(ACAEBIN) Q1, 2025 A Quarterly Publication of the Association of Chief Audit Executive of Banks in Nigeria



Eagle Eye

Audit Professional Skepticism in the Age of Technology





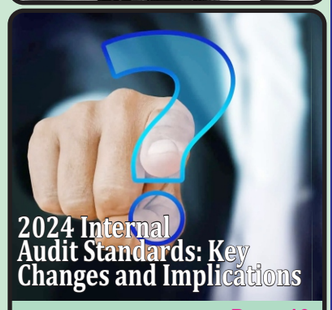
Page 30

Wellness

Urologists list reasons men with heart disease suffer erectile dysfunction



Page 29



Page 10

Soft Skills for Auditors: The Key to Effective Communication and Collaboration



Page 7

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

Design+print
Prowess
08039221516

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

CONTENT

4 Audit Professional Skepticism in the Age ...
7 Soft Skills for Auditors: The Key to Effective ...
10 2024 Internal Audit Standards: Key ...
12 Disrupt or Be Disrupted: How Internal Audit ...
15 Understanding Root Cause Analysis in Dealing ...
20 Leveraging Automation to Improve the Efficiency ...
25 Results-Driven Audit Follow-up: Strategies for ...
30 Cybersecurity Threat in The Financial Sector: ...

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)

www.acaebin.org facebook.com/acaebin



Editorial

As we enter the first quarter of 2025, the internal audit profession continues to evolve, shaped by rapid technological advancements, shifting regulatory landscapes, and the growing demand for agility. This edition of Eagle Eye Magazine provides valuable insights to help auditors stay relevant, resilient, and results-driven in this dynamic environment.

Our cover article, "Audit Professional Skepticism in the Age of Technology," explores the delicate balance between leveraging digital tools and maintaining the critical, questioning mindset essential for audit integrity. Additionally, "Soft Skills for Auditors" highlights the crucial role of collaboration in driving success.

The recent 2024 Internal Audit Standards introduce significant changes—our in-depth analysis breaks down their implications for practitioners. In an era of constant disruption, "Disrupt or Be Disrupted" challenges internal auditors to embrace transformation proactively. Complementing this, "Leveraging Automation to Improve Efficiency" examines how automation is reshaping banking audits.

To address critical audit challenges, we explore "Understanding Root Cause Analysis" and share "Results-Driven Audit Follow-Up" strategies for lasting impact. Given the ever-growing cybersecurity risks, "The Role of Internal Audit in Protecting the Financial Sector" underscores how auditors can strengthen financial institutions' defenses.

Beyond audit, we take a crucial look at health matters, featuring insights from urologists on why "Men with Heart Disease Suffer Erectile Dysfunction."

Finally, our "Compilation of CBN Circulars" keeps you informed on the latest regulatory directives.

As the profession adapts to a digital future, staying informed and proactive is more important than ever. We hope this edition equips you with the knowledge and strategies to thrive.

The future doesn't wait for your strategy to catch up-it rewards those who embrace adaptability and innovation.

Happy reading!

Olusegun Famoriyo
Editor-in-Chief

Audit Professional Skepticism in the Age of Technology



The increasing use of technology in auditing has transformed the audit landscape, presenting both opportunities and challenges for audit professionals (International Auditing and Assurance Standards Board [IAASB], 2018). One of the key challenges is the potential erosion of professional skepticism, a critical component of audit quality (Nelson, 2017). Professional skepticism is defined as "an attitude that includes a questioning mind and a critical assessment of audit evidence" (IAASB, 2018, para. 13). As noted by the American Institute of Certified Public Accountants (AICPA) (2019), "professional skepticism is essential for auditors to critically evaluate evidence and make informed decisions" (p. 2).

The use of technology in auditing, such as data analytics and artificial intelligence, can provide numerous benefits, including increased efficiency and accuracy (PricewaterhouseCoopers [PwC], 2020). However, it also presents challenges for audit professionals, including the potential for over-reliance on technology and lack of understanding of the underlying algorithms and models (Ernst & Young [EY], 2020). As noted by Deloitte (2020), "the increasing use of technology in auditing requires auditors to be vigilant in maintaining their professional skepticism" (p. 3).

This paper will explore the concept of audit professional skepticism in the age of technology, including the challenges and opportunities presented by technological advancements. We will examine the impact of technology on professional skepticism, and discuss strategies for maintaining and enhancing professional skepticism in the age of technology.

Defining Professional Skepticism

Professional skepticism is a critical component of audit quality, enabling auditors to critically evaluate evidence and make informed decisions (Nelson, 2017). Professional skepticism is defined as "an attitude that includes a questioning mind and a critical assessment of audit evidence" (IAASB, 2018, para. 13). It involves being alert to potential misstatements and inconsistencies in financial statements and being willing to challenge management's assertions (American Institute of Certified Public Accountants [AICPA], 2019). Professional skepticism is characterized by several key attributes, including:

Questioning mind: A willingness to question assumptions and evidence (IAASB, 2018).

Critical assessment of evidence: A critical evaluation of evidence to determine its reliability and relevance (AICPA, 2019).

Willingness to challenge assumptions: A willingness to challenge assumptions and conventional wisdom (Nelson, 2017).

Objectivity: A commitment to objectivity and impartiality in evaluating evidence and making decisions (IAASB, 2018).

The Impact of Technology on Professional Skepticism

The increasing use of technology in auditing has transformed the audit landscape, presenting both opportunities and challenges for auditors (International Auditing and Assurance Standards Board [IAASB], 2018). One of the key challenges is the potential impact of technology on professional skepticism, a critical component of audit quality (Nelson, 2017). These challenges include:

1. **Over-reliance on technology:** The increasing use of technology in auditing can lead to an over-reliance on technology, which can erode professional skepticism (Nelson, 2017).

2. **Lack of understanding of technology:** Auditors may not fully understand the technology being used, which can lead to a lack of skepticism about the results (IAASB, 2018).

3. **Increased complexity:** The increasing complexity of financial transactions and systems can make it more difficult for auditors to exercise professional skepticism (AICPA, 2019).

The Benefits of Technology on Professional Skepticism

Technology can enhance professional skepticism in several ways, amongst which are:

1. **Improved data analysis**: Technology can provide auditors with more detailed and accurate data analysis, enabling them to identify potential misstatements and inconsistencies in financial statements (PricewaterhouseCoopers [PwC], 2020).

