Association Of Chief Audit Executives Of Banks In Nigeria (ACAEBIN)

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

Download e-copy here

Design+print
Prowess
08039221516

(ACAEBIN) Q2, 2025 A Quarterly Publication of the Association of Chief Audit Executive of Banks in Nigeria



Eagle Eye

Strengthening Corporate Governance through Effective Internal Auditing: Challenges and Opportunities





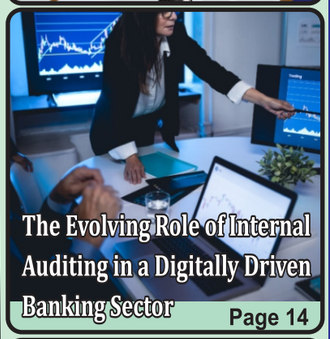
Internal Auditors and AI: The Urgent Need for a Paradigm Shift
Page 10

Wellness

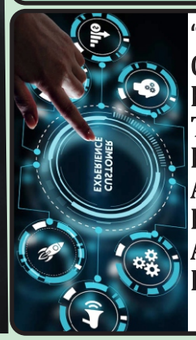
People sitting for too long risk hypertension, say physicians



Page 33



The Evolving Role of Internal Auditing in a Digitally Driven Banking Sector
Page 14



"Enhancing Customer Experience Through Effective ATM Reviews: A Strategic Imperative"
Page 7

ACAEBIN EXCO MEMBERS



Aina Amah
Chairperson



Mogbitse Atsagbede
1st Vice Chairman



Femi Fatobi
2nd Vice Chairman



Ugochi Osinigwe
Treasurer



Olusemore Adegbola
Auditor



Olusegun Famoriyo
Chairman, Research & Publication Sub-Comm.



Adeola Awe
Chairperson, Payment & Systems Sub-Comm.



Olurotimi Omotayo
Ex-officio I



Oluwole Esomojumi
Ex-officio II

DIRECTORY

NEXIM BANK
Ayaghena Razaq Ozemede
NEXIM House
Plot 975 Cadastral Zone AO,
Central Business District,
P.M.B. 276, Garki,
Abuja, Nigeria.
ozemedera@neximbank.com.ng 094603642



08024725055

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



08028346740

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



08033769975

Nova Merchant Bank
Adeola Awe
23, Kofo Abayomi Street
Victoria Island, Lagos,
Nigeria.
Adeola.Awe@novambl.com



0802 328 9408,
0913 483 2118

Optimus Bank Ltd.
Adeyinka Oladepo
55, Bishop Oluwole Street
Victoria Island,
Lagos
adeyinka.oladepo@optimusbank.com



07035316372

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



023014800, 07081876026,
08102853283

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



08023096373

Premium Trust Bank Limited
Dumebi Okwor
Plot 1612 Adeola Hopewell St,
Victoria Lagos
Dumebi.Okwor@Premiumtrustbank.com



08175500864

ProvidusBank Ltd.
Aina Amah
54, Adetokunbo Ademola Street,
Victoria Island, Lagos
aamah@providusbank.com



08029087442

Rand Merchant Bank
Femi Fatobi
3rd Floor, Wings East Tower,
17A, Ozumba Mbadiwe Street
Victoria Island, Lagos, Nigeria.
Femi.fatobi@rmb.com.ng



01-4637960,
08028514983

Stanbic IBTC Plc
Adenike Odukomaiya
Plot 1712, Idejo Street
Victoria Island, Lagos, Nigeria.
Adenike.odukomaiya@stanbicibtc.com



0803 324 1128

Standard Chartered Bank Nig. Ltd.
Michael Fatunbi
142, Ahmadu Bello Way
Victoria Island, Lagos,
Nigeria.
Michael.Fatunbi@sc.com



08023018717

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



08068250302

SunTrust Bank Nig. Ltd.
Yousuph Edu
1, Oladele Olashore Street,
Off Sanusi Fafunwa Street,
Victoria Island, Lagos, Nigeria.
[illegible]



08037274559

TajBank Nigeria Limited
Plot 72, Ahmadu Bello Way,
Central Business District Abuja,
Nigeria.

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



08033039481,
08056900079

Union Bank of Nigeria Plc
Victor Ikeneku
36 Marina,
Lagos.
voikeneku@unionbankng.com



08033338100

United Bank for Africa Plc
Kayode Ajayi
UBA House
57 Marina, Lagos
Kayode.Ajayi@ubagroup.com



08033293948,
07034125788

Unity Bank Plc
Olusegun Michael Famoriyo
Unity Bank Tower
Plot 42, Ahmed Onibudo Street,
Victoria Island, Lagos
Ofamoriyo@unitybankng.com



08023145535

Wema Bank Plc.
Oluwole Esomojumi
Wema
Towers
54 Marina, Lagos
oluwole.esomojumi@wemabank.com

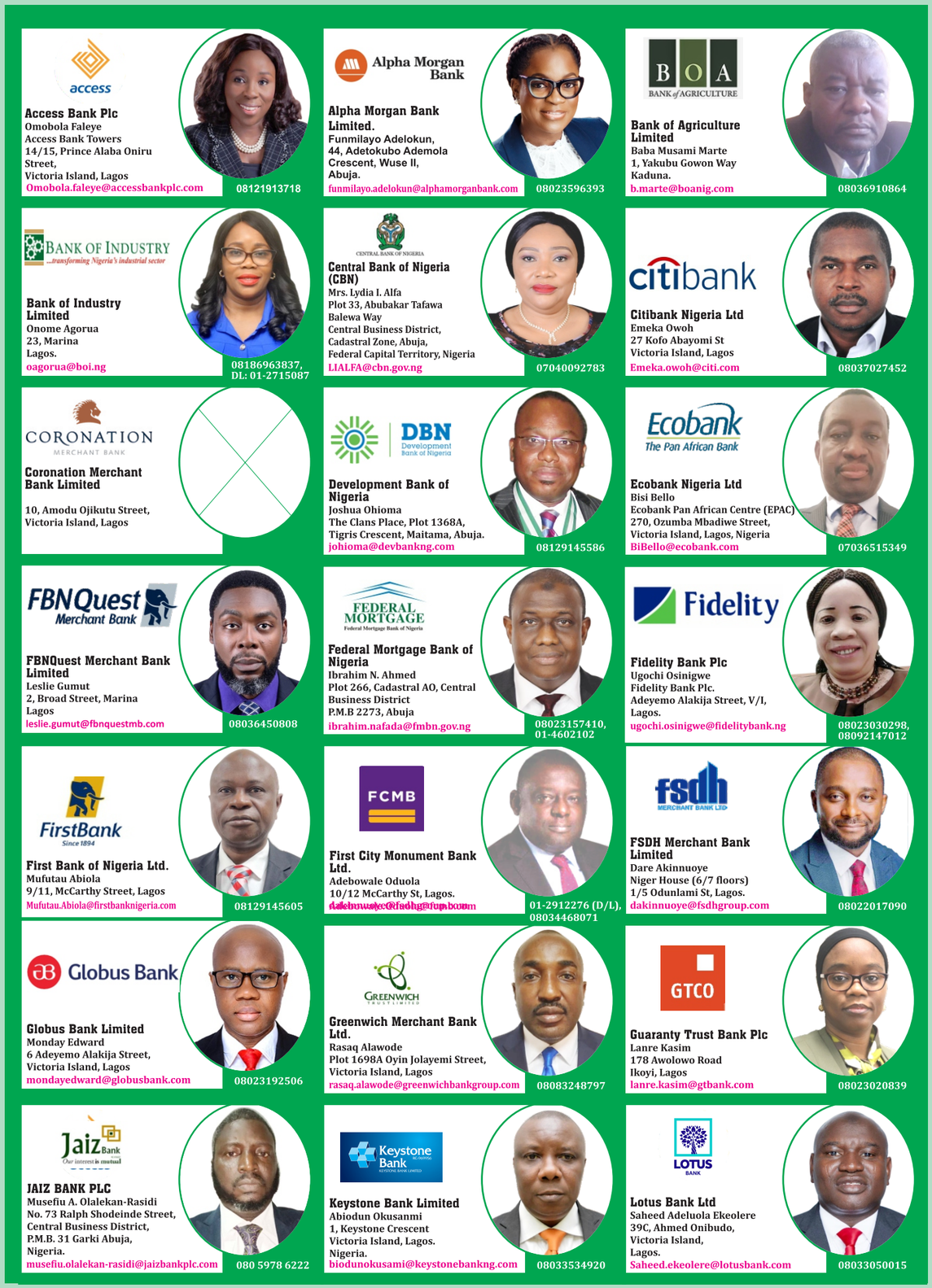


08094214819

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



08023270998



CONTENT

4 Strengthening Organizational Integrity ...
7 "Enhancing Customer Experience Through Effective ATM ...
12 Microservices Architecture: Implementations and ...
21 The Role of Internal Audits in Detecting and Preventing ...
24 The Internal Auditor's Dilemma: Balancing Work, Ethics...
26 Strengthening Corporate Governance through Effective ...
28 Ten Ways to Enhance Ethical Leadership in Internal Audit ...
30 Key Reminders to CAEs to Ensure Efficiency ...

Our Mission Statement

ACAEBIN is a non-profit making body that fosters interaction among CAEs in Nigeria and Strives to promote competence, ethical standards and professional behaviors amongst member organization.

