



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@acaebn.org
website: www.acaebn.org

Design+printbyProwess08039221516



Eagle Eye

A Quarterly Publication of the Association of Chief Audit Executives of Banks in Nigeria (ACAEBIN) Q2, 2022

Professional Ethics: The Moral Courage of Internal Auditor



Page 8
Cloud Computing in the 21st Century

Wellness

Page 34
Taking Care of Your Mental Health

Page 30
Managing Pushbacks in Audit Engagements

ACAEBIN EXCO MEMBERS



Uduak Nelson Udoh
(Chairman)



Felix Igbinosa
(1st Vice Chairman)



Prince Akamadu
(2nd Vice Chairman)



Gboyega Sadiq
(Treasurer)



Aina Amah
(Auditor)



Ugochi Osinigwe
(Chairman Research & Publication)



Mogbitse Atsagbede
(Chairman Payment & Systems)



Adekunle Onitiri
(Ex-officio I)



Olusegun Famoriyo
(Ex-officio II)

CONTENT

| | |
|----|--|
| 4 | Professional Ethics: The Moral Courage of Internal Auditor |
| 8 | Cloud Computing in the 21 st Century |
| 10 | The various Dynamics of Social Engineering Attacks on Nigerian Banks' Customers and the Recommended... |
| 16 | The Changing Face of Internal Audit |

| | |
|----|---|
| 23 | Internal Audit Charter as a Bedrock for Effective Performance of Audit Functions... |
| 26 | Service Level Agreement (SLA), the Audit Perspective |
| 30 | Managing Pushbacks in Audit Engagements |

Editorial



It is with great pleasure that I welcome you to the 2nd quarter 2022 edition of your flagship professional publication, the Eagle Eye. I am honoured to assume the role of the Editor in Chief of the Eagle Eye, having emerged as the chairperson of the Research and Publications Subcommittee in the 2022 Annual General Meeting which was successfully held at the onset of the quarter. The Communiqué and photo gallery have been featured in this edition for your delight. We thank the former EXCO members for all the work done to pilot the affairs of the Association and welcome on board the new EXCO members.

The recent pace of corporate failures and accounting scandals has affected investor faith in the corporations' and capital markets' openness, honesty, and accountability; the age long concept of professional ethics remains the moral courage for the Internal Auditor. This is pertinent for the fact that the nature of auditing establishes a unique position of trust with respect to customers, employers, employees, and the general public, who rely on the professional judgment and recommendations of auditors to make informed decisions. Ethical behavior involves adherence to unwritten norms and a culture of "doing the right thing." Therefore, auditors should insist on the moral value, ethical standards, and professional codes of conducts that boosts moral courage in them, which help them to carry out their work without fear or favour. This edition offers an indepth discussion on the issue of professional ethics and the moral courage it provides for the auditor.

We continue our discourse from Q1 edition on the audit Charter which also gives impetus to the internal auditor's adherence to professional ethics. It clearly defines

internal audit's purpose, authority, responsibility and position within the organisation - a precursor to the article on Internal Audit Charter as Bedrock for Effective Performance and Audit Function.

As cloud computing services are progressively gaining acceptance in 21st century organizations, their typologies, variants and risks are extensively discussed. The writer of the article gave extensive literature on Cloud Computing Deployment Models, Cloud Computing Services, Risk Associated with Cloud Computing and offered ideas on Best Practices for Storing Organization's Data in the Cloud. The menace of frauds perpetrated via social engineering has remained a bug in our everyday financial lives. We have included an article titled 'The various Dynamics of Social Engineering Attacks on Nigerian Banks' Customers and the Recommended Practical Solutions' to serve as a source of enlightenment against this scourge with practical ways to solve the same. The fight is frontal and continuous. All winning strategies, topmost which include public education, should be deployed.

Our Wellness corner highlights the need to take care of your mental health. Faced with the stress and challenges of everyday life which are multi-faceted, the need for sound mental health becomes very germane. According to the World Health Organization (WHO), mental health is 'a state of well-being in which the individual realizes his or her own abilities, can cope with the normal stresses of life, can work productively and fruitfully, and is able to contribute to his/her community'. Health is said to be wealth and their relationship which remains direct has been well outlined in the article.

I therefore enjoin you to read carefully and share the knowledge with family, friends and all within your social circle.

Ugochi Osinigwe
Editor-in-Chief

Reader's Comments: Kindly send your comments to info@acaebin.org

Members of Research and Publication Committee

| | |
|----------------------------|---------------------------------|
| Ugochi Osinigwe | (Fidelity Bank), Chairperson |
| Prince Akamadu | (Union Bank of Nig. Plc) |
| 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) |
| Femi Jaiyeola | (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 |



Professional Ethics: The Moral Courage of Internal Auditor

1. INTRODUCTION

The nature of auditing establishes a unique position of trust with respect to customers, employers, employees, and the general public, who rely on the professional judgment and recommendations of auditors to make informed decisions. Due to the fact that accountants and auditors provide information about companies that enables the public to make investment decisions, there is a widespread impression that individuals in the accounting profession have a significant responsibility to the public. For the public to depend on the presented information, there must be confidence in the accountants' and/or auditors' knowledge and conduct. According to Jensen (2006), the auditing profession should serve a crucial role of societal trust by serving as a vehicle for holding managers accountable for their conduct. This process should ensure that the financial data provided by management is accurate and comprehensive.

However, the recent pace of corporate failures and accounting scandals has affected investor faith in the corporations' and capital markets' openness, honesty, and accountability. Auditing is a public service that verifies the statements of financial management and reassuring investors. Therefore, as professionals in

this industry, auditors have ethical responsibility to investors and are obligated to conduct audits with the utmost integrity, independence, and objectivity (Fahimeh & Mahdi, 2013).

Internal auditors are expected to conduct their duties with due care, accountability, and consistency. Karssing (2011). The goal of The Institute's Code of Ethics is to establish an ethical culture within the profession of internal auditing by outlining the rules and standards governing the behavior of individuals and organizations when conducting internal audits. Rather than particular tasks, it describes the baseline requirements for conduct and behavioral expectations.

Ethical behavior involves adherence to unwritten norms and a culture of "doing the right thing." A range of elements, including industry and business rules, social and economic constraints, laws and regulations, and prevalent attitudes and beliefs, influence an individual's view of ethical action. These factors shape a set of written and unwritten ethical rules that are utilized when confronted with an ethical dilemma. For the accounting profession to gain public trust, ethical conduct is important.

Given the call for increased ethical behavior among

accountants and auditors, the purpose of this article is to examine the ethical issues that challenge the auditing profession. Specifically, the paper will discuss various professional ethics and types, ethical expectations for auditors, ethical dilemmas, threats, evaluating ethical choices, safeguards and steps to avoid ethical threats in the auditing engagement, as well as offer solutions for addressing ethical issues. This is studied within the context of the role that ethical sensitivity plays in bringing about the auditor's proper ethical conduct in the process of performing its duties. In other words, we will examine the impact of professional codes of conduct and ethical concerns on the work of the internal auditor, as mandated by various accounting authorities.

2. REVIEW OF RELATED LITERATURE

Concept of Professional Ethics

The Australian Council of Professions (2003) defines a Profession as a disciplined group of individuals who adhere to ethical standards and who hold themselves out as, and are accepted by the public as possessing special knowledge and skills in a widely recognized body of learning derived from research, education, and training at a high level, and who are willing to apply this knowledge and exercise these skills for the benefit of others. This demonstrates that a profession is a commitment to a specified and organized occupation based on authority over a body of information and the acquisition of specialized training.

A professional is a practitioner who belongs to a certain profession and is able to make judgments, apply their abilities, and reach educated conclusions in situations where the general public cannot because they lack the necessary knowledge. Professionals are controlled by codes of ethics and profess dedication to competence, honesty and morality, altruism, and the advancement of the public good within their respective fields of expertise. Professionals owe a duty to their clients and to the society Evetts (2011).

Professionalism is defined as the views a Professional hold about his or her own behaviour as a member of a Profession. It is frequently associated with the observance of the principles, laws, ethics, and norms of a Profession in the form of a code of conduct. Professionalization is both the pattern of a profession's evolution and the act of becoming a profession (Abbott, 1988). A set of moral principles or beliefs constitutes ethics. A system or code of behavior is based on moral duties and obligations that outlines how an individual should conduct themselves in society. Professional ethics are the standards of

personal and business conduct, values, and guiding principles that are required of professionals.

Moral Courage

Moral courage bridges the chasm between making a decision among alternatives and also acting on decisions previously made. Courage, according to the Greek philosopher Aristotle, is the Golden Mean between cowardice and recklessness, the exact location of which varies based on the circumstances. To discover the golden medium requires guts in every aspect of life (Ehiriudu, Ugwuozor, Igweonyia & Ani, 2021). According to Sanchez and Cabello (2013), courage is prosocial behavior such as speaking and acting on one's findings and beliefs. In addition, they emphasized that moral courage is moral competency that tends to overcome the fear of doing the right thing among auditing professionals.

Auditors, both internal and external, must understand how to exercise moral bravery. To auditing professionals, moral courage entailed balancing logical ethical principles against unthinking selfish benefits and routinely breaching ethical standards by surrendering to or acting on self-serving temptation (Kolodinsky 2012). This meant that an auditor should not bow to situational pressure when dealing or fulfilling their professional tasks, but rather be decorated with high moral intensity and the bravery to stick to the ethics of the profession.