2. **Increased efficiency:** Technology can automate routine audit tasks, freeing up auditors to focus on higher-risk areas and providing greater insights to stakeholders (Ernst & Young [EY], 2020).

3. **Enhanced audit quality:** Technology can provide auditors with more detailed and accurate information, enabling them to make more informed decisions and provide higher-quality audit services (Deloitte, 2020).

Strategies for Maintaining and Enhancing Professional Skepticism in the Age of Technology

Maintaining and enhancing professional skepticism is crucial in the age of technology, where auditors are increasingly reliant on technology to perform audits (International Auditing and Assurance Standards Board [IAASB], 2018). Here are some strategies for maintaining and enhancing professional skepticism in the age of technology:

1. **Maintain a questioning mindset**: Auditors should maintain a questioning mindset and critically evaluate the results of technology-based audit procedures (IAASB, 2018).

2. **Understand the technology being used**: Auditors should have a good understanding of the technology being used, including



its limitations and potential biases (American Institute of Certified Public Accountants [AICPA], 2019).

3. **Use technology to enhance skepticism:** Auditors can use technology to enhance their skepticism, such as using data analytics to identify potential misstatements and inconsistencies in financial statements (PricewaterhouseCoopers [PwC], 2020).

4. **Perform manual procedures:** Auditors should perform manual procedures to verify the accuracy of technology-based audit procedures (Ernst & Young [EY], 2020).

5. **Consider alternative explanations:** Auditors should consider alternative explanations for the results of technology-based audit procedures (Deloitte, 2020).

6. **Document skepticism:** Auditors should document their skepticism, and the procedures performed to address it (IAASB, 2018).

7. **Continuing professional education:** Auditors should participate in continuing professional education to stay up-to-date with the latest technologies and auditing standards (AICPA, 2019).

8. Collaboration with other professionals: Auditors should collaborate with other professionals, such as IT specialists and data analysts, to gain a deeper understanding of the technology being used (PwC, 2020).

Conclusion

In the age of technology, audit professionals face numerous challenges in maintaining professional skepticism. The increasing reliance on technology and data analytics can lead to a false sense of security, causing auditors to overlook critical risks and anomalies. However, it is essential for auditors to remain vigilant and skeptical, even in the face of advanced technology.

To maintain professional skepticism, auditors must stay up-to-date with the latest technological advancements and their potential impact on audit procedures. They must also be aware of the limitations of technology and the potential for biases and errors.

Professional skepticism is a critical component of audit quality, and auditors must prioritize its development and maintenance in the age of technology. By doing so, auditors can provide stakeholders with confidence in the accuracy and reliability of financial statements, even in an increasingly complex and technologically driven environment.

References

American Institute of Certified Public Accountants. (2019). Professional skepticism. AICPA.

Deloitte. (2020). Audit quality and professional skepticism. Deloitte.

Ernst & Young. (2020). Artificial intelligence and audit quality. EY.

International Auditing and Assurance Standards Board. (2018). ISA 200, Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with International Standards on Auditing. IAASB.

Nelson, M. W. (2017). Professional skepticism: A review of the literature. Journal of Accounting Literature, 38, 1-15.

PricewaterhouseCoopers. (2020). Data analytics and audit quality. PwC.

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

Soft Skills for Auditors: The Key to Effective Communication and Collaboration



The auditing profession has undergone significant changes in recent years, driven by advances in technology, increasing complexity of business operations, and evolving stakeholder expectations (Arens, Elder, & Beasley, 2016). As a result, auditors are required to possess a unique blend of technical skills, knowledge, and soft skills to effectively perform their duties (Institute of Internal Auditors, 2014). Soft skills, in particular, have become essential for auditors to communicate complex technical information, build relationships, and manage conflicts (Lau & Lee, 2018).

Communication and interpersonal skills are critical soft skills for auditors, as they enable effective interaction with clients, stakeholders, and audit team members (Cohen & Trompeter, 2015). Auditors with strong communication and interpersonal skills can build trust, convey complex technical information, and manage conflicts, ultimately leading to more effective audits and better outcomes for stakeholders (Goleman, 1995).

However, research suggests that auditors often struggle to develop and apply these critical soft skills, leading to ineffective communication, poor relationships, and decreased audit quality (Lau & Lee, 2018). Therefore, it is essential for auditors to prioritize the development of soft skills, particularly communication and interpersonal skills, to remain effective and relevant in today's complex and ever-changing



business environment.

Why Soft Skills Matter in Auditing

Soft skills are non-technical skills that enable individuals to effectively interact with others, communicate ideas, and build relationships. In auditing, soft skills are critical for:

Effective Communication: Auditors must be able to communicate complex technical information to non-technical stakeholders, including clients, management, and audit committees (Cohen & Trompeter, 2015). Research has shown that auditors with strong communication skills are more effective in conveying audit findings and recommendations (Lau & Lee, 2018).

Building Relationships: Auditors must build trust and rapport with clients, stakeholders, and audit team members to ensure effective audit outcomes (Goleman, 1995). A study by the Institute of Internal Auditors found that auditors with strong interpersonal skills are more effective in building relationships and achieving audit objectives (Institute of Internal Auditors, 2014).

Managing Conflicts: Auditors must be able to manage conflicts and negotiate with clients to achieve audit objectives (Arens, Elder, & Beasley, 2016). Research has shown that auditors with strong conflict resolution skills are more effective in managing conflicts and achieving audit objectives (Lau & Lee, 2018).

Teamwork and Collaboration: Auditors must be able to work effectively with audit team members, including auditors, consultants, and other stakeholders (Cohen & Trompeter, 2015). A study by the American Institute of Certified Public Accountants found that auditors with strong teamwork and collaboration skills are more effective in achieving audit objectives (American Institute of Certified Public Accountants, 2017).

The Impact of Soft Skills on Audit Outcomes

Soft skills, such as communication, teamwork, and problem-solving, are essential for auditors to effectively perform their duties and achieve successful audit outcomes (Institute of Internal Auditors [IIA], 2019). Research has shown that soft skills have a significant impact on audit outcomes, including audit quality, audit efficiency, and stakeholder satisfaction (American Institute of Certified Public Accountants [AICPA], 2020).

The Impact of Soft Skills on Audit Quality

Research has shown that soft skills have a positive impact on audit quality (PricewaterhouseCoopers [PwC], 2019). Auditors with strong soft skills are better able to identify and assess risks, and to develop effective audit strategies (Ernst & Young [EY], 2020). Additionally, soft skills are essential for auditors to effectively communicate audit findings and recommendations to stakeholders (Deloitte, 2020).