Editorial Team

Segun Famoriyo
Olusemore Adegbola
Femi Fatobi
Ugochi Osinigwe
Adeola Awe

Reader's Comments

kindly send your comments/feeback to info@acaebin.org

Members of Research and Publication Committee

Olusegun Famoriyo	(Unity Bank Plc, Chairman)
Ugochi Osinigwe	(Fidelity Bank Plc)
Baba M. Marte	(Bank of Agriculture)
Awe Adeola	(Nova Bank Ltd)
Femi Fatobi	(Rand Merchant Bank Nig. Ltd)
Abiodun Okusami	(Keystone Bank Ltd.)
Ayaghena R. Ozemede	(NEXIM Bank)
Musefiu R Olalekan	(Jaiz Bank Plc)
Dare Akinnoye	(FSDH Merchant Bank Ltd.)
Sadiku O. Kanabe	(The Infrastructural Bank Plc)
Ibrahim N. Ahmed	(FMBN)
Olusemore Adegbola	(Nigeria Mortgage Refinance Company)
Saheed Ekeolere	(Lotus Bank)
Emeka Owoh	(Citibank Nigeria Limited)
Kayode Ajayi	(UBA)
Rotimi Omotayo	(Polaris Bank Ltd)
Edward Onwubuya	(Sterling Bank Plc)
Joshua Ohioma	(Development Bank of Nig)
Onome Agorua	(Bank of Industry Limited)
Leslie Gumut	FBNQuest Merchant Bank Limited
Rasaq Alawode	(Greenwich Merchant Bank Ltd)
Dumebi Okwor	(Premium Trust Bank Limited)
Lydia I. Alfa	(Central Bank Nigeria, Advisory)
Rasaq Alawode	(Greenwich Merchant Bank Ltd)

Editorial



Beyond Compliance- Internal Audit's Quiet Revolution

Corporate governance has long served as the scaffolding of institutional trust. Yet in today's volatile, fast-evolving environment, that structure increasingly rests on the shoulders of a function often underestimated: internal audit.

Our cover story, "Strengthening Corporate Governance through Effective Internal Auditing," presents a powerful case for this shift. Internal auditors are no longer confined to checklists or post-facto compliance reviews. They are emerging as champions of accountability, architects of risk resilience, and stewards of long-term value integral to how organizations govern themselves.

However, this transformation is not without complexity. As this issue explores, the audit landscape is rapidly changing. The rise of artificial intelligence, the growing threat of fraud collusion, and the decentralization of systems via microservices all demand more than technical know-how. They require moral clarity. Today's auditor must wear many hats: technologist, ethicist, strategist. It is, fundamentally, a human endeavour.

Articles like "The Internal Auditor's Dilemma" remind us that auditors face significant pressure grappling with resistance, burnout, and misperceptions. Meanwhile, calls for ethical leadership and proactive audit exception handling emphasize the need to move from reactive oversight to values-driven engagement.

So where do we go from here?

The answer lies in redefining the internal auditor not as a silent observer, but as an active force in shaping culture, advancing transparency, and enabling digital transformation, with integrity at the core.

Effective governance today is not just about structures or systems it's about real-time decisions, behaviours, and trust. It starts with those who are willing to ask the hard questions before crises unfold.

In this edition, we invite you to consider not just how audits are performed, but why they matter especially now. To support your work, we also provide a compendium of published CBN Circulars from Q4 2024 through H1 2025.

Because in a world increasingly governed by complexity and code, it is not only policy but principle that will define the institutions worthy of trust.

Happy reading.

Olusegun Famoriyo
Editor-in-Chief

Strengthening Corporate Governance Challenges and Opportunities

In today's complex and dynamic business environment, corporate governance plays a crucial role in ensuring the accountability, transparency, and sustainability of organizations (Shleifer & Vishny, 1997). Effective corporate governance is essential for maintaining stakeholder trust, promoting organizational performance, and mitigating risks (Cadbury Committee, 1992). Internal auditing is a critical component of corporate governance, providing assurance on the effectiveness of risk management, control, and governance processes (IIA, 2017).

Research has shown that effective internal auditing can contribute significantly to good corporate governance by identifying and mitigating risks, improving operational efficiency, and ensuring compliance with laws and regulations (Gramling et al., 2004). Internal auditors can provide valuable insights and recommendations to management and the board of directors, helping to improve governance processes and organizational performance (COSO, 2017).

Despite its importance, internal auditing faces several challenges, including lack of resources, inadequate independence, and limited scope (IIA, 2017). These challenges can limit the effectiveness of internal auditing and compromise its ability to contribute to good corporate governance.



This article explores the role of internal auditing in strengthening corporate governance, highlighting the challenges and opportunities associated with effective internal auditing. By examining the benefits and limitations of internal auditing, this article aims to provide insights into the importance of internal auditing in promoting good corporate governance and organizational performance.

The Role of Internal Auditing in Corporate Governance

Internal auditing plays a vital role in corporate governance by providing assurance on the effectiveness of risk management, control, and governance processes (IIA, 2017). Effective internal auditing can help organizations improve transparency,

Continuing, the physician said, “If you sit down for too long, your blood will not be moving as in somebody who moves up and down and jumps up and down.

” Reduced blood flow can increase your risk of getting what is called thrombosis formation and can increase the risk of developing a blood clot in some people.

” If those blood clots dislodge, if they drop in the heart, they can cause a heart attack, if they drop in the lungs, they can cause pulmonary embolism. If they enter the brain, they can cause strokes.”

He advised people to shun sedentary lifestyles, exercise and be healthy. For those already living with cardiovascular diseases, he urged them to go for cardiovascular risk assessment.

The American Heart Association also confirmed that too much sedentary time increases the risk of cardiovascular disease, diabetes, and death.

In an advisory published on its website titled, 'Sitting too much may raise heart disease risk', the foundation expressed worry that sedentary time is rising, lamenting that adults spend more than nine hours a day being sedentary.

AHA said people are spending an estimated six to eight hours a day engaged in sedentary behavior, which includes sitting, driving, reading, TV viewing, screen time, and computer use.

“Our bodies were built to move all day. They weren't built to be idle and stationary with a metabolic rate similar to a person in a coma.

“When we're depriving ourselves of that kind of essential muscular activity throughout the day, very potent things happen inside our bodies”, it noted.



Also speaking, a Senior Consultant at the Lagos State Health Service Commission, Dr.-Sylvester Ikhisemojie, said indeed sitting for too long causes adverse health events.

According to him, this lack of physical activity is now known to be the precursor of loss of muscle mass, loss of bone density, progressive weight gain, and deep vein thrombosis.

“This has spurned a new term in the medical lexicon known as The Sitting Disease, a description of the range of effects that prolonged sitting can have on our overall health.

“These problems have been variously identified to include diabetes, high blood pressure, formation of blood clots in the lower limbs and elsewhere in the body, and the incidence of non-alcoholic fatty liver disease, itself a relatively new disease condition.

“All these problems, in addition to the ones already named in the paragraph above, constitute a significant threat to our overall health and life expectancy.

” The cumulative effects of these problems cannot be stressed too strongly. At the close of work and following the long hours sitting at our desks in the office, we take another long drive back home, perhaps take a shower and head to the dinner table before retiring to the sofa or couch for several more hours watching television.

“Home videos, Netflix, and a variety of entertainment channels keep us engaged in the sitting position for several more hours in the early evening before we retire to bed. We wake up the following morning and continue the damaging cycle of activity.

” Such physical inactivity has now also been linked to depression, certain types of cancer, and diminishing levels of physical fitness”, he explained.

Culled from: healthwise.punchng.com

People sitting for too long risk hypertension, say physicians

Sitting for too long is bad and has severe health consequences that many people who are engaged in such unhealthy habits are not aware of, physicians have said. The experts said sitting for too long is associated with obesity and increased blood pressure, especially among people with risk factors.

According to them, humans are built to stand upright, and the heart and cardiovascular system work more effectively that way. The physicians pointed out that swelling in the ankles, feet, and legs is often caused by a build-up of fluid in these areas due to too much sitting or standing.

A Consultant Physician and Cardiologist, Dr. John Asekhame, advised people not to sit for too long, citing various health risks. Asekhame who works with Providence Multi-Specialty Hospital, Abuja, said though not applicable to everyone, some people are susceptible to developing cardiovascular diseases by sitting for too long.

Speaking in an interview with PUNCH Healthwise, the cardiologist noted, “Sitting for too long increases your risk for obesity which increases your risk of adverse cardiovascular diseases. Sitting for too long is dangerous to health. ”If you notice some people when they sit for too long, they start having leg swelling, and the rest. So, it is encouraged to stand up probably after 30 minutes, exercise, and walk around or shake your body instead of being sedentary for a long time.

” Sitting for too long means that you are not consuming energy. It means that you are not burning out excess fat or energy which increases your risk of storing what you eat into fat.

“When that gets on for too long, you can develop what is called insulin resistance. So, insulin resistance can increase your risk of developing Type 2 diabetes.”

Asekhame reiterated that sitting for too long increases the risk of developing diabetes in people who have a risk, warning that diabetes on its own can cause stroke and heart attack even 'if your blood pressure is normal”.



Through Effective Internal Auditing:



accountability, and risk management, ultimately enhancing organizational performance (COSO, 2017). Internal auditing can contribute to good corporate governance in several ways:

Risk management: Identifying and assessing risks and evaluating the effectiveness of risk management processes (COSO, 2017).

Internal controls: Evaluating the design and operating effectiveness of internal controls, and providing recommendations for improvement (SOX, 2002).

Governance processes: Evaluating the effectiveness of governance processes and providing insights and recommendations to management and the board of directors (IIA, 2017).

