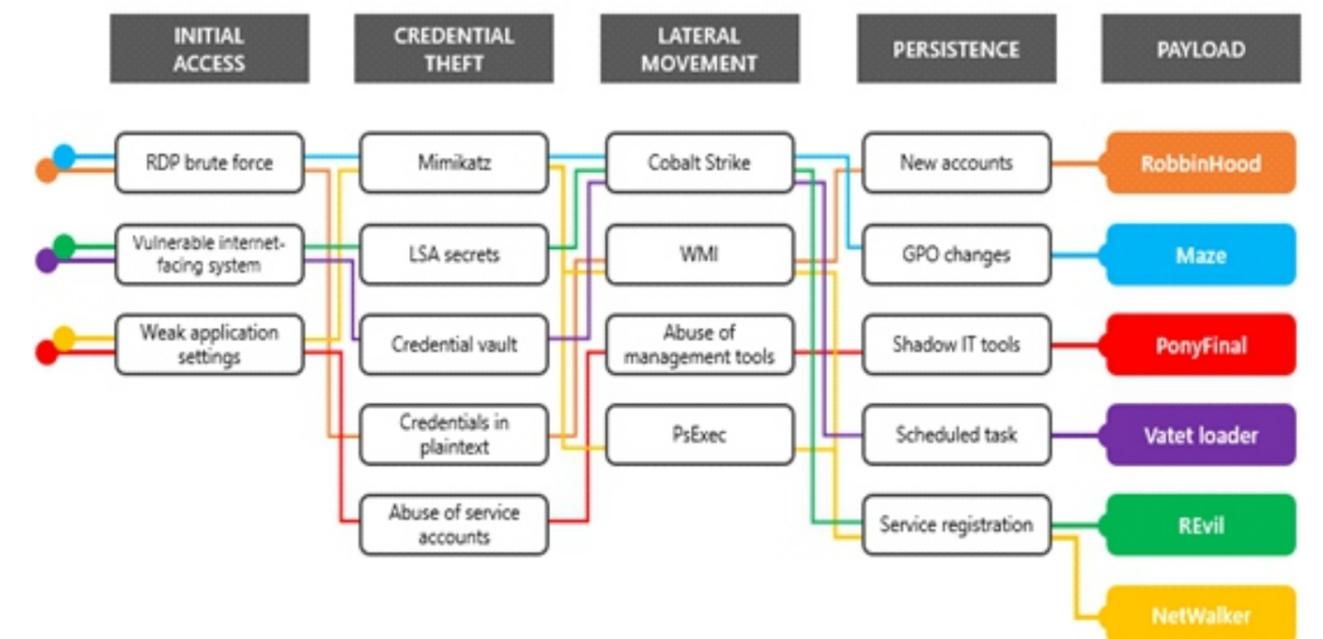
| Channel | Fraud Interest Index |
|--------------------|----------------------|
| ACROSS THE COUNTER | 0.86% |
| ATM | 6.05% |
| CHEQUE | 0.02% |
| E-COMMERCE | 0.10% |
| INTERNET BANKING | 1.92% |
| MOBILE | 25.36% |
| NON ELECTRONIC | 1.00% |
| POS | 4.46% |
| WEB | 60.23% |
| TOTAL | 100.00% |



these risks are as shown below:

- ◆ Unusually large orders or high-priced orders
- ◆ Fake telephone numbers (example 666-897-56340)
- ◆ Inconsistent address information (example: zip code does not match state or city)
- ◆ Randomly generated email address consisting of numbers and letters
- ◆ Use of fake website address – (example http://www.zyz.com)
- ◆ Multiple emails with request to fill questionnaires (phishing) and win expensive gifts – by complying with these solicitations, potential hackers would have access to your IP addresses etc and subsequently use same to carry out malicious attacks on your accounts.
- ◆ Email/correspondence conveying identical names or surnames (Business email compromises – BEC).
- ◆ Calls from fraudulent persons requesting you to partake in 'fake' project within the community in the form of 'international NGOs' with the intent to get access to your current and historical information.
- ◆ Offering of mouth-watering benefits for doing 'near to nothing' – please beware!!!