The Impact of Soft Skills on Audit Efficiency

Soft skills also have a positive impact on audit efficiency (KPMG, 2020). Auditors with strong soft skills are better able to manage their time and prioritize tasks and are more effective in their use of technology and other resources (PwC, 2019).

The Impact of Soft Skills on Stakeholder Satisfaction

Finally, soft skills have a positive impact on stakeholder satisfaction (AICPA, 2020). Auditors with strong soft skills are better able to build trust and credibility with stakeholders, and are more effective in communicating audit findings and recommendations (EY, 2020).

Key Soft Skills for Auditors

Some of the key soft skills required for auditors include:
Communication Skills: Verbal and written communication skills are essential for auditors to convey complex technical information to non-technical stakeholders.

Interpersonal Skills: Auditors must be able to build relationships, manage conflicts, and negotiate with clients to achieve audit objectives.

Emotional Intelligence: Auditors must be able to understand and manage their own emotions, as well as those of others, to ensure effective audit outcomes.

Time Management and Organization: Auditors must be able to manage their time effectively and prioritize tasks to meet audit deadlines.

Adaptability and Flexibility: Auditors must be able to adapt to changing circumstances, including changes in client needs, audit scope, and deadlines.

Benefits of Soft Skills in Auditing

The benefits of soft skills in auditing include:

Improved Communication: Soft skills enable auditors to communicate complex technical information more effectively, reducing the risk of miscommunication and errors.

Better Relationships: Soft skills enable auditors to build trust and rapport with clients, stakeholders, and audit team members, leading to more effective audit outcomes.
Increased Efficiency: Soft skills enable auditors to manage their time more effectively, prioritize tasks, and meet audit deadlines.

Enhanced Career Opportunities: Auditors with strong soft skills are more likely to advance in their careers and take on leadership roles.

Conclusion

Developing soft skills, particularly communication and interpersonal skills, is essential for auditors to perform their duties effectively. As the auditing profession continues to evolve, auditors must possess strong soft skills to communicate complex technical information, build relationships, and manage conflicts. By developing these critical soft skills, auditors can improve audit outcomes, build trust with clients and stakeholders, and achieve their career goals.

Furthermore, the importance of soft skills in auditing cannot be overstated. As noted by the Institute of Internal Auditors, "soft skills are essential for internal auditors to effectively communicate, build relationships, and manage conflicts" (Institute of Internal Auditors, 2014). Similarly, the American Institute of Certified Public Accountants emphasizes the importance of soft skills in auditing, noting that "communication and interpersonal skills are critical for auditors to effectively perform their duties" (American Institute of Certified Public Accountants, 2017).

In conclusion, developing soft skills, particularly communication and interpersonal skills, is critical for auditors to succeed in their roles. By prioritizing the development of these essential soft skills, auditors can enhance their performance, build stronger relationships, and drive greater value for their organizations.

References

American Institute of Certified Public Accountants. (2017). 2017 CPA Firm Top Issues Survey. American Institute of Certified Public Accountants.

Arens, A. A., Elder, R. J., & Beasley, M. S. (2016). Auditing and assurance services. Pearson.

Cohen, J. R., & Trompeter, G. L. (2015). Developing communication skills for auditors. Auditing: A Journal of Practice & Theory, 34(2), 147-164.

Deloitte. (2020). The importance of soft skills in auditing. Deloitte.

Ernst & Young. (2020). The role of soft skills in audit quality. EY.

Goleman, D. (1995). Emotional intelligence: Why it can matter more than IQ. Bantam Books.

KPMG. (2020). The impact of soft skills on audit efficiency. KPMG.

Institute of Internal Auditors. (2014). Soft skills for auditors. Institute of Internal Auditors.

Institute of Internal Auditors. (2019). Soft skills for internal auditors. IIA.

Lau, S. M., & Lee, K. M. (2018). The importance of soft skills in auditing. Journal of Auditing and Ethics, 2(1), 1-12.

PricewaterhouseCoopers. (2019). The importance of soft skills in auditing. PwC.

Emuebie Emeke, Head, Branch & Services Audit, Union Bank Plc.



2024 Internal Audit Standards: Key Changes and Implications



The Institute of Internal Auditors (IIA) introduced the Global Internal Audit Standards in January 2024, marking a significant update to the framework guiding internal audit practices worldwide. The standards, effective from January 9, 2025, aim to enhance the quality and effectiveness of internal auditing across various sectors. By promoting a principles-based approach for increased flexibility. Major areas of emphasis include governance, risk management, assurance, and advisory services, underscoring the internal auditor's contribution to value creation. The updates also tackle emerging risks and digital transformation, preparing auditors to address contemporary challenges.

Key Changes in the 2024 Standards

1. Emphasis on Value Creation: Internal audit is now expected to contribute to the creation of value for organizations, beyond just traditional assurance and compliance activities.

2. Alignment with Organizational Strategy: Internal audit must align its activities with the strategic objectives of the organization to provide deeper insights focused on value and ensure efficient risk management. This alignment allows internal audits to actively detect new risks, evaluate operational efficiencies and facilitate informed decision-making. By having a thorough grasp of the organization's objectives, challenges, and industry developments, Internal audit can provide suggestions that improve business performance and ensure adherence to regulatory compliance.

3. Integration of Technology and Data Analytics in Internal Auditing: The standards acknowledge the growing significance of technology and data analytics in the internal auditing process. By utilizing data analytics and business intelligence, internal auditors assist organizations in fostering growth and enhancing policy and decision-making to sustain a competitive advantage in an increasingly complex business environment.

4. Risk-Based Auditing: The standards reinforce the importance of risk-based auditing in identifying and prioritizing risks that can impact organizational goals. This method guarantees the effective allocation of audit resources (manpower, time allocation) while concentrating on areas with critical risk exposure. By aligning audit activities with the organization's risk profile, risk-based auditing improves the ability to identify vulnerabilities, maintain internal controls, and enhance overall governance. Additionally, it facilitates proactive risk mitigation, ensures compliance with regulatory requirements, and supports strategic decision-making.

Implications for Internal Auditors

1. Enhanced Skillsets and Professional Development: Internal auditors must develop a broader set of skills, including a deeper understanding of business strategy, risk management, and technological tools. Expertise in cybersecurity and digital transformation methodologies is essential for enhancing audit efficiency and aligning with organizational objectives. These competencies will empower internal auditors to provide more strategic insights and drive value in their assessments.