Challenges in Implementing Effective Internal Auditing in Corporate Governance

Internal auditing serves as a vital component of corporate governance, delivering independent assurance on the efficacy of risk management, internal controls, and governance processes, thereby enhancing organizational transparency and

accountability (IIA, 2017). However, implementing effective internal auditing can be challenging, particularly in complex and dynamic business environments. Some of the common challenges in implementing effective internal auditing in corporate governance include:

Independence and objectivity: Maintaining independence and objectivity is essential for internal auditors, but this can be compromised if they are not adequately separated from management or have conflicting responsibilities (SOX, 2002).

Resource constraints: Insufficient resources, including budget, personnel, and technology, can limit the scope and effectiveness of internal audit activities (IIA, 2017).

Lack of stakeholder support: Lack of support from management and the board of directors can limit the effectiveness of internal auditing and compromise its ability to influence governance processes (Gramling et al., 2004).

Complexity of governance processes: The complexity of governance processes and the need to navigate multiple stakeholders can make it challenging for internal auditors to provide effective assurance (COSO, 2017).

Emerging risks and regulatory requirements: Keeping pace with emerging risks and changing regulatory requirements can be a significant challenge for internal auditors (IIA, 2017).

Opportunities for Strengthening Corporate Governance

Strengthening corporate governance can bring numerous benefits, including improved organizational performance, enhanced stakeholder trust, and better risk management. Some of the opportunities for strengthening corporate governance include:

Implementing Effective Internal Auditing: Internal auditing can provide assurance on the effectiveness of risk management, control, and governance processes, helping to identify areas for improvement (IIA, 2017).

Enhancing Board Composition and Diversity: A diverse and experienced board can provide effective oversight and guidance, helping to drive organizational performance (Cadbury Committee, 1992).

Improving Transparency and Disclosure: Transparent and timely disclosure of information can help to build stakeholder trust and confidence in the organization (OECD, 2015).

Strengthening Risk Management: Effective risk management can help organizations identify and mitigate risks, reducing the likelihood of losses and reputational damage (COSO, 2017).

Fostering a Culture of Accountability: A culture of accountability can help to promote ethical behaviour and ensure that organizational decisions are made in the best interests of stakeholders (OECD, 2015).

Conclusion

Strengthening corporate governance through effective internal auditing is crucial for ensuring the accountability, transparency, and sustainability of organizations. While challenges exist, such as maintaining independence and objectivity, allocating sufficient resources, and keeping pace with emerging risks, the benefits of effective internal auditing far outweigh the costs. By leveraging opportunities to improve governance practices, organizations can enhance risk management, improve transparency and accountability, and drive long-term success. Effective internal auditing is essential for promoting good corporate governance and ensuring that organizations operate in a responsible and ethical manner.

References

Auditors (IIA). (2017). International Standards for the Professional Practice of Internal Auditing.

Cadbury Committee. (1992). The Financial Aspects of Corporate Governance.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). Enterprise

Risk Management - Integrating with Strategy and Performance. Institute of Internal

Gramling, A. A., Maletta, M. J., Schneider, A., & Church, B. K. (2004). The Role of Internal Auditing in Corporate Governance. Journal of Accounting Literature.

Organisation for Economic Co-operation and Development (OECD). (2015). G20/OECD

Principles of Corporate Governance.

Sarbanes-Oxley Act (SOX). (2002). Public Law 107-204.

Shleifer, A., & Vishny, R. W. (1997). A Survey of Corporate Governance. Journal of Finance.

Emuebie Emeke,
Head, Branch & Services Audit,
Internal Audit Department,
Union Bank

Compendium of published CBN Circulars from 4th Quarter 2024 to 2nd Quarter 2025.

S/N	DATE PUBLISHED	TITLE OF CIRCULAR	REFERENCE	DEPARTMENT
1	11/25/2024	Guidelines for the Electronic Foreign Exchange Matching System (EFEMS)	FMD/DIR/CON/OGC/038/151	Financial Markets Department
2	11/26/2024	Guidelines for the Electronic Foreign Exchange Matching System (EFEMS)	FMD/DIR/CON/OGC/038/152	Financial Markets Department
3	11/27/2024	Guidelines for the Electronic Foreign Exchange Matching System (EFEMS)	FMD/DIR/CON/OGC/038/153	Financial Markets Department
4	11/28/2024	Guidelines for the Electronic Foreign Exchange Matching System (EFEMS)	FMD/DIR/CON/OGC/038/154	Financial Markets Department
5	11/29/2024	Guidelines for the Electronic Foreign Exchange Matching System (EFEMS)	FMD/DIR/CON/OGC/038/155	Financial Markets Department
6	11/30/2024	Guidelines for the Electronic Foreign Exchange Matching System (EFEMS)	FMD/DIR/CON/OGC/038/156	Financial Markets Department
7	12/1/2024	Guidelines for the Electronic Foreign Exchange Matching System (EFEMS)	FMD/DIR/CON/OGC/038/157	Financial Markets Department
8	12/2/2024	Guidelines for the Electronic Foreign Exchange Matching System (EFEMS)	FMD/DIR/CON/OGC/038/158	Financial Markets Department
9	12/3/2024	Guidelines for the Electronic Foreign Exchange Matching System (EFEMS)	FMD/DIR/CON/OGC/038/159	Financial Markets Department
10	12/4/2024	Guidelines for the Electronic Foreign Exchange Matching System (EFEMS)	FMD/DIR/CON/OGC/038/160	Financial Markets Department
1	12/5/2024	Guidelines for the Electronic Foreign Exchange Matching System (EFEMS)	FMD/DIR/CON/OGC/038/161	Financial Markets Department
12	12/6/2024	Guidelines for the Electronic Foreign Exchange Matching System (EFEMS)	FMD/DIR/CON/OGC/038/162	Financial Markets Department
13	12/7/2024	Guidelines for the Electronic Foreign Exchange Matching System (EFEMS)	FMD/DIR/CON/OGC/038/163	Financial Markets Department
14	12/8/2024	Guidelines for the Electronic Foreign Exchange Matching System (EFEMS)	FMD/DIR/CON/OGC/038/164	Financial Markets Department
15	12/9/2024	Guidelines for the Electronic Foreign Exchange Matching System (EFEMS)	FMD/DIR/CON/OGC/038/165	Financial Markets Department
16	12/10/2024	Guidelines for the Electronic Foreign Exchange Matching System (EFEMS)	FMD/DIR/CON/OGC/038/166	Financial Markets Department
17	12/11/2024	Guidelines for the Electronic Foreign Exchange Matching System (EFEMS)	FMD/DIR/CON/OGC/038/167	Financial Markets Department
18	12/12/2024	Guidelines for the Electronic Foreign Exchange Matching System (EFEMS)	FMD/DIR/CON/OGC/038/168	Financial Markets Department
19	12/13/2024	Guidelines for the Electronic Foreign Exchange Matching System (EFEMS)	FMD/DIR/CON/OGC/038/169	Financial Markets Department
20	12/14/2024	Guidelines for the Electronic Foreign Exchange Matching System (EFEMS)	FMD/DIR/CON/OGC/038/170	Financial Markets Department
21	12/15/2024	Guidelines for the Electronic Foreign Exchange Matching System (EFEMS)	FMD/DIR/CON/OGC/038/171	Financial Markets Department

mitigations.

7. Continuous Learning

Continuous learning on ethics topics and case studies is essential to stay updated with the latest standards, regulations, and best practices.

8. Mental Health and Wellbeing Programs

Creating and implementing support structures to promote mental health awareness can significantly reduce pressures and scenarios where ethical fatigue may increase.

9. Role of Assurance Functions

Assurance providers, such as Internal Audit, play a crucial role in evaluating factors related to organizational ethics and culture, including conducting culture and strategy audits. These functions should also conduct audits of emerging technologies and areas impacted by new regulations, such as those related to ESG or AI, to protect against misuse of technology or "greenwashing" by auditing key ESG metrics.

10. Enhance Data Visibility

Using data to "tell the story" can assist internal audit in identifying gaps and tracking performance metrics against key goals. This includes sharing data with relevant teams and stakeholders to ensure transparency and accountability.

Promoting Transparency in Ethical Processes

Internal audit leaders play a crucial role in ensuring that technologies are designed and deployed ethically, adding value to organizations and society, and driving profits. To behave ethically and earn trust in an evolving digital age, internal audit and organizational leaders must quickly learn and digest new information, applying their judgement to situations they may not have encountered before.

Many organizations struggle with how to respond when their leaders reject Kahneman's "system two thinking" and even truth itself. Promoting transparency in ethical processes, establishing standard practices, and ensuring appropriate oversight and stakeholder involvement are critical. Assurance functions have been a crucial step in ensuring that organizations adhere to their core processes and regulatory requirements. These functions can reveal how well or poorly organizations align with expected standards, ensuring confidence in the organization's solutions and ethical approach.

Culled from: internalaudit360.com

2024 ACAEBIN AGM & FRAUD CONFERENCE: Key Takeaways for CAEs to Ensure Efficiency and Effectiveness

❖ Enhance consequence management and ensure the application of sanctions for fraudulent behaviour within banks to maintain discipline.

CAEs should ensure that sanctions/penalties are applied in line with their bank's policy, and such reported as stipulated by CBN, especially for those acts that are inimical to the industry.

❖ Promote awareness of whistleblowing platforms and encourage employees to report suspicious activities.