6. 1 RANSOMWARE TACTICAL STRATEGIES



7.0 IMPLEMENTABLE CONTROLS/AUDIT CHECKS WITHIN FINTECH'S SPACE (CARDS, E-CHANNELS ETC)

- (1) Confirm the availability of 3-tier architecture (web servers, application servers and data base server);
- (2) Ensure proper documentation of vendor agreement over cards, e-solutions and other e-channels.
- (3) 100% adherence to the compliance requirement of the twelve standards prescribed by Payment Card Industry Data Security Standards (PCIDSS)
- (4) Strong controls over cards production, priming etc, by ensuring that outsourced entities comply with the established due diligence criteria or documented policy.
- (5) Ensure that third party applications integrating with internal bank systems poses no risk to the existing data base.
- (6) Access to data (customers cum staff members) could be mismanaged for personal gains if not guarded appropriately.
- (7) Specifications and clauses within SLAs or MOUs between banks and FINTECH Companies should not be executed without respective detailed inputs from parties.
- (8) Confirm the status of the 'privacy laws' within the documented SLA by the parties.
- (9) Possible penetration of middleware application if not fully encrypted.
- (10) Evidence of documented change management guidance notes
- (11) Confirm to ensure that all source codes are secured to enable the entity to make necessary amendments, revalidations to existing running programs.
- (12) Ensure secured configuration of the security architectures.
- (13) Confirm that security metrics and service level agreement are duly executed.
- (14) Identify and avoid ineffective cloud-based solutions and understand new encryption technologies.
- (15) Use your expert resources to walk-through and test ransomware scenarios.

8.0 CONCLUSION

Heavy reliance on technology infrastructure means that firms can be vulnerable. Technology failure can mean that customers are unable to access services resulting in Loss of income or customers.

Given the nature of Fintech companies' services, they are prime targets for cyber criminals. Network security, data breaches, denial-of-service (DOS) attacks and rectification as well as other incidents which often crystalize on technology dependent processes should be of concern to the auditor.

Ransomware controls requires that there should be weapons-grade data back-ups; religious patch management, incident response plan and customers should know how to call as well as training and testing staff of the respective insitutions with internally generated suspicious mails.

*Julius Oreye,
Head Office Audit, Heritage Bank Plc.*



Advancing the Auditing Techniques in the Pandemic and Post Pandemic era

Auditing in the Pandemic and Post Pandemic era has led to a lot of new developments and techniques in Auditing in the world as we know it today. Auditors have begun to embrace the new normal to cope with the health risks emanating from exposure to COVID. The various government's extant rules and COVID protocols leading to lockdown of businesses and social distancing measures has led to crippling activities of various companies and businesses, while many other new companies and businesses especially in the technology space has sprung up given the prevailing opportunities arising from the lockdowns. Hence, opportunities now abound in the contactless space, where technology has been the main driver of our economy.

Now, virtually all aspects of the economy ranging from Health, Education, Entertainment, Finance and even Electioneering has found its way in modern technological advancements through the use of various mobile Applications, FINTECHs and other App platforms occasioned by the urgency to meet the needs of customers in the pandemic era. Since we are now in a modern world where technology has continued to prevail, auditing as we know it has to evolve with the changing times. This article helps to shed light on the aspects of Auditing affected most by these changes and how Auditors can navigate some of the challenges thrown up by the pandemic.

One of such techniques is **Online Audit**. This

technique involves the collection of audit evidence with the use of an automated system and at the same time analyzing the information obtained in a paperless environment. Online Audit has different imperatives for internal and external auditors. With the advancement in technology (Skype, Teams and Cisco Webex) videoconferencing, internal and external audit can now be conducted without stress. This has also led to reduction in travel expense, increased reliance on technology and use of Audit software for data mining and complex computations. The drawbacks of online Audit are; it can be expensive to set up or acquire, some technical knowledge is required, network downtime and compatibility with the entity's software.

One of the core challenges of Auditing is the inability to carry out physical test of inventory or on-site count of stock commodities such as cash, financial instruments (stock of cards, tokens, Cheques) and other items. It is important for auditors to recognize that there are alternatives to physical inspections. For any organization or business where inventory considered very material to the business, the existence of that inventory is going to be a relevant assertion. And in the vast majority of cases, historically, it has just been generally accepted that the way that an auditor can test the existence of that inventory is to physically observe its counting and that may entail the use of the **Roll forward and roll back technique**.