2. Broader Role in Risk Management and Governance: Internal auditors are expected to take a more integrated role in risk management and governance processes.

3. Increased Focus on Stakeholder Communication: Internal auditors must improve their communication skills to engage with key stakeholders effectively. The ability to communicate audit findings, transform complex data into actionable insights, and provide strategic recommendations that influence decisions. Strong communication skills are vital for collaborating with executive leadership, board members, and operational teams.

Implementation and Compliance

Internal audit functions are required to conform to the new standards by January 9, 2025. Organizations are encouraged to conduct gap assessments to identify areas that require alignment with the updated standards.

Challenges and Opportunities

Although the 2024 updates offer various advantages, they also bring forth multiple challenges for internal auditors, such as the necessity of constant adaptation to emerging technologies and changing risks. Nonetheless, the standards also create chances for internal auditors to enhance their impact within organizations and assume a more pivotal role in fostering business success.

References

1. Institute of Internal Auditors (IIA). (2024). International Standards for the Professional Practice of Internal Auditing (Standards).

Juliet Ekekwe
(Information Systems Audit, ProvidusBank Ltd)





Disrupt or Be Disrupted: How Internal Audit Can Thrive in a Digital Age

The digital age has brought about significant changes in the way businesses operate, and internal audit functions are no exception (Institute of Internal Auditors [IIA], 2020). As noted by the IIA, "the digital age has created new risks and opportunities for organizations, and internal audit must adapt to these changes to remain relevant" (p. 2). The increasing use of technology, data analytics, and artificial intelligence has transformed the business landscape, and internal audit must evolve to keep pace (PricewaterhouseCoopers [PwC], 2020).

The concept of "disrupt or be disrupted" is particularly relevant for internal audit functions, as they must adapt to the changing business landscape and leverage technology to stay relevant (Deloitte, 2020). As noted by Deloitte, "internal audit functions must be willing to disrupt traditional audit processes and leverage technology to improve audit efficiency and effectiveness" (p. 4). This requires a mindset shift from traditional audit approaches to a more agile and adaptive approach that leverages technology to provide greater insights to stakeholders (Ernst & Young [EY], 2020).

This paper will explore how internal audit can thrive in a digital age by embracing disruption and leveraging technology to improve audit processes. We will examine the impact of digitalization on internal audit, the role of technology in internal audit, and the skills and competencies required for internal auditors to succeed in a digital age.

The Impact of Digitalization on Internal Audit

Digitalization has had a profound impact on internal audit, with the use of technology becoming increasingly prevalent in audit processes (PricewaterhouseCoopers [PwC], 2020). As noted by PwC, "technology is transforming the way internal audit works, from data analytics to audit automation" (p. 3). However, digitalization also presents challenges for internal audit, including the need to stay up-to-date with emerging technologies and to address the risks associated with digitalization (KPMG, 2020).

How Internal Audit Can Thrive in a Digital Age

The digital age has brought about significant changes in the way businesses operate, and internal audit functions are no exception. To remain relevant and effective, internal audit functions must adapt to the changing landscape and leverage technology to enhance their audit processes (Institute of Internal Auditors [IIA], 2020).

To thrive in a digital age, internal audit functions must be willing to disrupt traditional audit processes and leverage technology to improve audit efficiency and effectiveness (Deloitte, 2020). As noted by Deloitte, "internal audit functions must be agile and adaptable, and willing to challenge traditional ways of working" (p. 4). This can involve embracing emerging technologies such as artificial intelligence, blockchain, and the Internet of Things (IoT) to improve audit processes and provide greater insights to stakeholders (Ernst & Young [EY], 2020).

Leveraging Technology to Improve Audit Processes

Technology can be leveraged in a number of ways to improve audit processes, including:

1. **Data analytics**: Data analytics can be used to analyze large datasets and identify trends and anomalies that may indicate control weaknesses or irregularities (PwC, 2020).

2. **Audit automation**: Audit automation can be used to automate routine audit tasks, freeing up audit resources to focus on higher-risk areas and providing greater insights to stakeholders (KPMG, 2020).

3. **Artificial intelligence**: Artificial intelligence can be used to analyze data and identify patterns that may indicate control weaknesses or irregularities (EY, 2020).

Benefits of Technology-Enabled Internal Audit

The use of technology in internal audit functions can bring numerous benefits, including improved efficiency and productivity (KPMG, 2020), enhanced risk assessment and identification (Ernst & Young [EY], 2020), increased accuracy and reliability of audit findings (PricewaterhouseCoopers [PwC], 2020) and better stakeholder engagement and communication (IIA, 2020)

Strategies for Implementing

Technology-Enabled Internal Audit

To implement technology-enabled internal audit functions, organizations can follow these strategies:

- Develop a clear technology strategy and roadmap (Deloitte, 2020)
- Invest in data analytics and AI tools (EY, 2020)
- Provide training and development opportunities for internal audit staff (IIA, 2020)
- Establish a culture of innovation and experimentation (KPMG, 2020)

The Skills and Competencies Required for Internal Auditors to Succeed in a Digital Age

The digital age has brought about significant changes in the way businesses operate, and internal auditors must adapt to these changes to remain relevant and effective. To succeed in a digital age, internal auditors require a unique set of skills and competencies that go beyond traditional auditing skills (Institute of Internal Auditors [IIA], 2020).

Technical Skills

Internal auditors require technical skills to navigate the digital landscape. These skills include data analytics and visualization (Deloitte, 2020), cloud computing and cybersecurity (Ernst & Young [EY], 2020), artificial intelligence and machine learning (KPMG, 2020) and robotic process automation (PricewaterhouseCoopers [PwC], 2020)

Soft Skills

In addition to technical skills, internal auditors require soft skills to effectively communicate and collaborate with stakeholders. These skills include communication and presentation skills (IIA, 2020), interpersonal and collaboration skills (Deloitte, 2020), adaptability and flexibility (EY, 2020) and critical thinking and problem-solving skills (KPMG, 2020)

Business Acumen

Internal auditors require business acumen to understand the organization's operations and risks. This includes understanding of the organization's strategy and objectives (PwC, 2020), knowledge of the organization's industry and regulatory requirements (IIA, 2020) and familiarity with the organization's technology infrastructure (Deloitte, 2020)

Conclusion

The digital age presents both opportunities and challenges for internal audit functions. To thrive in this era, internal audit must be willing to disrupt traditional audit practices and embrace new technologies, tools, and methodologies. By doing so, internal audit can provide greater value to the organization, improve audit efficiency and effectiveness, and enhance the overall risk management process.