Whistleblowing awareness should be encouraged and conducted at least on quarterly basis whilst assuring the confidentiality of the blowers. Used cases should be applied in driving the awareness campaign home amongst staff.

❖ Ensure adequacy of existing controls and processes within internal audit.

CAEs should ensure that controls are reviewed periodically in line with emerging risks and trends.

❖ Review audit coverage of cyber risks and digital platforms to ensure adequate monitoring of fraud risks.

❖ Evaluate the need for remote access and implement controls to restrict it to authorized personnel and applications. Review and set appropriate system idle time settings to prevent unauthorized access.

❖ CAEs in conjunction with CISOs to ensure that there is a process in place to deliver regular phishing and social engineering awareness training for all employees and implement a phishing drill program to test and reinforce employee preparedness.

Enhancing Customer Experience Through Effective ATM Reviews: A Strategic Imperative



In a world where digital banking channels are rapidly expanding, **Automated Teller Machines (ATMs)** remain a vital bridge between financial institutions and their customers. Despite the rise of mobile apps and online platforms, ATMs continue to be a primary self-service channel—especially for cash-dependent customers. However, their effectiveness directly influences how customers perceive a bank's reliability, accessibility, and service quality.

Frequent downtimes, security concerns, inaccessible locations, and poor user interfaces not only inconvenience customers but can also significantly damage a bank's reputation. That is why **effective ATM reviews** structured assessments of performance, security, accessibility, and user feedback are more than maintenance checklists; they are a strategic tool for improving **customer experience (CX)** and building long-term loyalty.

This article explores how banks can harness the power of ATM reviews to strengthen service delivery, reduce operational bottlenecks, and meet the evolving expectations of a diverse and tech-savvy customer base.

Understanding Customer Experience in ATM Services

Customer experience encompasses all interactions a customer has with a financial institution, and ATMs are often a frontline touchpoint. When customers approach an ATM, they expect quick, reliable, and secure transactions anything less can erode their trust.

Key Components of a Positive ATM Experience:

- **Availability & Accessibility:** Customers want ATMs that are operational 24/7 and conveniently located.

- **Functionality & Efficiency:** Machines must work seamlessly cash should be dispensed promptly, without errors or card issues.

- **User Interface:** The screen layout should be intuitive, with easy-to-navigate menus and multi-language support.

- **Security & Privacy:** Customers must feel safe during transactions, with secure PIN entry and protective physical surroundings.

- **Issue Resolution:** When problems occur, timely resolution (e.g., refunding failed transactions) greatly influences satisfaction.

- **Feedback Channels:** Avenues for sharing complaints, compliments, or suggestions are essential for ongoing improvement.

ATMs are no longer just cash dispensers—they represent a **brand experience**, and every malfunction or delay is a potential pain point that shapes customer perception.

The Strategic Role of ATMs in Customer Engagement

ATMs function as **customer touchpoints**—physical and digital contact moments that can reinforce or erode a customer's relationship with their bank.

1. Accessibility and Convenience

ATMs reduce reliance on bank branches, offering fast services in malls, airports, campuses, and high-traffic zones. But this convenience is compromised when machines are down, out of cash, or poorly maintained.

2. Speed and Performance

Fast, uninterrupted service is expected. Delays, failed transactions, or long queues not only frustrate users but reflect poorly on the bank's operational capabilities.

3. Security and Trust

ATM fraud including card skimming, phishing, and cyber-attacks poses real threats. Effective reviews ensure systems are updated, surveillance is functional, and fraud risks are minimized.

4. Inclusion and Personalization

Modern ATMs feature multilingual support, audio prompts, and interfaces for visually impaired users. Reviews help identify areas where inclusivity can be improved.

5. Feedback Integration

Customer complaints and usage data provide powerful insights. Integrating this feedback into ATM evaluations helps banks refine their strategies and improve service responsiveness.

ATM Trends Reshaping the Customer Experience

To meet rising expectations, banks are reimagining ATM functionality beyond simple cash withdrawals.

Key Emerging Trends:

- **Cash Recycling ATMs:** These machines accept deposits and dispense the same cash, reducing restocking needs and improving uptime.

- **Cardless Withdrawals:** Using QR codes, mobile apps, or USSD codes, customers can access funds without a physical card—boosting convenience and reducing fraud.

- **Biometric Authentication:** Fingerprint and iris scans improve security and accessibility, especially in areas with limited ID infrastructure.

- **Self-Service Kiosks:** Advanced ATMs now support bill payments, statement printing, PIN changes, and more—enhancing utility.

- **Inclusive Interfaces:** Multi-language options, voice-guided features, and touchscreens improve accessibility for all customer segments.

- **Real-Time Monitoring & Geo-Fencing:** GPS and IoT-enabled systems allow banks to track ATM status and send security alerts instantly.

- **Data-Driven Optimization:** Usage analytics help identify high-demand locations, ideal service times, and necessary design improvements.

By adopting these technologies, banks can make ATMs a core part of **digital transformation** and **customer-centric innovation**.

The Power of ATM Reviews

ATM reviews involve the structured evaluation of machines based on usage metrics, functionality, physical condition, customer feedback, and security protocols. Done well, they offer a clear window into the ATM network's health and customer impact.

Why Reviews Matter:

- **Early Detection of Issues:** Frequent malfunctions or downtime at specific locations can be identified and resolved proactively.

- **Customer-Centric Decision Making:** Reviews capture what customers are actually experiencing, not just what systems report.

- **Location Intelligence:** Feedback highlights concerns

Ten Ways to Enhance Ethical Leadership in Internal Audit Departments

majority of their decisions using System One. This suggests that internal leaders may have an innate cognitive barrier that prevents them from being as ethical as they wish to be. This barrier is often more unintentional than deliberate.

Monitoring Ethical Challenges

While there has been an increase in ethical standards and codes of conduct across all professional bodies - including the new Institute of Internal Auditor's Global Internal Audit Standards, the International Code of Ethics for Professional Accountants (IESBA), and the National Institute of Standards and Technology (NIST) Code of Ethical Conduct—there is no universally agreed-upon method to measure them. For example, how does an organization determine if a leader is acting and behaving ethically? Many organizations create and implement ethics programs to set and monitor compliance with broader enterprise goals. However, these goals can differ within the enterprise, large departments, and even within teams in the same department. Without regular assessment of basic, expected fair behaviours and a culture of leadership, unjust practices and unethical or unprofessional acts can be encouraged, causing extensive damage to the organization. As history has shown, this can lead to significant reputational damage and even the downfall of the organization.

Top 10 Ways to Enhance Ethical Practices in Internal Audit and Across the Organization

Internal audit leaders can create more value by shaping the environment in which they operate. These include:

1. Setting the "Tone from the Top"

The U.S. Sarbanes-Oxley Act of 2002 popularised the phrase "tone at the top," which means that employees take their cues from the leadership team. Promoting ethical decision-making at all levels of leadership and ensure ethical governance structures are in place is crucial for fostering a culture of integrity and accountability.

2. Creation of a "Speak up Policy"

A clearly communicated policy to assist employees in reporting instances of ethical lapses.

3. Formation of Ethics Committees & Champions

Reporting on ethical dilemmas and regularly evaluate mechanisms for reporting unethical behaviour. Ethics committees can also support ethics champions who are strategically embedded within internal audit and business lines as a resource when leaders are at risk of ethical fatigue or unintended ethical lapses. These ethics champions are also best placed to provide regular ethics training and promote ethics checklists to help internal audit leaders identify ethical threats.

4. Design Cross-Functional Teams

Developing and promoting cross-functional teams allows all key stakeholders to be involved in the ethical decision-making process. This approach ensures appropriate oversight and approvals at key stage gates, especially where ethics may be under greater scrutiny.

5. Combine Process Controls with Strategy

Build in process controls at the same time the strategy is developed to reduce the risk of unintended ethical consequences.

6. Build Knowledge of Emerging Technologies and Regulation

A sound understanding of emerging technologies and associated regulation is critical to reducing risk of compromising professional competence and due care. Business leaders, and second and third line of defence assurance providers must be able to identify, interpret, and evaluate the risks associated with emerging technologies to be able to recommend appropriate

Ethics are a crucial component of every organization and are broadly defined as the values and principles that govern and shape behaviours and leadership. According to a recent study by Gallup, only 20 percent of employees surveyed strongly agreed that they trusted the leadership of their organization. Forbes estimates that Generation "Z" will constitute 27 percent of the workforce in OECD countries and one-third of the Earth's population by the end of 2025. This generation is demanding greater ethical decisions and transparency from leaders more than any other generation before them.

The importance of ethical leadership, particularly in internal audit cannot be overstated. Organizations have moved beyond a set of simple ethics, such as: "Don't lie" and "Don't cheat," to operating in a more socially responsible and sustainable manner, both for long-term success and to promote positive change within internal audit, the industry, in our communities, and the wider world.

There have been numerous cases of ethical lapses in large organizations across the world, with some leading to regulatory changes on a global scale. While ethical considerations have always existed for internal audit leaders, they are once again under the spotlight due to the emergence of new technologies, such as Artificial Intelligence (AI) and Machine Learning (ML). Organizations are eager to adopt these technologies to their advantage, both within internal audit departments and the organization at large.

Additionally, there is a continuing focus on Environmental, Social, and Governance (ESG) factors. Investors and stakeholders are now considering non-financial factors in their decisions, alongside traditional financial metrics, to assess an organization's sustainability and ethical impact.