Marylin Douglas (2014) emphasized that courage is a multidimensional term with health, physical, and moral elements. Moral courage stands out the most among all the dimensions. Moral courage was described by Lopez (2003) as the ability to transform moral intentions into acts despite demands from the organization to do otherwise. When challenged with adverse repercussions and social criticism or enchantments, moral bravery enables auditors, groups, corporations, and organizations to stand up for their views and ideals for the greater good.

When confronted with temptations and professional challenges in the job, moral bravery is the auditor's capacity to remain steadfast and unyielding. The auditor employs moral fortitude and ethical principles to escape the issue presented in the profession. Moral courage and moral imagination develop empathy, which has an effect on auditors. Moral courage entails doing the right things and insisting on facing the blames and rebukes that may result from doing the right thing in accordance with ethical standards (Lopez 2003). They argued that moral courage transforms moral thoughts into deeds without regard for pressure, retaliation, or the

condemnation of like-minded individuals who profit from illegalities and infractions.

Significances of Moral Courage

The importance of moral courage in the auditing profession is as follows: First, moral bravery enables internal auditors to advocate fearlessly for their rights in the workplace. Hannah (2011) theorized that moral bravery enables auditors to act meaningfully on their intentions by reviewing and analyzing every topic seriously and correctly in a morally courageous manner prior to rendering a sound verdict on it.



Second, moral courage enables auditors to go the extra mile to instill sound morals in the course of doing their professional obligations, regardless of whose ox gets gored. This practice carefully adheres to professional norms of behavior. Thirdly, moral courage as a competence equips auditors to engage in activities that do not compromise the integrity of the auditing profession.

Moral Compass

Undoubtedly, life can be tough, and navigating the tricky waters of interpersonal relationships and sophisticated decision-making may be challenging. Every day, we make "good" or "poor" decisions that determine our conduct. When shopping at the store, it would be simple to conceal a bottle of expensive spices to save N500; yet most individuals prefer not to do so; why? What prevents us from flirting or texting someone new if we are in a committed relationship? What about deceiving our spouses, subordinates, and children? When our emotions, whether rage, envy, or love, overpower us, what prevents us from engaging in

violent or spiteful behavior? The answers to these questions constitute our "moral compass" in a broad sense. Gino (2016) described a moral compass as the aggregate word for an individual's views, goals, and judgments around what is right and wrong. A moral compass consists of the internal principles that drive ethical behavior and decision-making, similar to a navigational compass. Gino (2016) stated that the vague character of morality, which can change and evolve over time and depending on subjective experience, makes it difficult to argue for a universal moral compass or moral absolutes.

Moral Burden of the Internal Auditor

Ideally, auditors conduct their duties with due care, accountability, and consistency. Internal auditors face moral difficulties including competing ideals, codes of conduct, and interests, as do all other professionals. According to well-known key phrases: Should auditors examine, learn, or instruct? Should they frustrate or offer suggestions? Control or report? How forcefully should they convey their opinion when a solution is imminent? How critical should they be of their team of directors' policies and their colleagues' work? These general inquiries encompass a greater number of concrete challenges and conundrums with which internal auditors frequently contend. Wirtz and Karssing (2015).

3. IMPLICATION OF ETHICAL DILEMMAS IN PROFESSIONAL AUDIT PRACTICE

An ethical dilemma is a complicated scenario that frequently contains an apparent mental conflict between moral imperatives, wherein adhering to one

would necessitate violating another. It is a circumstance in which a person must choose an appropriate course of action. In moral philosophy, ethical dilemmas are frequently invoked in an effort to refute an ethical system or moral code, or to enhance it in order to resolve the paradox. In the exercise of professional judgment, auditors are regularly confronted with complicated, unforeseen moral challenges that cannot be resolved through the application of a code of conduct (Gaa, 1992). The auditors' professional conduct has been crucial in boosting the confidence of financial statement users and confirming the financial statements' integrity (Karajeh, 2004). Accounting was originally regarded by the public as having the highest level of integrity among other occupations (Pearson, 1988). However, after a series of high-profile scandals, this profession's reputation has declined (Herron and Gilbertson, 2004).

Internal Auditors have a fiduciary duty to the audit client and the employer. In such a connection, they are responsible for ensuring that their obligations are carried out in accordance with the ethical standards of honesty, integrity, objectivity, reasonable care, confidentiality and putting the public interest ahead of their own. The accounting and auditing profession is confronted with a range of types and degrees of ethical difficulties. The following are examples of the most prevalent ethical challenges in the corporate environment: Dealing with pressure to act unethically, especially from dominant superiors; Striking a balance between confidentiality and blowing the whistle on illegal or improper actions of others; Disclosing information in the public interest; and Wrongful trading in a distressed situation where insolvency is possible.

According to Okezie (2016), ethical dilemmas encompass a variety of ethical issues, including overstating performance and valuation, engaging in fraudulent activity, non-disclosure and withholding of information from auditors and other stakeholders, and making a decision without sufficient information. Other prevalent dangers to the accounting/auditing profession include:

- i. Familiarity Threat - auditor becoming unduly sympathetic towards its client as a result of long association.
- ii. Intimidation- auditor comes under intimidation by dominant individual or aggressive atmosphere at the clients.
- iii. Self Interest Threat – when personal interest of the auditor conflicts with that of the client

- iv. Advocacy Threat - where the auditor finds himself in a position he has to defend or promote the interest of its client before a third party.
- v. Self-review Threat - when the auditor has to audit the work that he helps to carry out.
- vi. Opinion Shopping - pressure on auditors to accept questionable accounting treatment.

4. CONCLUSION AND RECOMMENDATION



Auditors can be satisfied when they exemplified the culture of moral courage by embracing ethical behaviour that encourages morally courageous action in their workplace. Sekerka (2009) agreed that moral courage is an attribute that enhances good morals, sound judgements, justices, integrity, boldness in the face of difficulties. Ethical behaviour, moral virtues, and professional competency help moral courage to strive. White (1998) admonishes that durable moral courage should be seen among auditors, which is the capacity to insist on demonstrating genuinely and committed morally courageous behaviour.

Internal Auditors may encounter difficulties like; rejections in their workplace, condemnation for resistance to succumb to internal and external pressure, retaliation, and reprisal attacks by their colleagues, within and outside the organisation. Not minding the circumstances that surround the auditing profession, internal auditors should look at the ethics of the profession as a moral compass directing their activities in the profession. Auditors should insist on the moral value, ethical standards, and professional codes of conducts that boosts moral courage in them, which help them to carry out their work without fear or favour. Finally, moral courage among auditing professionals should be strengthened in all ramifications because it is a virtue and not vice and it is needed among the auditors.

Emuebie Emeke,
Internal Audit Department, Union Bank Plc



Cloud Computing in the 21st Century

Introduction

Cloud computing services are application and infrastructure resources that users access via the Internet. These services, contractually provided by various companies such as Microsoft (Azure), Amazon (AWS), Apple, Google, etc, enable customers to leverage powerful computing resources that would otherwise be beyond their means to purchase and support. Cloud services provide services, platforms, and infrastructure to support a wide range of business activities. These services support, among other things, communication; collaboration; project management; scheduling; data analysis, processing, sharing, and storage. Cloud computing services are generally easy for people and organizations to use, they are accessible over the Internet through a variety of platforms (workstations, laptops, tablets, and smartphones), and they are usually able to accommodate spikes in demand much more readily and efficiently than in-house computing services.

Cloud Computing Deployment Models

There are four primary cloud computing deployment models.

- **External cloud:** External cloud is defined as an off-premises infrastructure made available over the Internet which combines the resources of a broad network of users into one or more shared servers (e.g., Microsoft Office

365, Dropbox, Apple iCloud, etc.). A cloud environment that can be accessible by authorized users.

- **Internal cloud:** A cloud environment that is managed or owned by an organization on dedicated and usually on-premises servers that can provide high-level control over cloud services and infrastructure. This can be an appropriate model for highly sensitive data.
- **Community model:** A cloud computing environment that is shared or managed by a specific community of users from organizations that have shared concerns. This normally involves several related organizations on dedicated and on-premises servers of their choice and location.
- **Hybrid cloud or virtual private cloud model:** This model, comprised of both private and public clouds, allows for certain components to be hosted by an external party while others remain within the organization's control.

Cloud Computing Services

The followings are the major Cloud Computing Services:

- **Software-as-a-Service (SaaS)** – Capability to

use the provider's applications running on cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., Dropbox, iLearn, and MS Office 365).

- **Platform-as-a-Service (PaaS)** – Capability to deploy onto the cloud infrastructure customer-created or acquired applications created using programming languages and tools supported by the provider (e.g., Amazon Cloud Service, Microsoft Azure).
- **Infrastructure-as-a-Service (IaaS)** – Capability to provision processing, storage, networks, and other fundamental computing resources, offering the customer the ability to deploy and run arbitrary software, which can include operating systems and applications. IaaS puts these IT operations into the hands of a third party (e.g., Amazon Cloud Service, Microsoft Azure).

Risk Associated with Cloud Computing

Despite its advantages, Organizations must be very cautious about self-provisioning a cloud service to process, share, store, or otherwise manage organizational data. Self-provisioned cloud services may present significant data management risks or are subject to changes in risk with or without notice. Virtually all cloud services require individual users to accept click-through agreements. These agreements do not always allow users to negotiate or clarify terms and conditions, often provide vague descriptions of services and safeguards, and often change without notice.

Some of the risks associated with using cloud services include:

- Unclear, and potentially poor access control or general security provisions.
- Sudden loss of service without notification.
- Sudden loss of data without notification
- Data stored, processed, or shared on cloud service is often mined for resale to third parties that may compromise people's privacy
- The exclusive intellectual rights to the data stored, processed, or shared on cloud service may become compromised.