The roll forward and roll back technique entails that Auditors can work with the client/Auditee and think whether it would be possible and realistic to postpone the inventory counting and observation to a later date when restrictions are a bit relaxed and/or convenient for both parties. The auditor could count inventory and observe it at that point and then perform additional testing on the sales/withdrawals subsequent to the cutoff date or year-end as well as subsequent deposits and reversals. You could

forward to year end. Again using sales/withdrawal transactions and purchase/Deposit transactions and testing those during that interim period. Therefore, the roll forward and roll back are alternative approach that could be adopted

The Video Observation. This is another technique for attending physical inventory counting. One question for us to answer is “Is it even permissible under the auditing standards to not physically count inventory in person”? One aspect is that

International Standard on Auditing 501 Paragraphs 4 through 11 reference the requirement to attend the physical inventory counting unless it is impracticable to do so. There are actually some application paragraphs (Paragraph. A34 of AU-C ISA 501) that indicate that one circumstance that may make a physical observation impracticable is if the inventory is held in a location that may pose threats to the auditor's safety. The overriding consideration when using remote video is that the auditor needs to have a pretty good feel for the authenticity of the video



effectively roll back the inventory to the year end, even if it was counted subsequent to year end. Actually, this is not an extraordinarily thing for auditors to do, especially in situations where the auditor was engaged to perform an audit after the year end or after the inventory had been counted in the absence of the auditor. This process simply involves carrying out computations either by adding withdrawals/sales and deducting deposits/purchases to arrive at the closing balance of the inventory counted.

feed. If it's a live situation where perhaps someone from the client is on-site and can send a live video feed back to the auditor for them to watch, that makes it easier to determine authenticity. If you're using, for example, Skype or Zoom and somebody is actually walking around to the inventory and counting it in response to verbal commands of the auditor with an interactive dialogue, then you can be pretty comfortable of the authenticity of the procedure.

The other more traditional alternative procedure can be performed if the client is using a **cycle count procedure and a perpetual inventory system** (i.e., automated process for inventory management). A cycle count procedure is where the auditee/client essentially has controls in place where on a periodic basis, e.g, monthly, quarterly, they will conduct their own test counts of just a portion of their inventory. And then they go back to their perpetual system and prepare the counts, make corrections. Hence, with cycle counting, the client/auditees don't perform one huge year-end, wall-to-wall count in most cases. If the auditor had been testing those controls and relying on those controls to establish the existence of inventory, the auditor may be able to go back to the last prior cycle count that was taken and then be able to roll

The need for Auditors to meet up with deadlines on Audit year end deliverables has also skyrocketed because owners of businesses need to meet up with regulatory deadlines, Tax filings as well as position their businesses for more opportunities after accounting for all losses occasioned by the pandemic. Therefore, the increasing demand for Auditors to meet up with the pre-pandemic Audit cycle and financial year end reports. It is on this premise that Auditors will need to evolve existing practice in our changing environment.

Francis Uzoewulu
(Keystone Bank)



Reasons for the Recent Spike in Fraud on Digital Banking Platforms and how to Mitigate the Ugly Trend in the Banking Industry

Digital fraud is a problem banking business has been facing since the advent of e-commerce in the 1990s, and its threat only increases with each passing year these crimes cost banks billion in the last 24 months. But what is causing digital fraud to rise year over year? From current trends and consumer attitudes to technological enhancements and more sophisticated tactics, let us take a look at the top reasons digital fraud is rapidly increasing:

and increasing 10 times faster than card present transactions. Now, as more consumers are staying home because of COVID-19, even more commerce has moved online.

This trend makes it even easier for fraudsters to make fraudulent transactions. Point of sale (POS) lending has also become more common, allowing customers to make payments in instalments or take out loans for purchases both large and small. While POS lending makes it easy for consumers to gain approval and make a purchase in a matter of minutes, it also opens the door to fraudsters.