The choice is clear: disrupt or be disrupted. Internal audit functions that fail to adapt to the digital age risk becoming irrelevant and losing their value proposition. On the other hand, those that embrace disruption and innovation will be well-positioned to thrive in a rapidly changing business environment.

As internal audit functions navigate the digital age, they must keep in mind the following key takeaways:

- Embrace technology and innovation to enhance audit processes and improve efficiency
- Develop new skills and competencies to stay relevant in a rapidly changing business environment
- Focus on providing value-added services that support the organization's strategic objectives
- Foster a culture of innovation and experimentation within the internal audit function

By following these principles, internal audit functions can not only survive but thrive in a digital age.

References

Deloitte. (2020). Internal Audit in a Digital Age. Deloitte.

Ernst & Young. (2020). Digital Audit: Leveraging Technology to Improve Audit Quality. EY.

Institute of Internal Auditors. (2020). Internal Audit in a Digital Age: A Guide for Internal Auditors. IIA.

KPMG. (2020). Internal Audit in a Digital Age: Leveraging Technology to Improve Audit Efficiency and Effectiveness. KPMG.

PricewaterhouseCoopers. (2020). Digital Internal Audit: Leveraging Technology to Improve Audit Quality. PwC

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

Understanding Root Cause Analysis in Dealing with Critical Audit Issues



Definition of Root Cause Analysis (RCA)

Root Cause Analysis (RCA) is a systematic approach used to identify the underlying reasons behind problems or failures within an organization. In auditing, RCA helps in diagnosing the causes of non-compliance, fraud, financial misstatements, or operational inefficiencies. Rather than just addressing the symptoms, RCA focuses on eradicating the source of the issue to prevent recurrence.

Background and Significance

The concept of RCA can be traced back to early problem-solving techniques developed in the mid-20th century, notably within the Toyota Production System, which emphasized continuous improvement (Kaizen) and the "Five Whys" technique. Over time, RCA has evolved to incorporate structured methodologies such as Fishbone Diagrams (Ishikawa), Fault Tree Analysis (FTA), and Failure Mode and Effects Analysis (FMEA).

Organizations implement RCA to enhance efficiency, improve decision-making, and mitigate risks by addressing the root cause rather than just the symptoms of an issue. By systematically analyzing contributing factors and implementing corrective measures, RCA helps organizations maintain operational excellence and prevent recurring problems.

Importance of Root Cause Analysis in Auditing

RCA plays a vital role in the audit process by ensuring that errors, misstatements, or fraud are identified and corrected at their source. Key benefits include:

- Strengthening internal controls to prevent recurring issues.
- Enhancing risk management strategies.
- Ensuring compliance with regulatory requirements.
- Improving operational efficiency by addressing systemic weaknesses.
- Providing management with insights to improve decision-making.

Key Principles of Root Cause Analysis

Effective RCA in auditing is built on the following principles:

- **Systematic Approach**: Following a structured methodology rather than making assumptions.
- **Fact-Based Investigation**: Using data and objective evidence rather than speculation.
- **Focus on Prevention**: Addressing root causes rather than temporary fixes.
- **Holistic View**: Considering multiple factors including processes, people, and technology.
- **Continuous Improvement**: RCA should be an ongoing process, not a one-time exercise.

Common Critical Audit Issues Requiring RCA

Several audit issues necessitate the application of RCA, including:

- **Financial Statement Misstatements**: Caused by human errors, fraudulent activities, or weak internal controls.
- **Regulatory Non-Compliance**: Arising from improper documentation, misinterpretation of rules, or governance failures.
- **Fraudulent Transactions**: Involving manipulation of financial records, unauthorized payments, or false reporting.
- **Operational Inefficiencies**: Resulting from outdated processes, lack of training, or system failures.

Steps in Conducting Root Cause Analysis for Audits

The RCA process in auditing typically follows these steps:

- **Identify the Problem** – Clearly define the audit issue requiring investigation.
- **Gather and Analyze Data** – Collect relevant audit reports, financial records, and internal control documents.
- **Identify Possible Causes** – Use brainstorming sessions and analytical tools to determine potential reasons for the issue.
- **Determine the Root Cause** – Apply RCA techniques to pinpoint the fundamental reason behind the issue.
- **Develop and Implement Solutions** – Propose corrective actions and preventive measures.
- **Monitor and Evaluate Effectiveness** – Continuously track the implemented changes to ensure they prevent recurrence.

Tools and Techniques for RCA in Auditing

Several methodologies can be used to perform RCA in auditing, including:

- **5 Whys Analysis**: Asking "why" multiple times until the root cause is uncovered.
- **Fishbone (Ishikawa) Diagram**: Visualizing potential causes categorized under people, processes, technology, and environment.
- **Failure Mode and Effects Analysis (FMEA)**: Evaluating potential failures and their impact.
- **Pareto Analysis**: Identifying the most frequent issues contributing to audit failures.
- **Flowcharting**: Mapping out processes to find inefficiencies or control gaps.

Challenges in Implementing RCA in Auditing

Despite its benefits, RCA in auditing faces several challenges, including:

- **Resistance to Change**: Employees and management may resist the implementation of new controls.
- **Data Availability Issues**: Lack of accurate records can hinder root cause identification.
- **Time Constraints**: Comprehensive RCA requires time and effort, which may conflict with deadlines.
- **Lack of Expertise**: Auditors may require specialized skills and training to conduct effective RCA.



Best Practices for Effective RCA in Auditing

To maximize the effectiveness of RCA in audits, the following best practices should be followed:

- **Involve a Cross-Functional Team**: Engage professionals from finance, compliance, IT, and operations.
- **Use Multiple RCA Techniques**: Combining different methodologies ensures comprehensive analysis.
- **Ensure Executive Support**: Management buy-in is crucial for implementing corrective actions.
- **Foster a Culture of Continuous Improvement**: Encourage ongoing learning and process enhancement.
- **Regularly Review and Update RCA Framework**: Adapt to changing regulations and organizational needs.

Case Studies on RCA in Audit Investigations

Case Study 1: Financial Misstatement in a Large Corporation

Issue: A multinational company was found to have misstated revenues over three consecutive financial years.

RCA Findings: The root cause was pressure on the finance department to meet unrealistic earnings targets, leading to fraudulent revenue recognition.