Best Practices for Storing Organization's Data in

the Cloud

- Data belonging to organizations should only be stored with cloud services after relevant approvals have been obtained (Top Management, ISMS Manager, etc.)
- Appropriate risk assessment should be carried out regarding the proposed or continued use of cloud services.
- Due diligence must be conducted prior to sign-up to a cloud service provider to ensure that appropriate controls will be in place to protect data. Preference should be given to suppliers who are certified to the ISO/IEC 27001:2013 international standard.
- Service level agreements and contracts with cloud service providers must be reviewed, understood, and accepted before sign-up to the service.
- The location of the data must be understood e.g., UK, EU, USA, and the applicable legal basis established, such as the country whose law applies to the contract.
- Where available, two-factor authentication must be used to access all cloud services.
- Sufficient audit logging should be available to allow the organization to understand how its data is being accessed and to identify whether any unauthorized access has occurred.
- Confidential data stored in cloud services must be encrypted at rest and in transit using acceptable technologies and techniques. Where possible encryption keys should be held by the organization rather than the supplier.
- Backups must be taken of all data stored in the cloud. This may be performed either directly by the organization or under contract by the cloud service provider.
- All data must be removed from cloud services in the event of a contract coming to an end for whatever reason. Data must not be stored in the cloud for longer than is necessary to deliver business processes.

Jennifer Nwofor
ProvidusBank Limited



The various Dynamics of Social Engineering Attacks on Nigerian Banks' Customers and the Recommended Practical Solutions

1. **Meaning and understanding of Social Engineering.** tend to lure unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems.
2. **Forms of social Engineering.** Social engineering attacks tend to manipulate targets with the aimed of getting confidential or personal information that can be used for fraudulent or malicious purposes.
3. **Explanation of the various forms of social Engineering.** Social engineering is **the term used for a broad range of malicious activities accomplished through human interactions.** It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.
4. **Financial loss Attributable to the various forms of social Engineering Attacks.** Social engineers use a variety of means both online and offline to con unsuspecting users into compromising their security, transferring money or giving away sensitive information.
5. **Common Indicators of Social Engineering Attacks.** Commonly, social engineering involves email or other communication that invokes urgency, fear, or similar emotions in the victim, leading the victim to promptly reveal sensitive information, click a malicious link, or open a malicious file. Because social engineering involves a human element, preventing these attacks can be tricky for banks.
6. **Recommended practical solution.**
7. **What to do If you are Already a Victim of Social Engineering Attack.**

MEANING AND UNDERSTANDING OF SOCIAL ENGINEERING

Social Engineering is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. It is a manipulation technique that exploits human error to gain private information, access, or valuables which involves "human hacking" scams that

Social engineering is a popular tactic among attackers because **it is often easier to exploit people than it is to find a network or software vulnerability.** Hackers will often use social engineering tactics as a first step in a larger campaign to infiltrate a system or network and steal sensitive data.

FORMS OF SOCIAL ENGINEERING

The **six common types** of social engineering attacks include these:

- ▶ Phishing...
- ▶ Vishing and Smishing...
- ▶ Pretexting...
- ▶ Baiting...
- ▶ Tailgating and Piggybacking...
- ▶ Quid Pro Quo...
- ▶ Cyber Threats Beyond Social Engineering.

1. Phishing

Phishing is a social engineering technique in which an attacker sends fraudulent emails, claiming to be from a reputable and trusted source. For example, a social engineer might send an email that appears to come from a customer account manager at your bank. They could claim to have important information about your account but require you to reply with your full name, birth date, social security number and account number first so that they can verify your identity. Ultimately, the person emailing is not a bank employee; it's a person trying to steal private data.

Phishing is used to describe fraudulent email practices; similar manipulative techniques are practiced using other communication methods such as phone calls and text messages.

Phishing, in general, casts a wide net and tries to target as many individuals as possible. However, there are few types of phishing that hone in on particular targets.

- **Spear phishing** is a type of targeted email phishing. In a spear phishing attack, the social engineer will have done their research and set their sites on a particular user. By scouring through the target's public social media profiles and using Google to find information about them, the attacker can create a compelling, targeted attack. Imagine that an individual regularly posts on social media that she is a member of a particular gym. In that case, the attacker

could create a spear phishing email that appears to come from her local bank. The victim is more likely to fall for the scam since she recognized her Bank as the supposed sender.

- **Whaling** is another targeted phishing scam. However, in whaling, rather than targeting an average user, social engineers focus on targeting higher-value targets like CEOs and CFOs. Whaling gets its name due to the targeting of the so-called "big fish" within a company.

2. Vishing and Smishing

Vishing (short for voice phishing) occurs when a fraudster attempts to trick a victim into disclosing sensitive information or giving them access to the victim's computer over the telephone. One popular vishing scheme involves the attacker calling victims and pretending to be from the customer's bank. The caller often threatens or tries to scare the victim into giving them personal information or compensation. Vishing scams like the one often target older individuals, but anyone can fall for a vishing scam if they are not adequately trained as it is very common now in Nigeria.

Smishing (short for SMS phishing) is similar to and incorporates the same techniques as email phishing and vishing, but it is done through SMS/text messaging.

3. Pretexting

Pretexting is a type of social engineering technique where the attacker creates a scenario where the victim feels compelled to comply under false pretenses. Typically, the attacker will impersonate someone in a powerful position to persuade the victim to follow their orders. During this type of social engineering attack, the scammer impersonates Bank officers, higher-ups within the Bank, auditors, investigators or any other personnel they believe will help them get the information they seek.

4. Baiting

Baiting puts something enticing or curious in front of the victim to lure them into the social engineering trap. A baiting scheme could offer a free music download or gift card in an attempt to trick the user into providing credentials.

A social engineer may hand out free USB drives to users at a conference. The user may believe they are just getting a free storage device, but the attacker could have loaded it with remote access malware which infects the computer when plugged in.

5. Tailgating and Piggybacking

Tailgating is a simplistic social engineering attack used to gain physical access to an unauthorized location. Tailgating is achieved by closely following an authorized user into the area without being noticed by the authorized user. An attacker may tailgate another individual by quickly sticking their foot or another object into the door right before the door is completely shut and locked.

Piggybacking is exceptionally similar to tailgating. The main difference between the two is that, in a piggybacking scenario, the authorized user is aware and allows the other individual to "piggyback" off their credentials. An authorized user may feel compelled by kindness to hold a secure door open for a woman holding what appears to be heavy boxes or for a person claiming to be a new employee who has forgotten his access badge.

6. Quid Pro Quo

Quid pro quo (Latin for 'something for something') is a type of social engineering tactic in which the attacker attempts a trade of service for information. A quid pro quo scenario could involve an attacker calling the main lines of banks pretending to be from the IT department, attempting to reach someone who was having a technical issue. Once the attacker finds a user who requires technical assistance, they would say something along the lines of, "I can fix that for you. I'll just need your login credentials to continue." This is a simple and unsophisticated way of obtaining a user's credentials.

Financial Loss Attributable to the Various Forms of Social Engineering Attacks

According to PUNCH News Paper Publication June 01, 2022.

The number of password-stealing malware attacks in Nigerian Banks in the first four months of 2022 rose by **146.56** percentage.

In 2022, the number of Trojan-PSW (Password Stealing Ware) detections in Nigeria more than doubled when compared to the same period in 2021 – 2,654 detections in 2022 compared to 1,076 in 2021.

"Trojan-PSW is a malware that steals passwords, along with other account information, which then allows attackers to gain access to the corporate. Another popular attack tool used on banks and small businesses is Internet attacks, specifically, web pages with redirects to exploits, sites containing exploits and other malicious programs, botnet C&C centres network and steal sensitive information.

The emergence of digital banking has come with terms such as passwords and Personal Identification

Numbers.

Passwords and PINs remain the bedrock of digital or electronic banking.

The four-digit PIN for your debit card on online shopping sites, passwords on Internet banking platforms and other sites, and your debit card data are key to your life and financial resources.

The Automated Teller Machines and Internet banking platforms are under siege more than ever before from skimming. Skimming, where ATM thieves steal your PIN and account number using remote devices, is increasing dramatically. Often done by sophisticated crime rings, ATM skimming is becoming a high-tech art that's hard to detect.

Cyber criminals stole N5.20bn from Nigerian banks' customers in 9 months

On the back of rising electronic transactions, bank customers recorded a loss of N5.02 billion between January and September 2021 in 41,979 fraud-related incidences representing 91 percent success out of the total 46,126 fraud attempts.

This is according to data at the Nigeria Inter-Bank Settlement System (NIBSS) shown in its latest report titled Fraud in the Nigerian Financial Service

A breakdown of how the frauds were perpetrated in 2021, shows majority of the frauds was done via the web representing 47 percent, Mobile transaction 36 percent, Automatic Teller Machine 9 percent while internet banking 1 percent.

On year on year growth, Mobile channel rose by 330 percent, while Web and Point of Sales channels fraud activities increased by 173 percent and 215 percent respectively from 2019 to 2021.

On the technique applied to defraud bank customers in 2021, NIBSS revealed that Social engineering remains one of the principal ways in which fraudulent activities are attempted.

NIBBS disclosed that 56 percent of fraud techniques were Social engineering, followed by phone theft, card theft and fake assistant representing 6 percent.

PIN compromise was 3 percent of the total fraud activities, Robbery 2 percent, Lack of 2FA 1.9 percent, missing lost card 1 percent, card phone theft 1 percent.