1. Chaos caused by the global COVID-19 crisis.

Opportunistic hackers are taking advantage of the chaotic, global crisis to commit even more fraudulent activity. Tactics include stealing stimulus checks and unemployment benefits, collecting payments for fake COVID-19 treatments, tricking Bank customers into donating to fraudulent charities, and more. In fact, there were 1.1 billion fraud attacks in the first half of 2021, which is double the attack volume compared to the second half of 2020.

3. The advent of new marketplace platforms.

From social networks and dating apps to food delivery, alternative transportation, and vacation rentals, digital channels have revolutionized almost every industry. COVID-19 has caused a greater spike in mobile application use, with consumers ordering the delivery of everything from groceries to automobiles. With the growing number of marketplace platforms and services available and their widespread popularity -especially in recent months- fraudsters have shifted their tactics to take advantage of rising in-app and online marketplace purchases.

2. A changing e-commerce landscapes.

Another trend impacting the rise in fraud is more retail purchases shifting online. In particular, card not present (CNP) transactions have increased dramatically in recent years, with these transactions accounting for 27% of all debit transactions in 2019

4. Payments moving online.

In addition to consumers transacting more in online marketplaces, they are also using peer-to-peer payment (P2P) and e-Wallet apps more often. Users turn to these platforms to digitally split dinner checks with friends, send money to family members in other parts of the world, pay for services from a local vendor, and more. But with more than half of P2P transactions taking place between consumers and an unknown entity, the fraud risk is high.

5. Increasingly digital banking services.

Today's consumers demand more online and mobile services from their financial institutions. As a result, banks are going digital. They are doing more account onboarding and transaction approvals online and deemphasizing in-person transactions, which makes it harder to verify identities. Also, in response to consumer demands, a new breed of "challenger banks" – born and doing business entirely in the online world – have emerged and are differentiating themselves by providing easy-to-use and digital-native experiences. Most of these institutions' customers are those who have "thin file" credit histories (i.e., don't have much credit data). Less data means a greater risk of fraud.

6. New consumer expectations.

Today's consumers also expect their data to be secure. Yet they will abandon any transaction that takes too long, requires too much data, or is too complex. In fact, 92% of consumers expect a fast, frictionless experience while also getting one that is as trustworthy and secure as possible. These steep expectations are causing banks and retailers to juggle preventing losses with keeping fraud prevention measures from rejecting good customers and transactions. Cybercriminals understand the struggle these organizations face and take advantage of those that fail to strike the right balance of secure, yet frictionless customer experiences.

7. More sophisticated fraud tactics.

Due to an increasing number of data breaches over recent years, fraudsters can more easily access PII (personally identifiable information) and use it against consumers. For instance, fraudsters combine real and fake data (such as an address from one person mixed with another's social security number) to create new, synthetic identities that are harder to detect. Then, they establish open bank accounts and cards, acting like legitimate customers. Once they have established strong credit scores, the fraudsters ask for higher credit limits or larger loans and simply stop paying.

Synthetic identity fraud is damaging for consumers, but also expensive for lenders too. Fraudsters also leverage PII for account takeover. By using passwords and credentials obtained via data breaches or social engineering, they can gain control over accounts and make fraudulent online purchases. These transactions can be as minor as buying groceries on a debit card. Account takeover fraud is a serious threat for consumers that Juniper Research predicts will result in losses exceeding \$200 billion between 2020 and 2024.

8. Unclear legal jurisdiction of cross-border fraud.

Global commerce gives today's online retailers and marketplaces an opportunity to reach even more customers. Cross-border transactions do not come without some risk. Because they typically encompass multiple countries, it is difficult for individual jurisdictions to properly monitor for fraud risk. Further, data privacy and protection regulations vary across regions- if they exist at all, making it even easier for fraudsters to commit cross-border transaction crimes.

9. Technological advancements.

Today, fraud has also accelerated and grown even more sophisticated due to the rise of e-commerce, mobile payments, and computing power. Many of the same technologies that companies rely on to innovate and rapidly introduce new products and services are also being adopted by fraudsters. Criminals can more easily commit fraud using cheap, on demand compute power or deploy algorithms using machine learning that are more subtle and capable of manipulating fraud detection systems. The traditional rules-based fraud prevention systems that organizations have relied on for years now struggle to keep up.