Changes in the Regulatory Environment

As a result of changing landscapes and emerging technologies, regulation and reporting requirements have evolved, leading to increased pressure on internal audit leaders as demand for transparency reporting has grown. In the field of ESG, there are numerous guiding principles, frameworks, rating agencies, measurement targets, and regulation, such as the Corporate Sustainability Regulation Directive (CSRD) and the European Union Deforestation Regulation (EUDR). All of these support transparency reporting and help to prevent any potential "greenwashing."



In the field of AI, The EU AI Act was officially approved by the European Parliament in March 2024, with a staggered timeframe for its full implementation. The legislation aims to regulate AI systems and establish baseline standards for high-risk AI systems. Additionally, there are other pending legislations under development across the world, including in Japan, Brazil, and Canada. Compliance with such regulation allows organizations to demonstrate to investors, employees, and customers that they are acting in the best interests of society.

Leadership Challenges in Today's Environment

Over the past 20 years, many organizations ranging from banking, aviation, and telecommunications to professional services firms, have suffered significant consequences due to ethical lapses by their leaders. These lapses can stem from various drivers, including deliberate intentions driven by personal gain, regulatory complexity, client pressures, cultural issues, conflict of interest, insufficient knowledge or training (especially in new and complex areas), and profitability, cost, or time pressures.

The rapid evolution of global regulatory compliance requirements in areas such as AI, privacy, and ESG has introduced significant complexity. This has forced internal audit leaders to make quicker decisions, often in unfamiliar and developing areas. The increased pressures and ambiguity associated with complying with these regulations cannot be understated.

Innate Human Behaviours

Daniel Kahneman, in his book "Thinking. Fast and Slow," explains how humans have two modes of decision-making. System One is our intuitive system, which is fast, automatic, effortless, and emotional. System Two is our more deliberative thinking, which is slower, conscious, effortful, and logical. Most humans make the

such as poor lighting, unsafe areas, or long queues.

- **Brand Perception Management:** Timely responses to negative feedback show attentiveness and commitment to service.

- **Compliance and Benchmarking:** Reviews help assess accessibility standards and compare ATM performance across institutions or regions.

Building a Customer-Centric ATM Strategy

To fully align ATM operations with customer expectations, banks must develop a **customer-first framework** around deployment, technology, and feedback management.

1. Know Your Customers

Understanding who uses your ATMs, and how, is key to tailoring services.

- Conduct surveys and interviews.
- Analyze transaction patterns (e.g., peak hours, common services).
- Segment customers (youth, elderly, rural, urban) and design features accordingly.

2. Enhance Availability

- Place ATMs in high-demand areas like shopping centers, schools, hospitals, and transit hubs.
- Ensure 24/7 access where safe and practical.
- Provide accessible features for people with disabilities.

3. Offer Expanded Services

Modern customers expect more than cash withdrawal. Offer:

- Bill payments
- Cheque and cash deposits
- Fund transfers
- Mobile top-ups
- Mini statements
- PIN management

4. Adopt Modern Technology

Invest in machines that:

- Offer fast, seamless transactions
- Feature touchscreens and local language support
- Support contactless transactions (NFC-enabled)
- Provide real-time transaction alerts for transparency

5. Prioritize Security

Customers must feel protected. Ensure:

- Adequate lighting and surveillance cameras
- Anti-skimming hardware
- OTPs or biometric checks for high-value transactions
- Regular security audits and software updates

6. Practice Proactive Maintenance

- Use remote monitoring tools to track errors and low cash levels.
- Deploy quick-response teams to fix issues.
- Schedule routine preventive maintenance to avoid breakdowns.

Realizing the Benefits of Effective ATM Reviews

When ATM reviews are systematically implemented, the benefits are tangible for both banks and customers.

For Customers:

- Reduced transaction failures and downtime
- Improved security and trust in banking services
- Expanded access to services and locations

For Banks:

- Lower maintenance costs through targeted interventions
- Increased customer satisfaction and retention
- Stronger brand image and competitive advantage
- Better compliance with accessibility and safety standards

ATM reviews also serve as a feedback-rich source of operational intelligence, enabling smarter decisions on ATM placement, upgrades, and feature rollouts.

Conclusion

In the digital banking era, ATMs are far more than machines they are **critical customer experience hubs**. Every interaction at an ATM shapes a customer's perception of the bank's reliability, responsiveness, and service commitment. As such, banks must treat **ATM reviews not as a back-office task, but as a strategic imperative** that influences customer loyalty and competitive positioning.

Through regular, data-driven evaluations that prioritize user feedback, security, convenience, and accessibility, banks can ensure their ATMs meet the evolving demands of modern customers. Institutions that build a **customer-centric ATM**

Onwuemele Sunday Emeke CFE
Head Office Audit
United Bank For Africa Plc



Internal Auditors and AI: The Urgent Need for a Paradigm Shift

In the rapidly evolving landscape of the financial sector, artificial intelligence (AI) is reshaping risk management and compliance to fraud detection and customer engagement. As financial institutions increasingly deploy AI-driven tools, the role of the internal auditor has undergone a radical transformation. Once seen as an oversight function, internal audit in the finance industry is now tasked with a more dynamic and strategic role. The rise of AI not only challenges traditional audit practices but also opens new avenues for auditors to add value, drive innovation, and safeguard ethical standards in increasingly complex financial systems.

From Traditional Compliance to Strategic Risk Management

Previously, internal auditors in the financial sector were primarily responsible for evaluating internal controls, ensuring compliance with regulations, and conducting periodic audits. However, AI now allows for the automation of routine processes like transaction monitoring and compliance checks, freeing auditors to focus on more strategic concerns.

- **AI-Driven Insights:** AI systems are now capable of conducting real-time audits by analysing vast datasets and identifying irregularities or emerging risks at a much faster pace than human auditors.

- **Strategic Advisors:** Internal auditors are shifting from compliance enforcers to trusted strategic advisors, providing senior management with insights on AI's impact on financial risk, regulatory compliance, and the overall control environment.

Guardians of Financial AI Ethics and Governance

As AI becomes increasingly embedded in financial decision-making processes - ranging from loan approvals to investment strategies—internal auditors are taking on the responsibility of ensuring that these systems are ethical, transparent, and accountable.

- **AI Governance:** Financial institutions must establish governance frameworks to ensure AI systems are designed and used responsibly. Internal auditors are now assessing the integrity of AI models, ensuring they align with

- **Compliance:** Effective management of exceptions positions organizations favorably with regulators and auditors.

- **Fostering Continuous Improvement:** Each exception provides an opportunity for the organization to learn, adapt, and grow stronger.



Best Practices for Managing Audit Exceptions

1. Develop Clear Action Plans
As soon as an exception is identified, responsible teams should design practical, realistic action plans with defined timelines and clear accountability.

2. Secure Leadership Commitment
Senior management should visibly support and oversee the remediation process. Their involvement sends a strong message about the importance of wift resolution.

3. Conduct Root Cause Analysis
Instead of addressing surface-level issues, a deep dive into underlying causes ensures that corrective measures are sustainable and prevent recurrence.

4. Ensure Open Communication
Keeping relevant stakeholders informed throughout the process fosters collaboration, avoids bottlenecks, and keeps momentum strong.

5. Monitor and Validate Solutions
Following implementation, independent reviews should confirm that corrective actions have been effectively completed and desired outcomes achieved.

Pitfalls to Watch Out For

- **Delays in Implementation:** Postponing corrective measures increases exposure to risk and undermines audit credibility.

- **Poor Documentation:** Without proper documentation, demonstrating compliance during follow-ups or regulatory inspections becomes challenging.

- **Quick Fixes:** Temporary solutions that do not address root causes often lead to repeat findings and eroded trust.

Conclusion

Audit exceptions should never be treated as mere paperwork. They represent crucial opportunities for organizational strengthening and innovation.

By implementing audit recommendations with discipline, urgency, and transparency, organizations not only close immediate gaps but also build resilience for the future.

It is our responsibility to treat audit exception implementation as a strategic necessity one that secures operational excellence, reinforces internal governance, and positions our institutions for lasting success.

By acting decisively today, we transform vulnerabilities into competitive strengths, paving the way for a more secure and successful tomorrow.

Olusegun S. Kehinde
Internal Audit Department
Wema Bank

Strengthening Organizational Integrity Through Proactive Audit Exception Implementation

In today's ever-evolving corporate environment, audits remain a vital tool for protecting organizational assets, promoting transparency, and ensuring adherence to regulations.

However, the real measure of an audit's success lies not just in identifying exceptions, but in the deliberate and timely implementation of corrective actions.

Audit exception implementation serves as the critical link between recognizing risks and effectively mitigating them. When approached properly, it fortifies internal controls, enhances operational efficiency, and boosts stakeholder trust.

What Are Audit Exceptions?

Audit exceptions occur when actual conditions diverge from established standards, such as policies, procedures, regulations, or industry best practices. These deviations can vary from minor lapses to significant control failures, which, if ignored, could expose theorganization to considerable risks.

Failure to address audit exceptions on time could lead to regulatory sanctions, reputational damage, financial loss, and overall operational weaknesses.

Why Effective Implementation Matters

- **Reducing Risks:** Closing identified gaps promptly lowers the organization's exposure to both internal and external risks.
- **Driving Operational Efficiency:** Corrective actions often lead to better processes, resource optimization, and improved workflows.
- **Maintaining Regulatory**



organizational values, regulatory requirements, and ethical standards.