Solution: Implementing stronger financial controls, training staff on ethical accounting, and enforcing stricter compliance measures.

Case Study 2: Compliance Breach in a Banking Institution

Issue: A bank was fined for failing to comply with anti-money laundering (AML) regulations.

RCA Findings: The audit revealed inadequate customer due diligence procedures and outdated transaction monitoring systems

Solution: Enhancing compliance training, upgrading monitoring systems, and introducing independent reviews of high-risk transactions.

Conclusion

Root Cause Analysis is a critical tool in auditing that helps organizations identify the fundamental reasons behind audit issues, allowing them to implement long-term solutions. By systematically analyzing failures and weaknesses, auditors can enhance compliance, reduce financial risks, and improve operational efficiencies. Applying effective RCA techniques ensures that organizations not only address immediate audit concerns but also strengthen their governance and control environments for sustainable success.

References

- International Federation of Accountants (IFAC). (2020). *Handbook of International Quality Control, Auditing, Review, Other Assurance, and Related Services Pronouncements.*
- Public Company Accounting Oversight Board (PCAOB). (2019). *Auditing Standard No. 5.*
- Financial Reporting Council (FRC). (2021). *The Role of Root Cause Analysis in Audit Quality.*
- Organization for Economic Co-operation and Development (OECD). (2018). *Corporate Governance and Internal Controls.*
- Institute of Internal Auditors (IIA). (2020). *Root Cause Analysis in Internal Auditing: Best Practices and Case Studies.*

Egboro Evi Johnmark (Investigations Unit, Providus Bank Ltd)

Images of the 60th Quarterly General Meeting of the Association

held on December 12,2024 at Idera Hall,Radisson Blu Anchorage Hotel, Victoria Island
hosted by Suntrust Bank Limited with the theme: The Impacts of Financial Disruptions and the Role of Auditors



www.acaebin.org facebook.com/acaebin

Leveraging Automation to Improve the Efficiency and Effectiveness of Internal Audit in Banks

The banking environment today is fast-paced and becoming more complex. This has mounted pressure on internal auditors to ensure efficiency and accuracy in carrying out their audit processes.

The traditional methods, which are characterized by manual data gathering, transaction and process testing, and report generation, are time-consuming and resource intensive. As banks navigate a landscape rife with regulatory changes, cyber threats and market volatility, the need for more agile, comprehensive audit practices has never been greater.

Automation offers a transformative solution. By incorporating advanced technologies such as Robotic Process Automation (RPA), Artificial Intelligence (AI), and continuous auditing tools, banks can streamline their internal audit functions, reduce human error, and improve the detection of risks in real time. Automation not only enhances operational efficiency but also enables auditors to focus on more strategic and value-adding tasks, empowering them to better assess risks and ensure compliance with ever-evolving regulations.



Automation is the use of technology, systems, or machines to do tasks that would otherwise require human labour, with the primary purpose of eliminating the need for direct human involvement. The process involves the design, programming, and deployment of machines or software capable of completing repetitive, time-consuming, or sophisticated operations with great precision and consistency. The goal of automation is to use technology to improve human productivity.

Robotic Process Automation (RPA) is a form of automation that involves using software robots, or 'bots', to automate repetitive, rule-based tasks traditionally performed by humans. These bots mimic human actions by interacting with digital systems and performing tasks such as data entry, form filling, and data extraction.

This article explores how automation can revolutionize internal audits in the banking sector, offering insights into the technologies that are reshaping the industry and the tangible benefits they bring to both auditors and banks.

Applications of Automation in Audit Processes

Automation Utilization During the Opening Stage of the Audit.

- **Automated Dashboards and Audit Management Systems** facilitate the planning and tracking of audits, ensuring that timelines are clearly defined and adhered to. These systems provide audit teams with real-time updates on tasks and requirements, promoting accountability and transparency. Additionally, they enhance information sharing and collaboration among team members, fostering efficient work delegation and streamlining overall audit processes.

The system can automate the issuance of official invitations and notices for opening meetings directly from the audit plan, eliminating the need for manual scheduling and invitation management by the audit team, thereby enhancing efficiency and reducing administrative workload.

- **Gathering Client and System Data -** Automation can be used to automatically pull key data from the bank's systems, such as financial statements, transaction records, compliance reports, risk assets, general ledgers and prior audit findings. This solution can then be stored in a designated location. This reduces the manual effort required to gather and organize relevant documentation.

- **Risk Assessment and Prioritization -** Automated data analytics tools can analyze the bank's historical performance and transaction patterns to help identify high-risk areas in the audit. This allows auditors to focus on the most critical areas such as fraud detection, compliance with regulations or internal control weaknesses.

Automation Utilization During the Fieldwork Stage of Internal Audit

During this phase, the audit team performs the audit. Some of the procedures generally performed during fieldwork are as follows:

- Review supporting documentation.
- Review processes.

- Perform analyses.
- Identify exceptions.

The following examples have been extracted from the fieldwork stage of different audits to be mapped with RPA and automate the internal audit department:

- Robotic Process Automation (RPA) can be configured to identify and respond to potential fraud such as money laundering, erroneous transfers etc. using automated **rules-based** monitoring of transactions. Instances flagged as suspicious transactions will then be reviewed by the auditors. This will help auditors focus on other risk areas.

- RPA can automate the detection of suspicious logs in IT systems by continuously monitoring and flagging anomalies, ensuring quicker response to potential security threats. It streamlines the gathering of audit documentation by automatically collecting and organizing evidence from business processes, transactions, and IT systems. This reduces manual effort, increases accuracy, and provides up-to-date audit information.

- RPA combined with OCR (Optical Character Recognition) enhances audits by automating data extraction and processing. OCR scans documents (e.g., invoices, receipts, approval memos) and converts text into machine-readable formats, while RPA automates tasks like data entry, validation, reconciliation, document classification, and report generation. This can be used to review the general ledgers, entries into the general ledgers, expense report and supporting receipts, validating them against company policies, and cross-referencing with databases for consistency. It can also be used to review TAT and other key elements of reports rendered. This integration speeds up audits, improves accuracy, reduces human error, ensures compliance, and lowers costs. By eliminating manual tasks, RPA reduces errors, improves accuracy, and saves significant time, allowing employees to focus on more strategic work and enhancing overall efficiency

- RPA can be effectively used in continuous auditing by automating repetitive tasks. RPA ensures that audits are performed in real time, rather than at periodic intervals. This enables auditors to identify discrepancies or compliance issues promptly, improving efficiency, accuracy, and the ability to address risks more proactively. RPA can also be applied to audit entire populations rather than the samples. Tests can be run consistently and automatically to get results that can be analyzed for an exception or anomaly in the test.