HOW TO MITIGATE DIGITAL FRAUD IN THE BANKING INDUSTRY

In a recent global banking fraud survey, cyber-related fraud was found to be the most significant challenge faced by financial institutions today. As billions of stolen dollars make their way into fraudsters' pockets each year, banks stand to lose more than the money, but their customers and brand reputations too.

The good news is that digital banking security continues to evolve in response to changing customer expectations, technology, and industry trends. The bad news is that fraudsters too will continue to adapt their tactics to try and bypass these measures.

Banks and other financial establishments are under enormous pressure to proactively protect themselves and their customers from digital banking and payments fraud. As experts in banking app security and digital fraud prevention technology, these measures are recommended to mitigate fraud on digital banking platforms.

1. Educate your customers

Continuous engagement with customers about the dangers of fraud is vitally important. Realistic views of the risks they face, what to look out for, and tips for transacting safely are all shown to be well received. Banks also stand to gain their customers' trust by detailing the measures put in place to protect their



customers from fraud. When banks can show they have proactively secured their digital channels and are continually evaluating their options, their customers feel more at ease.

2. Use verified fraud prevention technology

The best defense against digital banking and payments fraud lies in identifying and eliminating threats before any damage gets done. A layered approach to fraud prevention has proved extremely effective at eliminating phishing and other attacks. The most successful systems call on a broad range of security features including device and browser identification, end-to-end encryption, strong app security, malware detection, and digital transaction signing.

3. Messages with meaning

Fraudsters mould to the identity of their victims,

which is why it's so important to confirm the identity of every individual attempting to log on to or transact through digital banking. The most reliable way to achieve this is through multi-factor, out-of-band customer authentication, which is proven to be far more effective than OTPs alone at reducing various types of fraud, including account takeover fraud and man-in-the-middle attacks.

4. Watch out for internal fraud

Unfortunately for banks, they are perfectly placed to attract fraudsters on the inside. In fact, research indicates that as much as 70% of banking fraud are link to insiders. The theft of bank customers' data is of particular concern, as account details and PIN codes get sold on the black market by fraudulent bank staff. While measures exist to screen and audit employees, internal fraud can go undetected for quite some time. A bank's ability to identify their customers, monitor transactions, and raise the alarm about suspicious activity in real-time is of far greater value.

5. Show you still care

Digital banking, although convenient, reduces the amount of personal interaction a bank has with its customers. But fraud is a touchy subject, and customers need an easy way reach out to their banks, report a suspected case of fraud, and be taken seriously when they do. In-app reporting features do well to meet this need, especially when paired with proactive notifications of suspicious activity and calls to action sent via a secure, in-app messaging services.

In summary, there is a great and urgent attention in the fight against fraud on the various banks' digital platforms as the survival of modern-day banking business is dependent upon the victory in the fight.

*Sunday Emeke Onwuemele CFE,
Forensic Investigation Unit,
Investigation and Fraud Management Team,
United Bank for Africa Plc.*



The 4-Dimensional Leadership Development

Preamble

The most constant factor in life is change and as such no professional or human in general should allow him/herself to be left behind in the race of excellence.

For Leaders in the corporate world be it- Executives, Senior, Mid or Lower Supervisors or Heads, it is important to always refresh or renew our knowledge and skills, so our organization can continue to deliver value to clients and meet up with designed obligations and profit maximization.

The above brought alive the 4-Dimensional Leadership Development. It is also known as **Executive Coaching**. It presents supervisors, managers, and executives a fresh opportunity to enhance their knowledge and skill capacities as effective and successful leaders.

Breakdown of the 4-Dimensional Leadership Development

The 4 D Leadership Development is a unique and exceptionally efficient approach to leadership capacity building. The model is grounded in relational, strength-based and constructivist principles and, combines a mix of knowledge, tools and strategies from human behavioral theory,

organizational development, performance management, best-practice, and evidence-based leadership concepts. 4 D Leadership Development is geared towards validating and affirming what leaders are already doing well and offers, through an individualized assessment and development approach, strategies, and a variety of processes for enhancing overall leadership capacity

The model described above comprises of 4 different stages known as Dimensions. These are listed below:

The Four Dimensions (Stages) of 4-D Leadership Development

The four stages are (i) Discover, (ii) Develop, (iii) Deliver and (iv) Discipline

1. Discover: This Dimension is the starting point. Although it initiates the process of leadership development, discovery is a process that is ongoing throughout all Dimensions and is critical for the most efficient and optimal development. Through collaboration with consultants, In-House Strategy experts and Executives, Leaders are supported to complete a Leadership Development Profile. This tool sets the discovery dimension/process in motion and results in a clear understanding of leadership experiences, strengths, needs and goals for leadership capacity enhancement.