- **Risk of Bias and Discrimination:** With AI's growing role in credit scoring, lending decisions, and investment strategies, auditors must be vigilant against the risk of algorithmic biases that could lead to discriminatory outcomes. They help ensure that data used in AI models is fair and that the models are transparent.

Pioneers of Continuous, Real-time Auditing in Finance

The advent of AI has introduced a new era of continuous auditing, where transactions and activities are monitored in real time, providing a more proactive approach to risk management.

- **Automated Auditing Systems:** AI tools enable internal auditors to continuously monitor financial transactions, detecting anomalies, fraudulent activities, and discrepancies as they occur. This is particularly important in the financial sector, where even minor errors or fraudulent activities can lead to significant losses
- **Instantaneous Reporting:** With real-time data processing, auditors can generate actionable reports instantly, allowing for quicker decision-making and timely interventions in high-risk areas.

Cybersecurity Audits in an AI-Driven Finance Ecosystem

As financial institutions adopt AI, they also face increasing cybersecurity risks. AI can help detect cyber threats, but it also presents new vulnerabilities that internal auditors must assess and mitigate.

- **AI in Cybersecurity:** Internal auditors are now evaluating how AI systems contribute to cybersecurity, ensuring that AI algorithms used in threat detection are robust and secure.
- **Digital Risk Management:** Auditors must assess AI models for vulnerabilities such as data manipulation, model adversaries, and data privacy risks, ensuring that financial institutions are protected from emerging digital threats.

Navigating Regulatory Compliance in the Age of AI

- In the finance industry, regulation is crucial. As AI continues to transform financial operations, auditors must ensure that AI implementations comply with an increasingly complex regulatory landscape
- .**Regulatory Alignment:** Internal auditors are now tasked with interpreting and applying new regulations related to AI, such as the European Union's General Data Protection Regulation (GDPR) or the upcoming AI Act. They assess whether AI systems in financial services comply with these standards.
- **Risk of Non-compliance:** With AI automating key financial processes, internal auditors must ensure that AI systems adhere to regulatory reporting standards, mitigate the risk of non-compliance, and avoid costly penalties.

Auditors as Change Agents in Financial Innovation

Internal auditors in the financial sector must not only keep pace with AI advancements but also actively promote and guide AI adoption. By becoming change agents, auditors ensure that the integration of AI contributes to long-term value creation while mitigating potential risks.

- **Skillset Evolution:** Auditors must become fluent in emerging technologies such as machine learning, blockchain, and advanced data analytics. This requires a shift from traditional audit practices to more interdisciplinary collaboration with data scientists, financial analysts, and AI developers.
- **Adopting Agile Methodologies:** The shift towards AI-driven processes demands that internal audit functions be more agile. Financial institutions are adopting agile audit methods, enabling auditors to quickly assess and adjust to new AI technologies as they are implemented.

Conclusion

AI is redefining the financial landscape, and the internal auditor's role is evolving in parallel. What was once a function focused primarily on post-event compliance and assurance is now becoming an essential part of strategic decision-making, risk management, and ethical governance. As AI reshapes financial services, internal auditors in the finance industry must embrace these disruptions, adopt new technologies, and provide the necessary oversight to ensure that AI delivers value responsibly and sustainably.

The internal auditor of the future will be not only a technologist and a risk manager but also an ethical guardian and strategic advisor. By adapting to the age of AI, auditors can ensure financial institutions remain resilient, compliant, and at the forefront of innovation.

By Segun Famoriyo
CAE, Unity Bank Plc.



Microservices Architecture: Implementations and the Internal Audit Perspective on the Security Concerns

Modern enterprise systems are rapidly transitioning from monolithic architectures (this refers to the traditional software design where all components (User interface, business logic, data access etc) are tightly integrated and run as a single application. As such, changes or scaling often require redeploying the entire system) to microservices which are flexible, scalable, and modular designs that promote faster innovation. However, this evolution introduces security complexities that must be proactively assessed. For Internal Audit, understanding these technical implementations and their associated risks is critical in ensuring effective controls and compliance with global standards such as ISO/IEC 27001:2022, ISO/IEC 27032:2023 and the NIST Cybersecurity Framework.

Microservices Implementation

In microservices architecture, applications are broken into small, independently deployable services that communicate over APIs (Application Programming Interface). These services can scale, fail and update independently thereby enabling agility but also expanding the attack surface, complicating data flows, and demanding coordinated security controls across distributed environments.

Internal Audit Security Concerns

1. Distributed Security Governance

Each microservice may implement its own access controls, logging, and security rules which may potentially lead to inconsistent enforcement.

✶ Audit Concern: Is there centralized visibility and policy enforcement across services?

✶ ISO 27001:2022 Ref: A.5.2 (Roles and Responsibilities – Information security roles and responsibilities shall be defined and allocated according to the organization needs.) and A.8.2 (Privilege Management – The allocation and use of privileged access rights shall be restricted and managed.)

✶ NIST CSF: ID.GV-1 (Governance policies and procedures - This control ensures that an organization defines, approves, and disseminates its cybersecurity policies to govern security practices effectively.)

2. Inter-Service Communication Risks

APIs between services may transmit sensitive data, often without proper encryption or authentication mechanisms.

✶ Audit Concern: Are communications between services encrypted (e.g., mTLS) and authenticated? mTLS (Mutual TLS) is a security protocol where both client and server authenticate each other using X.509 certificates, ensuring encrypted and two-way verification. It also enhances security over standard TLS by preventing unauthorized access and mitigating impersonation attacks.

✶ ISO 27032:2023 Ref: Section 6.5 (Secure Data Exchange)

✶ NIST CSF: PR.DS-2 (Data-in-transit protection - This control ensures that sensitive data transmitted over networks is encrypted to prevent unauthorized access or tampering (e.g., using TLS, VPNs, or IPSec))

3. Insecure Configuration and DevOps Pipelines

Frequent deployments and containerization (e.g., Docker, Kubernetes) can lead to misconfigurations if not tightly controlled.

✶ Audit Concern: Are secure build and deployment pipelines enforced, with approvals and

Balancing Work, Ethics and Sanity



productive at work, let these people know where you stand from the beginning. If your **partner** is your colleague, he/she must know that you will declare your relationship to the respective authorities or persons and you will not cover up anything for his/her sake.

✪ **Use Productivity Tools:** Honestly, this is not for any age group, as an auditor, you have a lot on your plate already. Using productivity tools like planners or mobile apps to schedule tasks effectively can prevent last-minute pressure and ease the load of planning.

✪ **Leverage Technology**: You may have heard this a lot but its a very important key to making your life easy. Automating routine audit tasks with data analytics tools can save time and improve efficiency.

✪ **Invest in Self-Care:** Regular exercise, proper sleep, and engaging in social activities can help manage stress levels. Please attend team bonding events and office hangouts where you'll have fun and laugh with your colleagues. There are also lots of common-interest networks that provides support system to its members.

Ultimately, the key to balancing work, ethics, and sanity lies in recognizing that as internal auditors, we are not just watchdogs but enablers of organizational success. By cultivating a balance between technical expertise and interpersonal skills, we can redefine our role and general perception from enforcers to trusted advisors, making the profession not just impactful but also personally fulfilling.

The Internal Auditor's Dilemma:

Everywhere I meet people, the conversation usually plays out this way:

The person: Hi, my name is X.

Me: Hello X, I'm Olawunmi after a little chit chat

X: So, Olawunmi, what do you do?

Me: I head the Audit function in my organization.

X: exclaims like a typical Nigerian You are the police! I'm sure people don't like you

As Internal Auditors, we are often perceived as corporate gatekeepers—meticulous, rigid, and, at times, intimidating. In financial institutions and regulatory-driven industries, our role is crucial in safeguarding compliance, identifying risks, and ensuring governance frameworks are adhered to.

However, behind the audit engagement meetings, risk assessments, and reports lies a group of professionals who are also navigating immense pressure, ethical dilemmas, and the challenge of maintaining personal well-being like everyone else in corporate Nigeria.

The Perception vs. Reality of Internal Auditors

The stereotype of Auditors as 'mean' or overly critical often stems from the nature of the job—the questioning processes, identifying control weaknesses, and ensuring adherence to policies. Yet, our function is not to 'catch' people; rather, we serve as advisors, helping our organizations mitigate risks before they become crises. This perception gap can sometimes lead to strained relationships within the workplace, making it essential for auditors to develop a 'tough skin', and strong interpersonal skills while maintaining their objectivity.

The Mental and Emotional Toll

Being an Internal Auditor means working under tight deadlines, balancing multiple engagements, and facing resistance from colleagues who may view audits as intrusive. Additionally, ethical dilemmas arise when we uncover fraud, non-compliance, or governance lapses, placing us in tough positions where integrity must take precedence over convenience. The pressure to remain independent while still fostering a collaborative work environment can lead to burnout if not managed properly.

Maintaining Work-Life Balance

If you are like me, you probably rolled your eyes at this sub-title and said “all na scam” in your mind. So, yes i get you, and I know you know the whole -time management, mental resilience mantra. However, lets talk about some things that are sometimes left unsaid:

✪ **Learn to Manage Office Politics:** You must Know your Boss; Know your Peers; Know the Power Brokers and manage the relationships accordingly. Navigating workplace dynamics is key. Building good relationships while maintaining professional integrity helps reduce resistance during audits.

✪ **Set Work Boundaries**: In our clime, Auditors are expected to be available round-the-clock, and to



participate in any and everything. Learn to strategically “pick your fight”. I believe understanding the Independence and Objectivity dimensions of Internal Auditing will help streamline your workload.