Information technology experts have attributed 70 per cent of cybercrimes in the country to social engineering and, therefore, urged Nigerians to be cybersmart by not divulging confidential information.

Safeguarding your identity in digital banking is tantamount to protecting your money or wealth. Protecting your identity on Internet banking platforms and the world of digital banking in general is a must.

Common Indicators of Social Engineering Attacks

- **Suspicious sender's address.** The sender's address may imitate a legitimate business. Cybercriminals often use an email address that closely resembles one from a reputable company by altering or omitting a few characters.
- **Generic greetings and signature.** Both a generic greeting—such as "Dear Valued Customer" or "Sir/Ma'am"—and a lack of contact information in the signature block are strong indicators of a phishing email. A trusted organization will normally address you by name and provide their contact information.
- **Spoofed hyperlinks and websites.** If you hover your cursor over any links in the body of the email, and the links do not match the text that appears when hovering over them, the link may be spoofed. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net). Additionally, cybercriminals may use a URL shortening service to hide the true destination of the link.
- **Spelling and layout.** Poor grammar and sentence structure, misspellings, and inconsistent formatting are other indicators of a possible phishing attempt. Reputable institutions have dedicated personnel that produce, verify, and proofread customer correspondence.
- **Suspicious attachments.** An unsolicited email requesting a user download and open an attachment is a common delivery mechanism for malware. A cybercriminal may use a false sense of urgency or importance to help persuade a user to download or open an attachment without examining it first.

TEN PRACTICAL WAYS TO PREVENT SOCIAL ENGINEERING ATTACKS

1. Multi-Factor Authentication
2. Continuously Monitor Critical System
3. Utilize Next-Gen cloud-based WAF
4. Verify Email Senders Identity

5. Identify your critical assets which attract criminals
6. Check for SSL Certificate
7. Penetration Testing
8. Check and Update your Security Patches
9. Enable Spam Filter
10. Pay Attention to Your Digital Footprint

1. **Multi-Factor Authentication**

- Don't rely on one factor – the most basic preventive measure guarantees your account security. Of course, the password ensures security, but we have realized they're inadequate on its own. Because it is far easier for someone else to guess your password and obtain access to your accounts.

- The passwords can be accessed through social engineering. Multi-Factor verification is required that could be anything from biometric access, security questions to an OTP code.

2. **Continuously Monitor Critical System**

- Make sure your system, which houses sensitive information is being monitored 24x7. When certain exploiting tactics are employed like Trojans, they sometimes depend on the system, which is vulnerable. Scanning both external and internal systems with Web application scanning can help to find vulnerabilities in your system.

- Besides, you should also perform a social engineering engagement at least once a year to assess whether your employees would fall victim to the dangers of social engineering. Once tracked, fake domains, if any, can be taken down instantly to avoid copyright infringement online.

3. **Utilize Next-Gen cloud-based WAF**

- You're probably already employing a firewall within your business, but a next-generation web application cloud-based firewall is specially designed to ensure maximum protection against social engineering attacks. The web WAF is very different from the traditional WAF that most companies deploy.

- To be specific, AppTrana can consistently

monitor a web application or website for anomalous activity and misbehaviour. Although social engineering threats depend on human mistakes, it will block attacks and alerts you to any endeavored malware installations. Implementing risk-based WAF is one of the best ways to prevent social engineering attacks and any potential infiltration.

4. **Verify Email Sender's Identity**

- Most scams involve the method of falsely obtaining victim's information by pretending as a trusted entity. Especially in a phishing attack, attackers send email messages that may appear like they are from a sender you trust like from a credit card company, a bank, a social networking site, or an online store. The emails often tell a story to make you click onto the false link, which looks legitimate.
- To avoid this kind of social engineering threats, contact the claimed sender of the email message and confirm whether he sent the email or not. Remember, legitimate banks will not ask your authorized credentials or confidential information through email.

5. **Identify your critical assets which attract criminals**

- *"When a lot of companies focus on protecting their assets, they're very focused on that from the perspective of their business"* – Jim O'Gorman, a member of Social-Engineer.org
- That is not necessarily the approach hacker will target your company. They always target the assets valuable to them.
- You should evaluate in the attacker's perspective and identify what to protect, considering the assets beyond your product, service, or intellectual property.
- *"Independent Assessment is the best tool to determine which of your assets criminals are most likely to target."* – according to O'Gorman.

6. **Check for SSL Certificate**

- Encrypting data, emails, and communication ensure that even if hackers intercept your communication, they can't be able to access the information contained within. This can be achieved by obtaining SSL certificates from trusted authorities.
- Furthermore, always verify the site, which asks for your sensitive information. To verify

the website's authenticity, check the URLs. The URLs which start with **https://** can be considered as trusted and encrypted website. The websites with **http://** are not offering a secure connection.

7. **Penetration Testing**

- The most effective approach among the ways to prevent social engineering attacks is conducting a pen-test to detect and try to exploit vulnerabilities in your organization. If your pen-tester succeeds in endangering your critical system, you can identify which system or employees you need to concentrate on protecting as well as the types of social engineering attacks you may be prone to.
- Learn more about how application Pen testing can mitigate Fraud.

8. **Check and Update your Security Patches**

- Cybercriminals are generally looking for weaknesses in your application, software, or systems to attain unauthorized access to your data. As a preventive measure, always maintain your security patches up to date and keep your web browsers & systems up to date with the latest versions.
- This is because companies release security patches as a response whenever they uncover security loopholes. Maintaining your systems with the recent release will not only reduce the possibilities of cyber-attacks but will also ensure a cyber-resilient environment.

9. **Enable Spam Filter**

- Enable Spam filters and close the door for offenders of social engineering security threats. Spam filters offer vital services in protecting your inboxes from social engineering attacks.
- Most email service providers offer spam filters that hold the emails which are deemed as suspicious. With spam features, you can categorize emails effortlessly, and freed from the horrible tasks of identifying mistrustful emails.

10. **Pay Attention to Your Digital Footprint**

- Oversharing of personal details online through social media can give these criminals more information to work with. For instance, if you keep your resume online, you should consider censoring your date of birth, phone number, and residential address. All that

information is useful for attackers who are planning a social engineering threat.

- Maintain your social media settings to "friends only" and think twice before you share anything on social media.

Other Daily Preventive Measures of Social Engineering Attacks

Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claim to be from a Bank or legitimate organization, try to verify his or her identity directly with the company.

- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Don't send sensitive information over the internet before checking a website's security. (See Protecting Your Privacy for more information.)
 - ⦿ Pay attention to the Uniform Resource Locator (URL) of a website. Look for URLs that begin with "https"—an indication that sites are secure—rather than "http."
 - ⦿ Look for a closed padlock icon—a sign your information will be encrypted.
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group. (See the APWG eCrime Research Papers).
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic. (See Understanding Firewalls for Home and Small Office Use, Protecting Against Malicious Code, and Reducing Spam for more information.)
- Take advantage of any anti-phishing features offered by your email client and web browser.

- Enforce multi-factor authentication (MFA). (See Supplementing Passwords for more information.)
- Increase the sensitivity of your spam filters.
- Never reuse a password across many accounts.
- Authenticate via two-factor or multi-factor methods.
- If you're unsure, reset your passwords straight away.
- Employees should be educated.
- Have zero trust for anybody you don't personally know, if they are using name drops, authorization "say so", or "time sensitive" things verify with their source. ie call your boss etc to verify any requests for access.

What to do if you are already a victim of Social Engineering attack.

- If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity.
- If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.
- Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future.
- Watch for other signs of identity theft.
- Consider reporting the attack to the FraudhelpDesk officers of various banks or other law enforcement agents if necessary.

**Onwuemele Sunday Emeke CFE
Forensic Investigation Team
United Bank For Africa (UBA) PLC**



The Changing Face of Internal Audit

Introduction

The year 2020 saw the globe plunge into an unprecedented health crisis, the likes of which could not have been anticipated by global institutions, world governments, health / environment / security agencies or any scientific or technology based entities. Today, in 2022, the impact of the changes the world at large has experienced in every sector and on every continent are still being dealt with by governments, businesses, and individuals.

Almost in one fell swoop, things that erstwhile were deemed impossible, difficult, or challenging became the order of the day. With lock-downs instituted from one country to the other where people could not go about their daily lives, let alone carry out their regular business – the lock-downs bringing about stay at home orders; permissions for only key business to operate; protection measures; international travel bans – and the impact of these on personal relations and business operations, led people to find alternative ways to keep their lives and businesses going.

1. Digitization in the Banking Industry and the New Players

This new normal we are in today shows a continuous

integration of digitization in our daily lives and by extension in our business operations. As financial institutions, the emergence of Financial Technology (FINTECH) companies is not a new topic; we now have banks either acquiring FINTECHs, FINTECHs acquiring banking licenses and banks creating FINTECH arms. We have now moved forward to telecoms entities providing banking services to their customers – MTN and Airtel have been granted payment service Bank (PSB) licenses by the Central Bank of Nigeria (CBN), where deposit takings, cross border payments, e-wallet operations, and debit/pre-paid cards can be offered to customers. MTN's MoMo Payment Service Bank (MoMo PSB) Limited, formally commenced operations on the 19th of May 2022 with an agent network of over 166,000 active agents.

The foregoing meant growth in customer base, transactions, revenue, regulations and by default, growth in risks, controls, and compliance concerns. The new normal demands evaluation of the opportunities presented by the changed or hybrid operations in each specific organization using methods that matches the development. This implies that relying on or requiring physical proximity to, manual handling or operation of and/or central or fixed locations or base for deliberation, review,

assessment or reporting on activities need to change as the digital space, where most of the new transactions will take place, is not limited to physical or singular unique location(s).