2. Develop: This Dimension focuses on key elements cultivated and leveraged within the discovery dimension; shaping and providing direction for an individualized Leadership Development Plan.

Through a collaborative process the Leader works with a designated consultant, in-house strategists, or even executives to develop the most effective plan for prioritized and preferred areas of development. This dimension holds the greatest amount of work as it entails specifying and sharpening priority leadership enhancement objectives and the concrete steps necessary for the most efficient and successful leadership development.

3. Deliver: Delivery is dependent upon the acute vision, plan and work developed from the previous dimensions. Through clear and relevant discovery combined with individualized and strengths-based capacity development, delivery of individual and organizational outcomes is inevitable. The Leader will work with the consultant to ensure that the plan



maintains clear focus and direction and that leader's efforts are purposeful and perpetual to approximate defined and preferred outcomes

4. Discipline: This is the most critical of all. It is the result of the preceding dimensions; it is about optimal learning and leadership development (Discipline). When learning and development are optimized, there are less challenges; less of a need for the negative type of discipline (reprimands, progressive discipline, firing) for the Leader, within the team and among all staff. Leaders are supported to develop the most effective and proactive tools for decreasing challenges, challenging/resistive behaviour and increasing optimal learning and development, the greatest discipline

Benefits of the Four-D Leadership Development

- * Provides supportive and collaborative external supervision
- * Helps in implementation of Organizational Vision and Mission alignment
- * Helps leadership design and actualize purposeful intermediate and long-term personal and/or professional goal
- * Prepare leaders to develop and support staff in terms of motivation, focus, enthusiasm
- * Enhance relationship and communication skills in an organization
- * Helps in managing conflict and "crisis" situations more effectively
- * Assist in designing a proper work-life balance lifestyle

The New Path

We need to begin to see ourselves as leaders because people watch and learn from us. This happens both in our private and public lives and as such we must always upgrade our leadership skills. Change is constant and same should be applied in our skills and service delivery. The industry we have found ourselves has been the most dynamic in the globe as at today -with the support of Information Technology. What this means is we must be renewed and always refreshed and should also see ourselves as leaders who should not fail.

*Bolanle Alalade
(ProvidusBank Ltd)*



Dealing with Anxiety

The changes being experienced after the COVID-19 pandemic has caused a lot of pressure on people, families, and societies. It has affected the way people live and work. The work community is adapting to the new 'normal', while some others are waiting for life to get back to what it used to be. Work life and home life is gradually merging. The pressure to work smarter is on the rise as the need for physical offices and manual service is on the decline. To crown it all, the present inflation rate has affected everything including food, shelter etc., with little relief in sight. All these factors can lead to a feeling of anxiety.

Anxiety is an expected feeling for an average adult. One gets anxious about several issues like meeting up deadlines, preparing a tough presentation or meeting up new clients. Anxiety is necessary for survival. An example would be in the face of danger, where the feeling of anxiety is expressed in form of a raised heartbeat, defensiveness, sweating or alertness.

Anxiety becomes dangerous and eventually a disorder when the feeling of worry is not proportional to the cause. An anxiety disorder can also be detected by the length of time the anxious feeling lasts.