Another aspect of setting boundaries refers to managing your personal relationships within the organization. In corporate Nigeria, we spend most of our time in the office, it's almost impossible to not have “work besties”, colleagues-turned-family, or even be romantically involved with a colleague. To keep being objective, which is key to being

automated scanning?

✶ ISO 27001:2022 Ref: A.8.8 (Technical Vulnerabilities - Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.), A.8.32 (Change Management)

✶ NIST CSF: PR.IP-1 (Configuration Management - This control ensures standardized, secure configurations for hardware and software to reduce vulnerabilities and maintain consistency across systems.)

4. Inadequate Identity and Access Management (IAM)

Identity and Access Management (IAM) in microservices is often implemented using token-based systems (e.g., OAuth2), but token misuse or poor design can expose services.

✶ Audit Concern: Are tokens securely managed, short-lived, and traceable?

✶ ISO 27032:2023 Ref: Section 7.3 (Access Control Mechanisms)

✶ NIST CSF: PR.AC-1 (Access control policies - Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.)

5. Fragmented Logging and Incident Detection

✶ Logs from multiple services must be aggregated for meaningful monitoring. Without this, incident detection and response are weakened.

✶ Audit Concern: Is centralized logging (e.g., via SIEM – Security Information and Event Management) in place, with alerting on anomalies?

✶ ISO 27001:2022 Ref: A.5.25 (Logging - The organization shall assess information security events and decide if they are to be categorized as information security incidents)

✶ NIST CSF: DE.CM-1 (Security monitoring - The network is monitored to detect potential cybersecurity events. This control focuses on continuous surveillance of network traffic, devices, and communications to identify anomalies, intrusions, or malicious activity.)

6. Data Residency and Retention Risks

Data flowing across services and environments (cloud, hybrid) may violate regulatory requirements if not tracked.

✶ Audit Concern: Is data classification and retention aligned with legal/regulatory expectations?

✶ ISO 27001:2022 Ref: A.8.11 (Data Quality - Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.) and A.8.10 (Information Deletion - Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.)

✶ NIST CSF: PR.DS-5 (Protection of data-at-rest - This control ensures safeguards (e.g., DLP tools, encryption, access controls) are in place to prevent unauthorized exfiltration, exposure, or loss of sensitive data.)

Internal Audit Recommendations

1. Establish Audit Visibility Across Microservices: Use tools that allow auditors and compliance teams to observe access, transactions and configurations across all services.

2. Enforce Zero Trust Principles: Microservices should adopt Zero Trust practices by verifying every request, using strong identity controls and encrypting all communications.

3. Integrate Security into DevSecOps: Ensure that security checks are embedded into CI/CD pipelines for static code analysis, container scanning and image signing.

4. Centralize Logs and Incident Response: Use log aggregation tools and correlate across services to detect lateral movement and anomalous behavior early.

5. Map Controls to Recognized Frameworks: Internal audit should regularly benchmark controls against ISO 27001:2022, ISO 27032:2023, and the NIST CSF to ensure coverage of emerging risks.

Conclusion

The emerging trend to microservices offers significant business and technical advantages but introduces distributed security risks that require coordinated governance. Internal auditors must improve their technical mastery around microservices implementations and align their evaluations with modern cybersecurity frameworks. As such, they not only assess risk but actively contribute to a more resilient, compliant and secure enterprise.

By Fatunbi Abdulrazak Ishola, Keystone Bank Limited.



The Evolving Role of Internal Auditing in a Digitally Driven Banking Sector

Introduction: A Shift from Tradition to Transformation

The banking sector is undergoing a profound digital transformation, replacing legacy systems with smart technologies like artificial intelligence (AI), blockchain, cloud computing, and mobile platforms. This digital shift has elevated customer expectations and operational efficiency, but it has also introduced complex risks, cyber threats, and regulatory demands.

In response, internal auditing has evolved from its traditional role - focused largely on compliance and financial accuracy - into a dynamic, technology-enabled function that supports digital resilience, risk anticipation, and strategic advisory. Auditors are no longer passive observers; they are proactive guardians of integrity in the digital banking ecosystem.

Redefining Internal Audit for the Digital Age

Today's internal audit teams are expected to assess more than just financial transactions. They must evaluate mobile applications, monitor cybersecurity measures, scrutinize IT infrastructure, and audit digital transformation initiatives. This expansion reflects the banking sector's increasing reliance on digital platforms and data-driven decision-making.

Key shifts in the audit scope include:

✪ **Auditing digital banking systems** such as mobile platforms, AI-driven services, and APIs.

✪ **Reviewing data governance and privacy compliance** under regulations like GDPR and NDPR.

✪ **Assessing cybersecurity resilience**, IT change management, and disaster recovery frameworks.

✪ **Providing assurance on digital projects**, from system implementation to post-rollout effectiveness.

In short, internal auditing has become a multidisciplinary discipline combining financial scrutiny with IT governance, risk

L. Whistleblower Mechanisms and Confidential Reporting

Establishing a secure and anonymous reporting system encourages employees and customers to report fraudulent activities.

Auditors assess and act on whistleblower reports to prevent financial losses.

3. Challenges and Limitations of Internal Audits in Detecting and Preventing Fraud Collusion

Despite the robust role of internal audits, several challenges hinder their effectiveness:

a. Collusion Complexity: Fraud collusion often involves multiple layers of deception, making it difficult to uncover

b. Management Override of Controls

Senior executives or key decision-makers can manipulate financial records, override established controls, or exert undue influence on auditors, reducing audit effectiveness.

c. Limited Access to Real-Time Data

Internal auditors may face delays in accessing critical transactional data, making it challenging to detect fraud before it escalates.

d. Inadequate Use of Advanced Fraud Detection Tools

Many Nigerian banks still rely on traditional audit methods rather than leveraging artificial intelligence, machine learning, and predictive analytics to detect fraud patterns effectively.

e. Resistance from Staff and Lack of Cooperation

Employees involved in fraud collusion may resist audit inquiries, provide misleading information, or manipulate records to conceal fraudulent activities.

f. Weak Regulatory Enforcement and Legal Barriers

In some cases, regulatory loopholes and slow legal proceedings hinder the effective prosecution of fraud perpetrators, reducing the deterrent effect of internal audits.

g. Insufficient Audit Resources and Staffing

Many internal audit departments operate with limited personnel and resources, making it difficult to conduct comprehensive fraud investigations across all banking operations.

h. Evolving Fraud Schemes

Fraudsters continuously develop sophisticated schemes that exploit technological vulnerabilities and outdated audit approaches, making detection more complex.

4. Conclusion

Internal audits play a vital role in safeguarding Nigerian banks against fraud collusion by ensuring financial integrity, regulatory compliance, and operational stability. As the three lines of defence, auditors identify control weaknesses, monitor for irregularities, and assess risk exposures that could enable fraudulent activities.

By promoting accountability and transparency, internal audits help embed ethical practices within banking operations. The use of tools such as data analytics, forensic techniques, and whistleblower systems further enhances fraud detection and prevention.

To maximize impact, internal audit functions must remain independent, adequately resourced, and backed by strong regulatory oversight. A proactive and empowered audit system is essential to maintaining public trust and protecting the long-term health of Nigeria's financial sector.

References

Adetoso, A., & Akinselure, O. (2021). Fraud Control and Fraud Prevention in Nigeria Banking Industry. International Journal of Research in Finance and Marketing (IJRFM) Vol. 6 Issue 12, Pp. 66 ~ 83 http://Euroasiapub.Org/Current. Php?Title=Ijrfm Aham Nzenwata,

Akinyomi, O. (2021). Examination of Fraud in the Nigerian Banking Sector and its Prevention. Asian Journal of Management Research, 3(1), 184-192. Carnegie Mellon University. (2016). Internal Audit

Types. https://Www.Cmu.Edu/Finance/Audit-Services/Internal/Types-OfAudits.Html

Chomwa, S. (2017). Internal Audit: The Types of Internal Audits. https://Medium.Com/@Cshikati/Internal-Audit-The-Types-Of-InternalAudits- 5eaf6ca43981

Tauseef, A. (2023). Emerging Risk Trends in the Banking Sector and how Internal Audit Needs to Respond.Http://www.Internalauditor.Me/Article/EmergingRisk-Trends-In The-Banking-Sector-And-How-Internal-Audit-Needs-ToRespond-2/

Onwuemele Sunday Emeke CFE
Head Office Audit
United Bank For Africa Plc



unauthorized loans, or manipulate transaction records.

✪ **Employee-Vendor Collusion:** Employees may collude with vendors to approve inflated invoices or pay for services not rendered.

✪ **Internal Employee Collusion:** Multiple employees may collaborate to override system controls, steal funds, or manipulate financial statements.

2. Best Practices and Strategies for Effective Fraud Collusion Detection and Prevention by Internal Auditors

Fraud collusion is one of the most challenging forms of fraud to detect, as it involves multiple parties conspiring to manipulate systems and controls. Internal auditors play a critical role in identifying and preventing collusive fraud. Below are 10 best practices and strategies they can employ:

a. Develop a Strong Anti-Fraud Culture

Promote ethical behaviour and a zero-tolerance policy for fraud.

b. Conduct Fraud Risk Assessments Regularly

Identify high-risk areas and transactions prone to collusion.
Use data analytics to assess fraud risks in procurement, payroll, and financial reporting.

c. **Strengthen Internal Controls**

Implement segregation of duties to prevent unauthorized access and control over financial processes.