2. Auditing in a Digital Era

The tools, knowledge and skills of internal auditors must evolve with the evolving times. The tools used to carry out audits; the knowledge – terms, terminologies, applications, options, uses – of digital platforms, outlets, services; and the skills – comfort with basic computer applications and IT (Information Technology) audit software, development of IS (Information Systems) audit skills, (re)learning – must rise to meet the changes in the industry.

The volume and breadth of transactions, reports, customer service requests, incident reports, regulatory filing and the checks that will need to be done on these items cannot be done effectively with the usual tools and cannot be done effectively using the usual processes.

Throughout the history of auditing, audit tools have had to be more advanced or at least at par with the tools used by process owners. As of today, there is no audit team that does not use a computer system and one or more software applications to carry out their audits. From the use of various Spreadsheet software applications to the Computer Assisted Audit Techniques (CAATs) i.e. specifically designed auditing software; our current audit teams leverage existing technologies in executing their roles.

Our current audit teams generally are divided – in one way or another – between business process auditors and Information Technology/Information System Auditors and perhaps Investigation or Forensic teams. While IT/IS auditors specialize in the audit of information technology or information systems, the future demands that business process auditors, who are now dealing with more advanced and more technical business processes, require more advanced and more technical IT and IS audit skills to bring increased value to their audit execution and in proffering recommendations.

We know from experience that the computer knowledge, expertise and experience of our audit teams has direct impact on their ability to optimize the use of the technologies available to them. Likewise, our auditors' knowledge, expertise, and experience of

existing and advancing technologies will have a direct impact on their ability to review and advise management on risks and controls related to technologies adopted by the organization.

3. Conclusion

The various audit teams must invest in audit tools capable of providing a agile approach to audit in the light of high volume of transactions in the digital age. A new breed of internal auditors will be needed to move organizations forward in the digital world. Business must recognize and support this as our auditors are a vital part of our workforce trainings, sessions, seminars, knowledge sharing, meetings and all other avenues where new technologies are discussed should have audit team members in attendance and continually learning to stay ahead of or at least in sync with the changes.

The journey has already begun, the digital role of audit in each organization must be defined, the



mindsets and aspirations of internal auditors must be assessed and any roadblocks to the achievement of digital auditors must be identified and addressed by each organization.

For this, regular upskilling, trainings, attendance at seminars and knowledge sharing sessions, continuous engagements with groups such as the Association of Chief Audit Executives of Banks in Nigeria (ACAEBIN), security agencies and continuous interactions with regulators, would serve to keep auditors abreast of new technologies, audit approaches and guidelines and regulations affecting new and emerging technologies.

Ugoada Chikelu
Head, Internal Audit
Nova Merchant Bank Ltd

Being the opening remark by His Excellency, Mr. Udom Emmanuel, Governor, Akwa Ibom State on the occasion of the Annual General Meeting/Retreat of the Association of Chief Audit Executives of Banks in Nigeria (ACAEBIN) held at the Ibom Icon Hotel & Golf Resort, Uyo on March 31, 2022.

Protocol

On behalf of the Government and the people of Akwa Ibom State, I welcome members and other associated delegates of the Association of Chief Audit Executives of Banks in Nigeria (ACAEBIN) to our beautiful and peaceful State.

Permit me to thank you and other organizations, institutions, corporate entities in making our capital city of Uyo the preferred destination for conferences, retreats and meetings. You may have probably been told that Akwa Ibom State today is known as "Nigeria's Best Kept Secret."

As a Financial Services professional, I am acutely aware of the critical roles you play in the Financial Services Industry: ensuring full compliance with ethical standard, keeping the books right and building a culture of transparency. You are, to put it bluntly, the financial services ombudsman.

As the world evolves new approaches to getting things done, especially now that the Covid-19 pandemic has brought disruptions to our private and public operations, there is the urgent need to expose professionals in the financial services industry to new vistas of job deliverables, such as this Retreat holding here today. Today's Retreat is therefore a good move in the right direction.

Transparency which as a key aspect what you do has been the abiding article of faith or the defining pillar of our governance. We came to serve the people diligently and to achieve that, we have utilized the lean resources available to do the most for our people. We maintain zero-tolerance for wastages. Our Financial records are in the public domain, our budgets and how such were or are executed, are also matters of public knowledge.

The result of this key approach is the reason why we have achieved so much even in this season of economic adversity. I am sure most of you came into



our state with Ibom Air. We are the first subnational ever, to own a commercial airline.

You may have seen on your way to the city Centre that Akwa Ibom State is a construction hub, with world class road infrastructure on-going; you may also have seen the International terminal at the Victor Attah International Airport, which upon completion soon, would be the smartest of such terminals in the nation. We have established over 20 employment and wealth generating industries in the state. We came to serve, and as one of you, a Financial Services expert in public space, I hope I can be your worthy ambassador when I leave office.

I am pleased to welcome you one more time to the state and to Uyo, our beautiful state capital. I wish you a rewarding stay.

It is a great honour and privileged to now declare this meeting and Retreat open as I wish you successful and rewarding deliberations.

God bless us all!

ACAEBIN's visit to the Deputy Governor of Akwa Ibom State, Mr Moses Frank Ekpo who represented the Governor, Mr Udom Emmanuel ahead of the Retreat.



Yinka Tiamiyu presenting a copy of the Eagle Eye Magazine to the Deputy Governor, Mr. Moses Frank Ekpo.

The Deputy Governor familiarizes with the visitors.



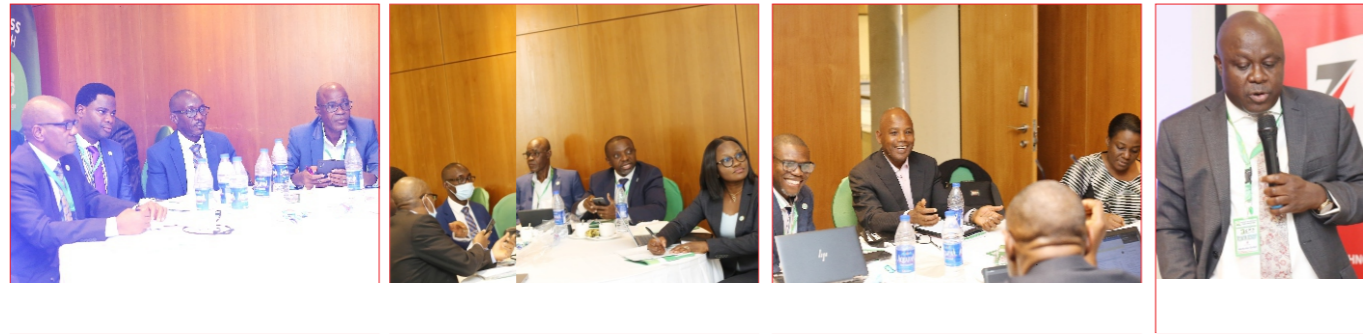
Day One of the 2022 Annual Retreat/Conference and General Meeting of Members on March 31st 2022 at the Ibom Hotel and Golf Resort, Uyo, Akwa Ibom State.



Day One event of the 2022 Annual Retreat/Conference and General Meeting of Members on March 31st 2022 at the Ibom Hotel and Golf Resort, Uyo, Akwa Ibom State continued.



Strategy session and Gala Night at the day two event of the 2022 Annual Retreat/Conference and General Meeting of Members on April 1st 2022 at the Ibom Hotel and Golf Resort, Uyo, Akwa Ibom State.



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

Continues from last edition

1 Reporting and Monitoring

A written report will be prepared by the internal audit department following the conclusion of each internal audit engagement and will be distributed as appropriate. A summary of the audit report will be communicated to the Audit Committee. The Audit Committee may also request for the full report if deemed necessary.

The internal audit report will include management's response and corrective action taken or to be taken regarding specific findings and recommendations. The internal audit department will be responsible or appropriate follow-up on engagement findings and recommendations. The internal audit department will retain control over the resolution of all significant findings until they are cleared.

The Chief Audit Executive (CAE) will periodically report to senior management and the Audit Committee on the internal audit activity's purpose, authority, and responsibility, as well as performance relative to its plan. Reporting will also include significant risk exposures and control issues including fraud risks, governance issues, and other matters needed or requested by the Audit Committee and

senior management.

2 Organisation

The CAE will report functionally to the Audit Committee and administratively (i.e. day to day operations) to the Managing Director.

As part of the functional reporting, CAE prepares and submits to the Audit Committee for review and approval:

- ➔ The internal audit charter
- ➔ The risk based internal audit plan
- ➔ The internal audit budget and resource
- ➔ Reports about internal activity's progress, findings, performance relative to its plan and other issues as required.

The CAE will communicate and interact directly with the Audit Committee including executive sessions and between the Audit Committee meetings, as appropriate. The Audit Committee will communicate with the CAE on the internal audit activity's

performance relative to its plan.

Administrative reporting is the oversight by the Managing Director and the relationship within the Organization's management structure that facilitates the day-to-day operations of the internal audit activity.



The Audit Committee will approve all decisions regarding the performance evaluation of the CAE

The CAE is responsible for development and issue of the internal audit activity's internal standards, manuals, and guidance papers. The Audit Committee will review and approve the internal standards, manuals, and guidance papers as part of its oversight role.

3 Independence

- The Internal Audit Department shall remain independent of all line and functional management; its personnel shall report to the CAE who shall report administratively to Managing Director and functionally to the

Audit Committee.