It is important to know what activates anxiety as this

will help prevent its escalation into a disorder. Some of the most common causes of anxiety are classified below by Medical News Today:

- ❑ Environmental stressors which include family issues, relationship issues, work issues
- ❑ Social stressors which include stage fright, fear of rejection and humiliation, fear of negative judgement and public embarrassment
- ❑ Medical factors which include symptoms of a disease, effects of a medication, withdrawal from substances/medications.
- ❑ Genetics

Some red flags to look out for when an anxiety is becoming a disorder are:

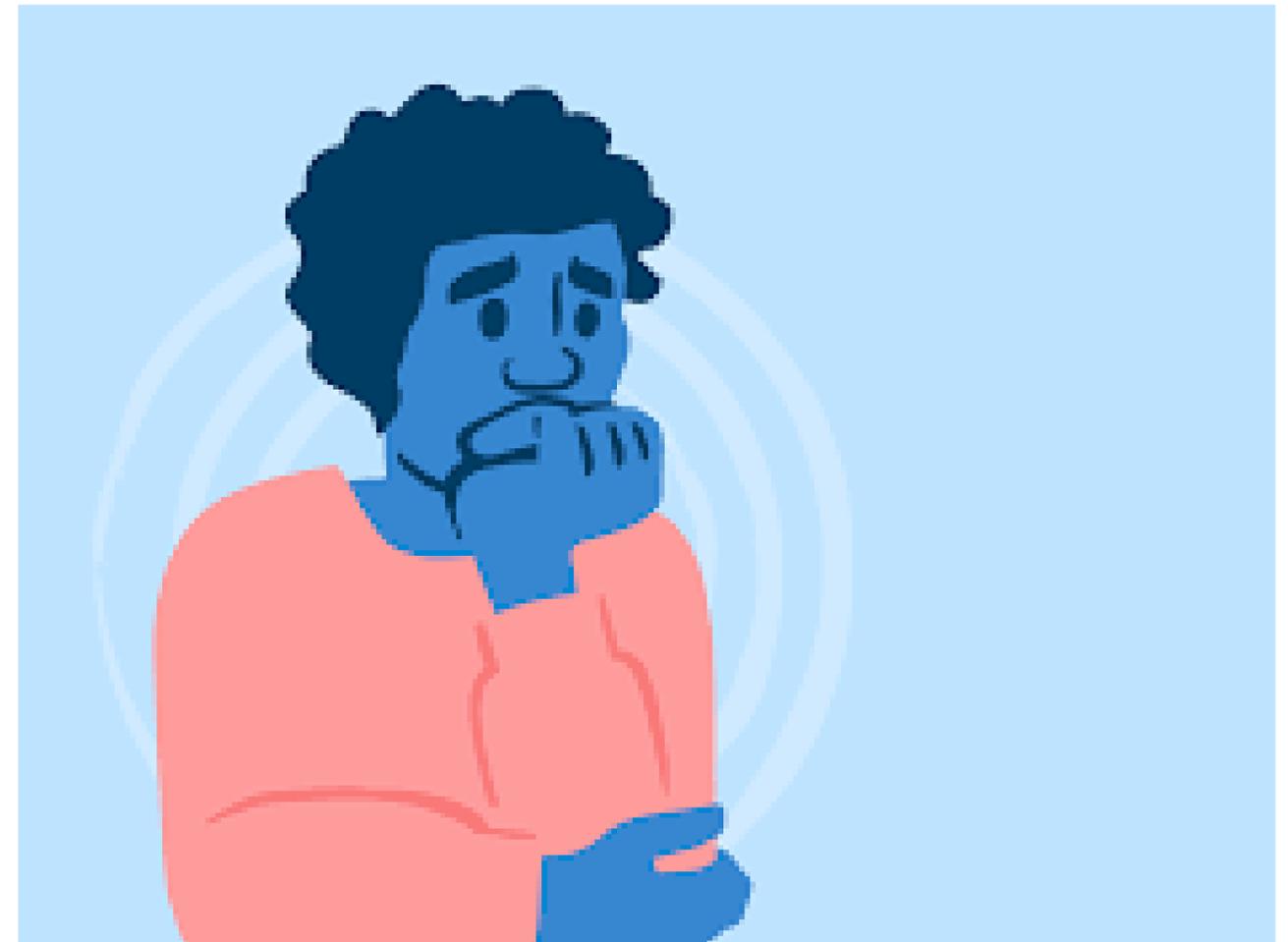
- ❑ When anxiety is affecting one's routine for example losing focus, fidgeting, or displaying extreme nervousness, sleeping disorders also known as insomnia, eating disorders.
- ❑ When one starts withdrawing from social

activities, suddenly introverted or prefers to be alone.