Enforce dual approvals for critical transactions such as vendor payments and contract awards.

d. Leverage Data Analytics and Continuous Monitoring

Use advanced forensic tools to detect anomalies in transactions.
Implement real-time monitoring systems to flag unusual patterns or relationships.

e. Enhance Employee Background Checks and Training

Conduct thorough due diligence on employees, vendors, and business partners.
Provide regular fraud awareness training to employees and management.

f. Encourage Rotation of Duties and Mandatory Leave

Regularly rotate employees in high-risk functions to reduce the risk of long-term collusion.
Enforce mandatory leave policies to enable audits without employee interference.

g. Improve Vendor and Third-Party Due Diligence

Vet vendors and suppliers through Know Your Supplier (KYS) processes.
Monitor vendor transactions for signs of inflated invoices or shell companies.

h. Conduct Surprise Audits and Forensic Reviews

Perform unannounced audits to deter fraud and uncover suspicious activities.
Engage forensic experts when collusion is suspected.

I. Strengthen Reporting and Investigative Mechanisms

Establish confidential reporting channels for employees and external stakeholders.
Implement a robust investigation framework for suspected fraud cases.

j. Collaborate with Regulatory Authorities and Industry Peers

Share fraud trends and intelligence with relevant financial crime agencies.
Participate in industry anti-fraud initiatives to stay ahead of emerging fraud schemes.

k. Ethical Training and Awareness Programs

Internal audit teams educate employees on fraud risks, ethical banking practices

analytics, and business advisory.

Empowering Auditors Through Technology

The tools used by internal auditors have also transformed. Technology has expanded auditors' capabilities, allowing for more comprehensive, continuous, and real-time oversight.

1. Advanced Data Analytics

Data analytics enables auditors to analyse vast datasets quickly, identifying anomalies and control breakdowns that might otherwise go unnoticed. Predictive modelling and trend analysis help in proactively identifying risks.

2. Artificial Intelligence (AI) and Machine Learning (ML)

AI and ML enhance audit accuracy by learning from historical data and continuously adapting to new patterns. These tools can automate anomaly detection, fraud prediction, and even risk classification in real time.

3. Robotic Process Automation (RPA)

RPA automates routine audit tasks - such as data collection, document comparison, and reconciliation - allowing auditors to focus on strategic risk areas. It improves efficiency and reduces human error.

4. Audit Visualization Tools

Platforms like Power BI and Tableau allow internal auditors to visualize patterns, risk concentrations, and audit results in real time. These tools improve board-level reporting and decision-making.

5. Cloud-Based Audit Systems
Remote access, real-time collaboration, and centralized data management are all made possible through cloud-based audit tools. In the post-COVID era, remote auditing has become standard practice.

6. Cyber Forensics and Digital Assurance

Forensic tools help trace digital footprints, recover deleted files, and audit system logs. This capability is essential for investigating cyber incidents, insider threats, and digital fraud.

Upskilling the Auditor: A New Competency Framework

To remain effective in a digitally transformed banking sector, internal auditors must expand their skill sets. Today's auditors are expected to be conversant in:

✪ **Cybersecurity and IT governance frameworks** (e.g., COBIT, ISO 27001)

✪ **Regulatory compliance**, especially regarding data privacy and digital services

✪ **Digital banking products and automation systems**

✪ **Data analytics and AI application in audit**

✪ **Risk-based and agile auditing methodologies**

Banks are responding by:

✪ **Recruiting hybrid talent** (auditors with IT and data science expertise)

✪ **Investing in upskilling programs**

✪ **Promoting cross-functional collaboration** between audit, IT, compliance, and data teams

This shift from a control-checking role to a strategic advisory function marks a significant evolution in the internal audit profession.

Digital Transformation in Banking: Opportunities and Risks

Digital transformation has fundamentally altered how banks operate. This transformation, while offering operational efficiencies and improved customer experience, also presents a new set of audit priorities.

Enhanced Customer Experience

✪ **24/7 access** to banking via mobile apps and web platforms

✪ **Personalized services** using behavioural data and analytics

✪ **Automated self-service** tools like chatbots and robo-advisors

Audit Focus: Validating the reliability, security, and data privacy of these digital interfaces.

Operational Efficiency and Cost Reduction

✪ **Automation of routine tasks** such as loan processing and reporting

✪ **Paperless workflows** and digital document management

Audit Focus: Reviewing automation controls, system outputs, and audit trails for accuracy.

Financial Inclusion

✪ **Mobile banking in underserved areas**

✪ **FinTech partnerships and agency banking**

Audit Focus: Ensuring secure, compliant service delivery in extended customer networks.

Cybersecurity and Digital Risk

✪ **Growing threats** like data

breaches, phishing, and ransomware

✪ **Increased reliance on third-party vendors**

Audit Focus: Cybersecurity auditing, penetration testing oversight, and third-party risk management.

Competition from Digital-Only Banks

✪ **Neobanks and blockchain-based services** challenge traditional banking models

Audit Focus: Reviewing emerging business models and validating new digital controls.

Enhancing Internal Audit Effectiveness in a Digital World

Modern audit functions must be agile, integrated, and responsive to new digital realities. Key strategic actions include:

a. Building Digital Competencies

✪ Upskill internal teams in cybersecurity, data analytics, and IT auditing.

✪ Recruit new talent with tech-audit hybrid backgrounds.

b. Integrating Technology into Audit Processes

✪ Use audit management systems to plan, execute, and report seamlessly.

✪ Adopt continuous auditing platforms that monitor operations in real time.

c. Risk-Based and Agile Auditing

✪ Prioritize audits based on dynamic risk scoring.

✪ Use agile sprints to assess fast-evolving systems and innovations.

d. Collaboration Across Functions

✪ Coordinate with IT, cybersecurity, data governance, and compliance units.

✪ Regularly engage senior management and boards on digital risk oversight.

IT-Audit Integration: The Future of Control Assurance

Integrating IT with internal audit functions is now critical for effective assurance in a digital banking environment. This integration includes both evaluating IT systems and using IT tools to enhance audit quality.

Key Integration Components

i. Audit Planning and Risk Tools

✪ Predictive modelling to identify high-risk areas

✪ Automated risk scoring systems for resource allocation

ii. Computer-Assisted Audit Techniques (CAATs)

✪ Full-population data analysis

✪ Transaction testing using tools like ACL Analytics, IDEA, and Teammate

iii. Automated Workflow Tools

✪ Structured electronic working papers

✪ Standardized audit templates and checklist automation

iv. Dashboards and Data Visualization

✪ Real-time summaries for board and management use

✪ Heat maps and trend visuals for clearer communication

v. Continuous Monitoring

✪ 24/7 audit tools flagging anomalies as they occur

✪ Threshold-based alert systems for quick intervention

vi. Cybersecurity Audits

✪ Review of IT general controls (e.g., access, change management, backups)

✪ Application control testing for critical banking platforms

✪ Evaluation of digital resilience and incident response readiness

Conclusion: Toward a Strategic and Digital-First Internal Audit

The future of internal auditing in banking lies in proactive assurance, strategic insight, and digital fluency. As digital transformation continues to reshape the sector, internal audit functions must rise to meet these new expectations—not just to remain relevant but to lead.

Auditors must become innovation enablers, not blockers. They must assess risk in real time, communicate with clarity, and deliver assurance across digital frontiers. The internal audit function must evolve into a **tech-savvy, risk-intelligent, and future-ready partner** in organizational governance.

As financial institutions look toward the future, those who empower their auditors with the right tools, skills, and strategies will not only navigate digital disruption successfully but emerge stronger, more trusted, and more resilient.

Emuebie Emeke, Head, Branch & Services Audit, Internal Audit Department, Union Bank



The Role of Internal Audit in Detecting and Preventing Fraud Collusion in Nigerian Banks

The Nigerian banking sector is vital to the nation's economic growth and stability, making it a frequent target for financial fraud and collusion. These fraudulent schemes often involve collaboration between internal and external actors seeking to exploit system weaknesses. Collusion—where employees, management, or third parties conspire to manipulate records, misappropriate funds, or bypass controls—poses a particularly serious threat, leading to financial losses, reputational harm, and diminished public trust.

Internal audits play a critical role in detecting and preventing such activities. By assessing the effectiveness of internal controls, identifying system vulnerabilities, and ensuring regulatory compliance, auditors serve as a key line of defence. Techniques such as risk assessments, transaction reviews, and forensic audits help uncover red flags and deter fraud. Furthermore, internal audit functions contribute to prevention efforts by recommending stronger controls, improving governance frameworks, and promoting a culture of accountability.

This article explores how internal audits help detect and prevent fraud collusion in Nigerian banks. It highlights audit methods, common challenges, and best practices for strengthening fraud risk management and enhancing institutional integrity.

Some Forms of Fraud Collusion in Nigerian Banks

✪ **Employee-Customer Collusion:** Bank employees may work with customers to create fraudulent accounts, process

Images of the 1st Stream of Training for Intermediate Information System and Technology Auditors and Middle Level Managers held between 13th and 14th of May,2025 on 'Review of Networks, Databases, I.T. Infrastructures, API Integration and Third-Party Controls, and Cybersecurity Assessment.'



Happy Birthday



The EXCO and entire members rejoice with you on the occasion of your birthdays, wishing you all the best in life.

Signed:
Management

Images of the 2024 Annual General Meeting and Fraud Conference of ACAEBIN

held on March 12th and 13th,2025 at Marriott Hotel, Lagos with the theme: Fraud and Governance: Strengthening Institutional Frameworks in Nigeria