- Internal Audit Department shall be independent of the activities audited, to ensure impartiality and credibility of the audit work undertaken. The department must also be independent from the day to day internal control process;
 - Internal Audit department shall exercise its assignment on its own initiative in all departments, offices and functions of the company.
 - The internal audit function shall be free of any undue influences which could restrict, overrule or otherwise affect the judgments as to the content of a report or in any way require the Department to function under duress or which could affect the institution or conduct of an investigation;
 - CAE shall be authorized to communicate directly, and on his own initiative, to the Board and the members of the Audit Committee;
 - The internal audit function should be subject to an independent review as and when required. This review can be carried out by independent professionals e.g. practicing chartered accountants.

4 Quality Assurance and Improvement Programme

The Internal Audit Department will continue to evolve and develop in response to new challenges, changes and expectations, with the goals of:

- Achievement of a more comprehensive compliance with the *International Standards for the Professional Practice of Internal Auditing (Standards)*, the Institute of Internal Auditors' Practice Advisories, Practice Guides, and Position Papers;
- Revisiting methodology, processes and practices to deliver "real time" value to the company.
- Refining risk identification and assessment capabilities to enhance risk-based auditing to

align with the Organization's priorities and needs.

- Expanding audit coverage to include the full spectrum of major risks and activities.

The Internal Audit Department will develop detailed internal guidance and procedure manuals governing major areas of the internal audit activity. The Audit



Committee will review the guidance and manuals and approve as appropriate.

As part of the internal audit plan, the CAE will present to the Audit Committee a training and development programme for each professional within the Internal Audit Department with the goal of ensuring the skills of individual professionals are maintained and updated in accordance with the needs of the Organization and internationally recognized best practices for internal auditing. The programme will be supported with a proposed budget. The Audit Committee will review and approve the programme and the budget.

5 Professionalism

The internal audit activity will undertake, to maximum extent feasible for the Company, to govern itself by adherence to the Institute of Internal Auditors' mandatory guidance including the Definition of Internal Auditing, the Code of Ethics, and the International Standards for the Professional Practice of Internal Auditing (Standards). This mandatory guidance constitutes principles of the fundamental requirements for the professional practice of internal auditing and for evaluating the effectiveness of the

internal audit activity's performance.

The Institute of Internal Auditors' Practice Advisories, Practice Guides, and Position Papers will also be considered for adherence, as applicable, to guide operations.

In addition, the internal audit activity will adhere to the company's relevant policies and procedures and the internal audit activity's corporate internal audit standards, manuals and guidance.

6 Continuity and Impartiality

- Internal audit within Organizations shall be a permanent function.
- Internal Audit department shall be objective and impartial in performing its assignment.
- Objectivity and impartiality entail that the Internal Audit department itself seeks

to avoid any conflict of interest. To this end, staff assignments within the department shall be rotated periodically. Internally recruited auditors shall not audit activities or functions they performed in the past two years, and they will not be allowed to audit the work earlier performed by them.

- Impartiality requires that audit department is not involved in the operations of the company or in selecting or implementing internal control measures. However, audit department may give recommendations for strengthening internal controls and can also give opinions on specific matters relating to internal control procedures as per the request of senior management.

Rasaq A Ozemedo
CAE of NEXIM Bank



Service Level Agreement (SLA), the Audit Perspective

A Service Level Agreement (SLA) is a contract between a service provider and its customers that document what services the provider will furnish and defines the service standards the provider is obligated to meet. It is imperative that the SLAs contain the necessary information to use and manage the service delivery. The agreement varies between vendors, services, employers and industries. Also, reviewing SLA should be done in line with the organization's documented and approved Service Level Management Process and Procedure as well as Vendor Management Policy. International Organization for Standardization (ISO) Standards and The Central Bank of Nigeria (CBN) Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers. Organizations shall regularly monitor, review and audit supplier service delivery (Monitoring and review of supplier service **ISO/IEC 27001:2013 A15.2.1**).

As Information Technology (IT) outsourcing became emergent in the late 1980s, Service Level Agreements have been pivotal in regulating such relationships. Since then, SLAs have been critical in setting expectations of a service provider's performance and establishing sanctions for missing targets and incentives for exceeding them.

Later, SLAs evolved to accommodate new approaches by developing managed services and the cloud computing services era. Shared services replaced customized resources in planning new contracting methods. Thus, businesses used Service Level Commitments to generate broad agreements to encompass all service providers' customers.

Types of Agreements / Contracts

Service Level Agreement (SLA): This is agreement

signed between the Customer/Client and the Service Provider.

Operational Level Agreement (OLA): This is signed between Business Units/Divisions and Internal IT of the same Organization.

Underpinning Contracts (UC): This is signed between Service Provider and the Vendor.

For each external supplier, the organization shall agree a documented contract. The contract shall include or contain a reference to:

d) authorities and responsibilities of the organization and the external supplier.

The organization shall assess the alignment of service level targets or other contractual obligations for the external supplier against SLAs with customers and manage identified risks. At planned intervals, the organization shall monitor the performance of the external supplier. Where service level targets or other contractual obligations are not met, the organization shall ensure that opportunities for improvement are identified. At planned intervals, the organization shall



- scope of the services, service components, processes, or parts of processes to be provided or operated by the external supplier.
- requirements to be met by the external supplier.
- service level targets or other contractual obligations.

review the contract against current service requirements. Changes identified for the contract shall be assessed for the impact of the change on the Service Management Systems (SMS) and the services before the change is approved (**ISO/IEC 20000-1: 2018, Clause 8.3.4.1 Management of external suppliers**).

For each internal supplier or customer acting as a supplier, the organization shall develop, agree and maintain a documented agreement to define the

service level targets, other commitments, activities and interfaces between the parties. At planned intervals, the organization shall monitor the performance of the Internal Supplier or the customer acting as a supplier. Where service level targets or other agreed commitments are not met, the organization shall ensure that opportunities for improvement are identified (ISO/IEC 20000-1: 2018, Clause 8. 3.4.2 Management of internal suppliers and customers acting as a supplier).

In line with the Organization's Internal Policy and/or Procedure for Vendor Management, Prequalification of Vendors/Contractors/Suppliers are carried out and the records maintained for reference purposes. This is a process to identifying and pre-screening competing suppliers and contractors against a pre-determined set of criteria. This ensures the vendors have the baseline capacity and capability to provide goods and or services prior to being invited to bid for a particular project/request. This helps minimize the risk of contract failure as substandard or non-compliant vendors would already have been barred from entry.

Key Components of a Service Level Agreement (SLA)

When reviewing the Organization's Service Level Agreement (SLA), the following should be considered for quality, availability and responsibilities of the contract based on the peculiarity of the Service Level Agreement:

1. **Agreement Overview:** The agreement overview outlines the fundamentals of the agreement, such as the parties in agreement, the start date, and a general introduction of the services provided.
2. **Description of Services:** An SLA must have a comprehensive description of all the services offered, under which circumstances they perform, and the turnaround times.
3. **Exclusions:** A list of excluded services should also explain limitations and avoid confusion and assumptions from the other party.
4. **Service Performance:** Both the customers and the service provider must agree on SLA metrics which are set of key performance indicators (KPIs) for specific performance measurement, evaluation and continuous monitoring. At planned intervals, the organization shall monitor, review and report on performance against service level targets (ISO/IEC 20000-1: 2018, Clause 8. 3.3

Service Level Management)

5. **Redressing:** The compensation should also be defined, including the pay rate for service providers who cannot fulfil their obligations.
6. **Stakeholders:** An SLA must clearly define the parties involved and their respective responsibilities in the agreement.
7. **Security:** All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information (Addressing security within supplier agreements ISO/IEC 27001:2013 A15.1.2)
8. **Risk Management and Disaster Recovery:** Risk Management and Disaster Recovery Plans and Processes must also get laid out in the event of unforeseen circumstances. The Organization shall document and maintain business continuity plans and procedures. The business continuity plans shall provide guidance and information to assist teams to respond to a disruption and to assist the organization with response and recovery (ISO/IEC 22301:2019, Clause 8.4.4.1 Business Continuity Plans Clause)
9. **Service Tracking and Reporting:** The service tracking and reporting section encompasses the reporting structure, tracking intervals, and the stakeholders taking part in the agreement.
10. **Periodic Review and Change Processes:** You must routinely review the SLA and accepted Key Performance Indicators (KPIs) to prevent or rectify mistakes and make changes. Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures, and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks (managing changes to supplier services ISO/IEC 27001:2013 A15.2.2).
11. **Right to Audit:** Service Provider shall grant to the Customer/Bank access to perform an audit of all books, records, processes and procedure of Service Provider related to the performance of the services in this agreement

at any time. Service Provider shall maintain accurate records at all times. The Customer/Bank shall be permitted to conduct these audits with its internal resources/personnel or by securing the services of a third-party IT or auditing firm, solely at the Customer/Bank's election. The Customer/Bank shall have the right to (a) access any premises used by Service Provider to provide the Services or from where the services are managed or administered; (b) interview any Service Provider's Personnel; (c) copy, at its own expense, any record related to the services performed pursuant to this agreement (Section 3 - Vendor/Contractor/Third-Parties subsection 3.2 "Issuance of Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers" dated October 10, 2018).

12. **Confidentiality:** A confidentiality agreement (also called a nondisclosure agreement or NDA) is a legally binding contract in which a person or business promises to treat specific information as a trade secret and promises not to disclose the secret to others without proper authorization.