- ❑ When one starts experiencing physical symptoms like high blood pressure.

positive believable thoughts, hanging out with positive minded friends.

- ❑ Build a support network – always have someone trustworthy to talk to like a friend or a family member.



- ❑ When the severity or duration of an anxious feeling is not proportional to the trigger or the stressor.

What to do when red flags are spotted as suggested by Medical News Today:

- ❑ Apply stress management techniques like making a to-do list, organize tasks according to due dates, delegate where necessary, taking time off to rest.
- ❑ Apply relaxation techniques like taking deep breaths, practicing meditation, taking long baths/showers, taking vacations, exploring favorite hangout spots, yoga.
- ❑ Practice positive thinking by consciously replacing reoccurring negative thoughts with

- ❑ Engage in physical exercise – this helps release chemicals in the brain that produce happy feelings, it also improves self-image.

- ❑ Seek medical help.

In conclusion Anxiety is a normal emotion, however it can easily become a disorder which can lead to depression and mental health disorders.

Deliberate actions to maintain work-life-balance, having a good social network and investing in a balanced diet can help control anxiety. "It is health that is real wealth. And not pieces of gold and silver." Ghandi, Look out for yourself and a friend.

Nina Yalwa
ProvidusBank Limited



Access Bank Plc
Yinka Tiamiyu
Plot 999C Damole Street,
Victoria Island, Lagos
tiamiyuy@accessbankplc.com
08023220367, 2364062



Bank of Agriculture Limited
Daniel Olatomide
1 Yakubu Gowon Way Kaduna.
d.olatomide@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



Citibank Nigeria Ltd
27 Kofo Abayomi St
Victoria Island, Lagos
Tel: (234)1 2798400, 4638400 Ext. 8446
DL: (234)1 2798446, 4638446.



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



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



Ecobank Nigeria Ltd
Felix Igbiosoa
21 Diya Street, Gbagada Lagos
FIGBINOSA@ecobank.com
07068754692 ; 08023633203
D/L: 01 2260449



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



Federal Mortgage Bank of Nigeria
Wakeel Imam Galadanci
Plot 266, Cadastral AO, Central
Business District
P.M.B 2273, Abuja
wakeelimam@yahoo.com
08023040123, 01-4602102



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
Uduak Nelson Udoh
9/11, McCarthy Street, Lagos
Uduak.udoh@firstbannigeria.com
01-9054583, 08022902268



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



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



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



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@hbnig.com
08037025486



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



JAIZ BANK PLC
Abdullahi Usman
No. 73 Ralph Shodeinde Street,
Central Business District,
P.M.B. 31 Garki Abuja, Nigeria.
ABDULLAHI.USMAN@jaizbankplc.com
09-4605138, 08032089010,
08086103555



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



Lotusbank
Idowu Omitoogun
2, Bourdillon Road
Ikoyi Lagos.
Idowu.Omitoogun@lotusbank.com
08050962939, 07085343113



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



Nigeria Mortgage Refinance Company
Olusemore Adegbola
No 18 Mississippi Street,
Off Alvan Ikoku Way
Maitama, Abuja, Nigeria
oadegbola@nmrc.com.ng
08033769975



Nova Merchant Bank
Ugoada Chikelu
23, Kofo Abayomi Street
Victoria Island, Lagos.
Ugoada.chikelu@novamb.com
08091024491



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



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



Providus Bank Ltd
Aina Amah
Plot 72, Ahmadu Bello Street
Victoria Island, Lagos.
amah@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.
Emeka Owoh
142, Ahmadu Bello Way
Victoria Island, Lagos
emeka.owoh@sc.com
08037027452



Sterling Bank Plc
Cyril Osheku
1st Floor,
Sterling Bank Plc Head Office
(Annex), Ilupeju
239/241, Ikorodu Road, Lagos.
Cyril.osheku@sterlingbankng.com
08023046639, 08056656866



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



TajBank Nigeria Limited
Aminu Habu Alkassim
Plot 72, Ahmadu Bello Way,
Central Business District,
Abuja.
aminu.alkassim@tajbank.com
08032868266



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
ofamoriyo@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
08023270988