Automation Utilization During Audit Closing and Follow Up

Control Log Automation:

- **RPA bots** can be programmed to extract and send out exceptions from approved reports to the responsible Teams/Units

- **RPA bots** can monitor inboxes or systems (like an audit management tool) for incoming responses to the additional evidence requests or regularization evidence.

- **Automated reminders** can also be sent by the bot on exceptions yet to be

- **The bot can** review evidence sent for regularization and forward the same to the audit team for review.

- **The bot** can escalate cases that remain unresolved after multiple reminders, either by notifying the audit team or sending additional notices.

- **Dashboard views** can be created for audit managers to quickly assess progress and status of open exceptions.

Importance/ Benefits

- **Improved Efficiency, Accuracy and Consistency:** Automation greatly enhances efficiency in the internal audit department by reducing time spent on manual, repetitive tasks like data entry and report generation. This allows auditors to focus on more complex, value-added activities. Automated systems can process large volumes of data quickly and accurately, minimizing errors and accelerating audit cycles. As a result, the bank's audit function becomes faster, more accurate, and better equipped to handle increased workload without additional resources.

- **Increased Coverage and Scope:** Automation in the internal audit department significantly expands the coverage and scope of audits. By automating data collection, analysis, and reporting, auditors can access and analyze larger datasets across multiple systems, ensuring a more comprehensive review of bank operations. Automation enables audits to be conducted more frequently, covering a broader range of processes, transactions, and risk areas that might be time-consuming or overlooked with manual methods. This enhanced coverage allows the audit team to identify potential issues or risks earlier, improve overall risk management, and provide more valuable insights to management. As a result, the bank can achieve a deeper, more thorough understanding of its operations and regulatory compliance, leading to improved decision-makingand stronger governance.

- **Real-time Risk Detection:** Automation enhances the ability of the internal audit department to detect risks in real time. By continuously monitoring transactions and processes, automated systems can quickly identify anomalies, patterns, or deviations from expected behaviour that may signal potential risks, fraud, or compliance issues. This real-time capability enables auditors to address problems as they arise, rather than discovering them after a lengthy audit cycle. As a result, the bank can respond more swiftly to emerging threats, reduce the impact of risks, and ensure better ongoing risk management and compliance. Real-time risk detection enhances the bank's ability to protect its assets and maintain regulatory standards proactively.

Overcoming Challenges in Implementing Automation

- **Initial Costs and Investment**: Implementing automation systems often requires significant upfront investment, including the costs of purchasing software, hardware infrastructure, and potentially hiring specialized personnel to ensure proper integration and setup. While these initial costs can be substantial, it is important to consider the long-term benefits, such as improved efficiency, reduced manual labor, and minimized errors. Organizations should evaluate the return on investment (ROI) over time, considering not only financial savings but also the gains in productivity and scalability that automation can offer. Proper budgeting and strategic planning are essential to ensure a smooth transition and to justify the investment in automation as a catalyst for future growth and operational excellence.

- **Skill Gaps and Training Needs**: A key challenge in implementing automation in a bank's internal audit department is addressing skill gaps among staff. Auditors may lack the technical expertise required to operate automation tools effectively, such as knowledge in data analytics or specific audit software. To overcome this, the bank must invest in targeted training programs to equip staff with the necessary technical and analytical skills. This will ensure the tools are fully utilized, improving efficiency and accuracy in audits while fostering a culture of continuous learning and adaptation to new technologies.

- **Integration with Existing Systems**: Ensuring seamless integration with existing systems is key. Banks typically have complex legacy systems in place, which may not be compatible with modern automation tools. This can lead to difficulties in data transfer, system synchronization, and workflow alignment. To overcome this, careful planning and possibly custom development work are required to ensure the new automation tools integrate smoothly with current infrastructure. This process can be time-consuming and costly, but it is crucial to ensure that automation enhances, rather than disrupts, existing audit processes. Effective integration improves data accuracy, streamlines workflows, and maximizes the potential of automation

- **Data Security and Privacy Concerns**: Implementing automation in a bank's internal audit department raises data security and privacy concerns due to the handling of sensitive financial data. Automation tools must be designed with strong security features, such as encryption and secure access controls, to prevent data breaches and unauthorized access. Additionally, banks need to ensure compliance with data protection regulations and train staff on proper data governance. Striking the right balance between automation and stringent security measures is essential to protect customer trust and meet regulatory requirements.

Conclusion

Leveraging automation in the Internal Audit function presents a transformative opportunity to enhance both efficiency and effectiveness. Automating routine processes allows auditors to focus on higher-value activities, resulting in faster, more accurate audits and better decision-making. While initial investment expenditures, talent gaps, system integration, and data security must all be addressed, the long-term benefits significantly surpass these obstacles. With the correct strategy, training, and secure implementation, automation can assist to speed up audit processes, decrease errors, improve compliance, and ultimately drive improved governance and risk management in the banking industry. Banks that embrace automation position themselves to be more agile, data-driven, and capable of fulfilling the always changing demands of the financial industry.

References

https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/robotic-process-automation-for-internal-audit