13. **Escrow agreement:** An escrow agreement is a contract that outlines the terms and conditions between parties involved and the responsibility of each. Escrow agreements generally involve an independent third party, called an escrow agent, who holds an asset of value until the specified conditions of the contract are met. This is specifically for software Developers of software developing companies to warehouse the source codes of the solution with an escrow agent should the Developer goes out of business or changes the line of business.

14. **Intellectual Property Right:** Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements related to intellectual property rights and use of proprietary software products (ISO/IEC 27001:2013 A18.1.2).

15. **Force Majeure:** Neither party will be liable for inadequate performance to the extent caused by a condition (for example, natural disaster, act of war or terrorism, riot, labour condition, governmental action, and Internet disturbance) that was beyond the party's reasonable control.
16. **Termination Process:** To avoid schedule conflicts, the SLA should also define the circumstances by which the agreement can be prematurely terminated or will expire. It is also essential to establish the notice period from each party.
17. **Signatures:** Ultimately, all stakeholders and authorized participants must make the agreement legal by signing the document. The Organization's internal Policy must specify



Top Management's responsibility for signing new and renewal of Service Level Agreements.

Conclusion

A Service Level Agreement (SLA) is important to ensure that all parties understand its documented contents to maintain and improve IT service quality through a constant cycle of agreeing, monitoring and reporting upon IT service achievements and instigation of actions to eradicate poor service in line with business or cost justification. Similarly, meaningful SLA help ensure that quality and timelines standards are maintained, while providing useful insights into operational processes.

Abdulrazak Fatunbi
Fidelity Bank Plc



Managing Pushbacks in Audit Engagements

The Oxford Advanced Learners Dictionary defines Pushback as an act of opposing or resisting a plan, an idea, or a change. We have over the years identified reluctance on the part of some audit clients to readily accept criticism as represented in audit findings. There are also extreme cases of standoff or impasse between Chief Audit Executives (CAEs), or members of their staff and management over a contentious issue. The inevitability of resistance during the auditing process is underscored by the April 2020 survey conducted by Ernst and Young across 437 CAEs or equivalents. The survey identified pushbacks as one of the key challenges facing Internal Audit.

Two things however stand out: A factual and well-presented audit finding cannot be successfully flawed by the client, though it is virtually impossible not to have complaints related to audit reports. It is based on the latter premise that I chose to use “managing”

rather than “preventing” pushbacks in the subject caption. Secondly, the propensity and severity of pushbacks can be a measure of maturity of the Internal Audit (IA) function.

Sources of tension

Ideally, the client and management of IA are joint stakeholders in the quest to strengthen their organization's risk management, governance processes and internal controls. However, it is management's responsibility to determine and set performance goals, as well as implement controls. Furthermore, IA has no authority to insist on a different form of corrective action when the engagement client's proposal is adequate and effective.

Misunderstanding or misalignment of these roles at strategic level is a major source of conflict, making

recommendation without considering the full ramifications of the issues or feasibility of such recommendation. Knowing that the business understands their issues and constraints better and would be responsible for effecting the corrections / remediations, it is more impactful to have “agreed corrective actions” rather than a recommendation. In other words, the auditor provides an avenue to discuss the issues and interact with the engagement client such that they together agree on the most appropriate measures to remediate the issues. The client sees the solutions as his own and would be keen to follow through the corrective actions as agreed with the auditors.

The client in this instance cannot possibly antagonize his own well thought-out regularization process. It is important though for the auditor to be able to provide guidance and technical support in the discussion leading to the corrective actions. This has worked for

which in turns dovetails into the overall rating for the area or entity reviewed. The bottom-line therefore, is that there is need for robust discussion and agreement by both sides.

The impact of preconceived notions on part of the engagement clients is significant. Notwithstanding the improvements in communications and steps taken to ensure more participatory audit procedures by some auditors over the years, some audit engagement clients still harbor suspicions which stem from the age-long (traditional?) belief that auditors are policemen and faultfinders. This is an area in which auditors need to demonstrate that they are indeed enablers of business and valuable partners in solving organizational problems.

It's not about what we say but what we do genuineness of purpose needs to be demonstrated by actions. We have reached a stage where colleagues



us in my organization.

Similarly, the application of timelines for correction of observed lapses can be a source of friction. There are instances where the auditors mandate their clients to close audit issues within timelines specified by the auditors, often without recourse to their clients' inputs. In reality, the engagement clients understand their issues better, have more information about dependencies (and constraints) and what it takes generally, to close the issues. It is therefore more effective to apply timelines that the risk /process owner agrees to.

However, the auditor is not expected to accept any proposed timelines without questioning. The engagement client should be informed that the longer it takes, to close an issue, the higher the risk inherent and the more adverse the rating could be;

from other departments routinely engage IA for advisory services and seek our support in facilitating some projects. These include value-adding activities such as thematic reviews and consulting activities that solve business problems. Doing this has improved IA relationships with the engagement clients in my organization. We thus have less tendencies for push backs from planned engagements, as they see us more as partners. There are still occasional disagreements but these in recent years have been minimal and not cardinal/fundamental in nature.

Audit reports can have impact on a professional's career. Tempers could therefore rise if the audit rating comes with sanctions, such as those impacting on the management's performance assessment or incentive compensation. It is often helpful for the auditor to fully explain the audit process including scope,

objectives, report ratings and give regular feedback in course of the audit. There is no need of delaying 'bad news' which inevitably results in shocks.

The auditor should promptly provide an assessment of issue assurance i.e closure of previous audit findings, state the implications (if any) in the current audit before going far into a new or subsequent audit. Ideally, failure or poor ratings in issue assurance would result in an adverse rating in the current audit. Regular feedbacks and constructive engagements also give less room for rancor between auditors and their clients. The use of a rating guide is helpful in this respect. A way around this issue is for improved

improvement/Unsatisfactory) to be more objective and easily explainable to stakeholders. Doing this would largely remove prejudice from the clients' minds and give less room for resentments.

As simple as it seems, phraseology or wording of audit findings can make or mar an audit report. We should always remember that people naturally do not want their inadequacies exposed especially to their bosses. The auditor should make conscious efforts to avoid harsh or indicting comments or personal biases, which could lead to the engagement clients withdrawing their cooperation, and possibly frustrating the audit. This is especially where fraud



disclosures and transparency in audit ratings on the part of auditors.

Lack of understanding about the audit process is another source of pushbacks. Simple actions such as regular interactions between both sides in course of the review can go a long way to ease tensions. Many engagement clients would like to better understand audit ratings. Though the auditor is entitled to his opinion, the basis of assessment should not be a 'black box' which he only can decrypt.

The auditor should explain the key drivers of audit ratings and throw light on scoring / rating guides to guide the client. The final audit report should also capture the basis of assessment. Though there is always the element of subjectivity in ratings; it is better for the audit ratings (e.g Satisfactory/ Room for

has not been proven. For example, an audit observation that states that *"our review of cash and teller activities revealed significant non-compliance with operational procedures...."* is a safer and more appropriate option at the initial instance where actual theft has not yet been established. This contrasts with an observation like the following statement which could result in immediate adverse reactions and rancor: *"our review of cash and teller activities revealed poor treatment of transaction and missing cash..."*

Another example: *'the department is ineffective in managing....'* compared with *'the process of managing the bank's....is ineffective.* The former can be perceived by the client as pointing to his inefficiency as a manager while the latter beams the searchlight away from the departmental head's personality to the process being reviewed. It is for a similar reason that I

have refrained from referring to parties being audited as 'auditees' in this write-up. It is more comely to refer to them as clients. The Team Leads and Audit Managers should instill a quality control system that promptly identifies and corrects such weaknesses. Indeed, they are better prevented.

There are often findings with dependencies arising from audits. These are issues that cannot be wholly resolved by the client being audited. Recognizing this would give less cause for frictions. A practical way of addressing such is to do a proper root cause analysis, identify the factors required to close the issues and the persons responsible for the desired outcomes.

The report should then reflect the 'joint action owners' (complete spectrum of officers responsible for remediation) rather than making the client being audited solely responsible for closing such issues. Added to this is the need to the audit report to distinguish policy and procedural infractions from good-to-have observations. The audited entity or client should be assessed on the former, not on good to have issues. Doing these would ensure objectivity and give less room for unnecessary frictions which are not helpful to the organization.

The big elephant in the room is the auditor's competence, which is quite easy for the client to decipher or identify. Although auditors typically take steps to enhance their preparedness for engagements, there is still the possibility of Detection Risk which is the risk that the auditor will not detect a misstatement that exists in an assertion that could be material, either individually or when aggregated with other misstatements. There is also chance that the auditor would exhibit inadequate technical depth or understanding of the review area. If such occurs, it will result in needless frictions and disagreements with the engagement clients, who will gleefully point out inadequacies/errors in the auditor(s) assertions. It is therefore imperative for auditor to understand the product offerings, the related assets, and liabilities, how transactions are processed, the data, the systems, and the risks etc.

Experts have opined that internal auditors should do extensive trainings to keep pace with changing business trends and issues from a business standpoint, technical standpoint, and leadership as well as interpersonal standpoint. Audit leaders should drive the efforts to ensure that auditors are life-long learners and naturally inquisitive.

However, auditors should not be quick to jettison or drop audit findings because of pushbacks. We should actually welcome it to better understand the clients'

viewpoints including the depth of issues at stake and how reaching the implications of the findings could be. I have discovered that pushbacks on the basis of responsibility for a lapse, helps my team to identify interdependencies (other departments responsible for fixing the issue), joint corrective action owners (complete spectrum of officers responsible for remediation) and possible targets of future audits and spot checks.

Conclusion

People may still pushback on you when you have done a good job. Even the most thoroughly researched, rigorously supported, and fairly presented audit reports can generate disagreements. Such pushback would however not stand the test of time where proper audit procedures have been followed. What is required in such instance is for the auditor to be tough and resilient in those scenarios so that you can push through all the resistance and then work with people in a constructive manner.

However, pushbacks are largely avoidable and manageable by taking care of little things including showing empathy by also walking in the shoes of the business people they audit, improving stakeholders' engagements, employing a participative audit approach to minimize conflict and build a shared interest in the engagement, using more appropriate wordings in audit observations and reports and instilling a process of agreeing factual accuracies with the client, even before the audit exit meetings. Contentious issues should not be left till the close out meeting as you cannot always predict the outcomes especially considering that persons who were not part of the audit e.g divisional heads of the engagement clients and other managers (within and outside audit) might be attending. You would not look professional arguing with clients in presence of your boss!

The use of 'audit satisfaction survey' questionnaires /surveys after audits have also been known to be a veritable source of clients' post-audit feedback and a tool for improving audit engagements. My team's approach is for the client to send the survey response directly to the Audit Manager/Unit Head. We have found this useful in improving quality of subsequent audit engagements and relationship with clients. Collaboration is the way to go in building highly collaborative and mutually beneficial relationships.

Michael Ajuyah
Head, Credit Audit
Internal Audit & Management Services
Ecobank Nigeria Ltd



Taking Care of Your Mental Health

Health, in common language, is wealth. An individual's state of health must be in its totality to enable the achievement of wealth. At the centre of this healthiness lies a person's state of mental health. In simple terms, mental health is the psychological and emotional well-being of an individual. According to the World Health Organization (WHO), mental health is 'a state of well-being in which the individual realizes his or her own abilities, can cope with the normal stresses of life, can work productively and fruitfully, and is able to contribute to his/her community'.

Mental health is very vital at every stage of life from childhood through to adulthood because it determines the extent of functionality in all facets of one's life. As such, a neglect of this aspect of one's health can result in several disorders like moodiness/acute depression, anxiety disorders, panic attacks, etc.

Maintaining good mental wellness is of utmost importance as positive mental health enables people to realize their full potentials, make positive impacts and help in improved performance/output at work. In taking care of our mental health, the following tips are very helpful:

- 1) **Eat right & sleep well:** The human body like every other machine, needs some time out for refreshing for optimal performance always. Ensure to eat good foods, take plenty vegetables, whole grains, fruits and proteins. Cut down on your sugar and soda intake. Try getting adequate rest especially at night, as sleep is very vital for our brains & for a healthy nervous system.
- 2) **Regular exercise & workouts:** Physical exercise can help to eliminate mood swings, ease of fatigue as well as manage stress. You need not register at the gym or run a mile to

achieve this. There are several & simple workouts you can do in the comfort of your home, which are also easily accessible from Youtube downloads and other mobile apps.

- 3) **Recreation for renewal:** Try making out some time to enjoy some fun moments with your loved ones and friends. Do those hobbies

consequences of setting unrealistic goals which could lead to despair, anger, depression, anxiety and sense of loss.

- 5) **Need help, seek it:** Be prompt in asking for help whenever you have challenges in your health. Don't die in silence and be not ashamed in asking for assistance or support if



and simple things that give you pleasure like listening to your favorite songs, taking a stroll in the neighborhood, watching movies at home or cinemas, playing games, painting, cycling, dancing, reading, baking, travelling to new places as your pocket permits and so on. Leisure times help us to maintain balance and to ease off irritability.

- 4) **Self-love:** Because you can only give to others what you have, try to treat yourself with love and respect. Avoid extreme self-criticism. Speak positively to yourself and into your life, deviate from being too hard on yourself. Do not over-exert yourself. It's okay to have big dreams and ambitions, but make sure they are achievable so you wouldn't suffer the

you're feeling stressed or unwell. Try speaking with your family, a trusted friend or a professional therapist for treatment.

The list is endless, but occasionally, shut down all the noise around you and breath. Yes, inhale deeply and reflect. Look around you, admire the beautiful works of nature and be thankful. Meditation helps in relaxing the nerves, eases off tension and in relieving anxiety, thereby helping us to be in a better place to regain our sanity and sense of being.

Nneka Okwuogu
Business Office Audit
UBA Plc



ASSOCIATION OF CHIEF AUDIT EXECUTIVES OF BANKS IN NIGERIA [ACAEBIN]

Secretariat: Plot 1398B Tiamiyu Savage Street, Victoria Island, Lagos.

Telephone: +23413424805, Website: www.acaebin.org

E-mail: info@acaebin.org

...Objectivity & Integrity

COMMUNIQUE ISSUED AT THE END OF THE 2022 ANNUAL RETREAT AND CONFERENCE OF THE ASSOCIATION OF CHIEF AUDIT EXECUTIVES OF BANKS IN NIGERIA (ACAEBIN), HELD BETWEEN MARCH 30TH AND APRIL 2ND, 2022 AT THE IBOM ICON HOTEL & GOLF RESORT, UYO, AKWA IBOM STATE.

The Association of Chief Audit Executives of Banks in Nigeria (ACAEBIN) held its 2022 Annual Retreat and Conference recently. In attendance were Regulators and other key Industry Practitioners. The event was declared open by the Executive Governor of Akwa Ibom State, Mr. Udom Emmanuel, who was ably represented by the Deputy Governor, Mr. Moses Frank Ekpo. Discussions at the retreat centered on the theme, 'Shaping Internal Audit Evolution.' With rapid changing stakeholder expectations, newer perspectives on risk management, and demands from the board, senior management, and regulatory authorities, Internal Audit is evolving to not only enhance operational efficiency and compliance with internal controls, but also enable value preservation and creation. Below is the resolution reached during the conference:

1. According to Companiesmarketcap.com, six out of ten world's most valuable companies in 2020 have leveraged on disruptive technology. Therefore, banks need to be agile, innovative, embrace Artificial Intelligent powered by risk modeling and apply continuous auditing while ensuring data protection and privacy.
2. As the digital space widens, the Internal Audit Function should ensure a well-defined strategy on digital acceleration as such, banks must, through training and retraining, ensure that Chief Audit Executives (CAEs) and other internal audit staff have sufficient knowledge of key information technology risks, controls and available technology-based audit techniques.
3. In leading audit transformation through Advanced Analytics & Artificial Intelligence (AI), Internal Auditors should embrace skills-based hiring, incorporate data analytics and continuous audit capabilities into risk assessment, planning, scoping, execution and the reporting phases of the internal audit methodology.
4. As emerging risks occasioned by the Covid-19 pandemic continue to rise and organizations embrace remote working, the Internal Audit Function should ensure banks put in place a framework for remote working. This should guide how remote working is performed; who should have access to what and how risks associated with the remote working can be mitigated with proper network segmentation to ensure that critical IT infrastructures, especially, financial applications are put in a separate segment of the network with additional security. Also, Internal Audit should review periodically the Virtual Private Network (VPN) used for remote access with a view to identifying any emerging vulnerabilities.
5. In a bid to enhance insight to reports to the Audit Committee, Internal Audit function must innovate and reinvent itself into an agile, multi-skilled and technology-enabled function, providing concise, timely and action-oriented reports with visuals/dashboards.
6. As the concept of Environment, Sustainability and Governance (ESG) continues to garner traction in both the public and private sectors, the Internal Audit Function must participate in ESG risk assessment and guidance for the identification of key risks and ensuring that they are audited annually with non-compliance highlighted and reported to senior management and Board Audit Committee.
7. As the economy and society continue to evolve, the Internal Audit Function should embrace the following seven basic techniques in navigating the Nigeria regulatory landscapes: Anticipate, Collaborate, Adapt, Educate, Brainstorm, Innovate and Negotiate - constructively engaging the Regulators on existing and new regulations that need re-alignment.
8. In ensuring collaboration across assurance functions for business impact, the Audit Charter should be updated to incorporate Combined Assurance Framework using Integrated Governance, Risk and Control (GRC) softwares that make it possible for assurance functions to interact, source, analyze, track, and communicate data to gain deeper insight into organizational operations. Internal Audit should liaise with other internal and external assurance providers to ensure proper coverage and minimize duplication of efforts.

Signed: Association of Chief Audit Executives of Banks in Nigeria (ACAEBIN)



Happy Birthday Distinguished CAEs



PRINCE AKAMADU



April 06



RASHAQ ALAWODE



April 11



ABIODUN GBADAMOSI



April 16



MOGBITSE ATSAGBEDE



May 12



RICHARD BELLO



June 07



YEMI OGUNFEYIMI



June 13



LYDIA ALFA



June 19

We your colleagues join your families and friends to wish you long life in good health of mind and body



Access Bank Plc
Yinka Tiamiyu
Plot 999C Damole Street,
Victoria Island, Lagos
tiamiyu@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



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



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




Ecobank Nigeria Ltd
Felix Igbiososa
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




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



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




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



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



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



Greenwich Merchant Bank Ltd
Rasaq Alawode
Plot 1696A Oyin Jolayemi Street,
Victoria Island, Lagos
rasaq.alawode@greenwichbank
group.com
08083248797



Sterling Bank Plc
Femi Jaiyeola
1st Floor,
Sterling Bank Plc Head Office
(Annex), Ilupeju
239/241, Ikorodu Road, Lagos.
Femi.jaiyeola@sterling.ng
07012952707



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



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



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




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



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



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



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



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



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