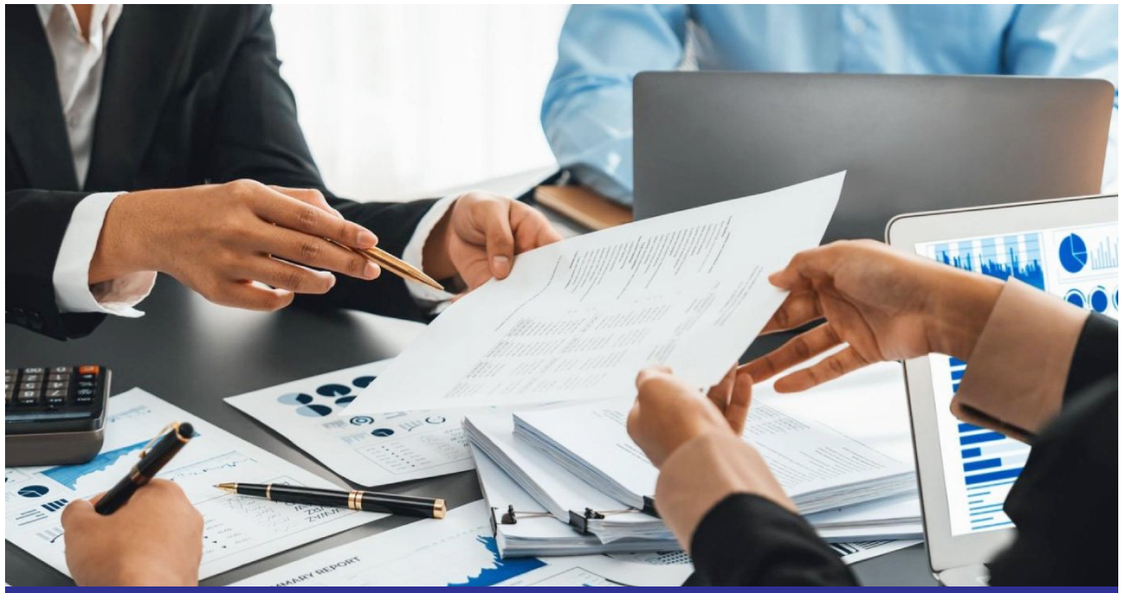
Seyi Otubobola and Jonathan Joshua
Internal Audit, Access Bank

Happy Birthday Distinguished CAEs



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

Signed:
Management



Results-Driven Audit Follow-up: Strategies for Success

Audit follow-up is a critical component of the audit process, ensuring that audit recommendations are implemented and that audit objectives are achieved (Institute of Internal Auditors, 2017). The purpose of audit follow-up is to monitor and report on the implementation status of audit recommendations, identify any obstacles to implementation, and take corrective action (International Organization for Standardization, 2018). Effective audit follow-up is essential for ensuring that audit recommendations are implemented, audit objectives are achieved (Cohen & Simnett, 2015) and risk identified are closed. Research has shown that audit follow-up can have significant impact on the implementation of audit recommendations (Knechel et al., 2012). A study by Knechel et al. (2012) found that audit follow-up was associated with higher levels of implementation of audit recommendations. Similarly, a study by Cohen and Simnett (2015) found that audit follow-up was an important factor in ensuring the implementation of audit recommendations.

Despite the importance of audit follow-up, research has also shown that it is often neglected or not performed effectively (Cohen & Simnett, 2015). A study by the Institute of Internal Auditors (2017) found that audit follow-up was often not performed or was performed inadequately. This can have serious consequences, including the failure to implement audit recommendations, failure to achieve audit objectives.

A result-driven audit follow-up approach requires a structured and systematic process, including clear goals and objectives, effective communication and stakeholder engagement, and ongoing monitoring and evaluation (International Organization for Standardization, 2018). By adopting such approach, organizations can ensure that audit follow-up is performed in a timely and effective manner, and that audit recommendations are implemented and verified (Cohen & Simnett, 2015).

This article provides an overview of the key strategies and best practices for results-driven audit follow-up, including planning and preparation, communication and stakeholder engagement, and monitoring and evaluation. By following these strategies, organizations can ensure that audit follow-up is performed effectively and efficiently, and that audit recommendations are implemented and sustained over time.

Effectiveness and Efficiency of Audit Follow-up

The effectiveness of audit follow-up can be measured in several ways, including implementation of audit recommendations,

achievement of audit objectives and improved governance and risk management (Cohen & Simnett, 2015). The efficiency of audit follow-up can be measured in several ways, including timeliness of follow-up activities, cost-effectiveness of follow-up activities, use of technology. The factors affecting effectiveness and efficiency of audit follow-up includes quality of audit recommendations, level of management support and the level of auditor training (Institute of Internal Auditors, 2017).

Types of Audit Follow-up

There are several types of audit follow-up, including:

Routine follow-up: This type of follow-up involves regular monitoring of the implementation of audit recommendations (Cohen & Simnett, 2015).

Special Follow-up: This type of follow-up involves in-depth review of specific audit recommendations, often in response to a significant risk or issue (Knechel et al., 2012).

Verification follow-up: This type of follow-up involves verifying the implementation of audit recommendations, often through testing or other forms of verification (Institute of Internal Auditors, 2017).

Progress Follow-up: This type of follow-up involves monitoring the progress of management in implementing audit recommendations (International Organization for Standardization, 2018).

Final Follow-up: This type of follow-up involves a final review of the implementation of audit recommendations, often to ensure that all recommendations have been implemented (Cohen & Simnett, 2015).

Self-Assessment Follow-up: This type of follow-up involves having management assess their own progress in implementing audit recommendations (Knechel et al., 2012).

Audit Committee Follow-up: This type of follow-up involves reporting to the audit committee on the implementation of audit recommendations (Institute of Internal Auditors, 2017).

External Follow-up: This type of follow-up involves external auditors or other external parties reviewing the implementation of audit recommendations (International Organization for Standardization, 2018).

Benefits of Audit Follow-up

Audit follow-up provides several benefits, including:

Improved audit quality: Audit follow-up helps to ensure that audit recommendations are implemented, which improves audit quality (Cohen & Simnett, 2015)

Increased accountability: Audit follow-up helps to ensure that management is held accountable for implementing audit recommendations (Knechel et al., 2012).

Enhanced risk management: Audit follow-up helps to identify and mitigate risks associated with non-implementation of audit recommendations (Institute of Internal Auditors, 2017).

Better Decision Making: Audit follow-up provides stakeholders with assurance that audit recommendations are being implemented, which informs better decision making (International Organization for Standardization, 2018).

Improved Governance: Audit follow-up helps to ensure that organizations are governed effectively, with audit recommendations being implemented and risks being managed (Cohen & Simnett, 2015).

Increased Efficiency: Audit follow-up helps to identify areas where processes can be improved, leading to increased efficiency (Knechel et al., 2012).

Enhanced Credibility: Audit follow-up helps to enhance the credibility of the audit function, as stakeholders can see that audit recommendations are being implemented (Institute of Internal Auditors, 2017).

Better Resource Allocation: Audit follow-up helps to ensure that resources are allocated effectively, as audit recommendations are implemented and risks are managed (International Organization for Standardization, 2018).

Improved Compliance: Audit follow-up helps to ensure that organizations are complying with relevant laws, regulations, and standards (Cohen & Simnett, 2015).

Enhanced Stakeholder Confidence: Audit follow-up helps to enhance stakeholder confidence in the organization, as stakeholders can see that audit recommendations are being implemented (Knechel et al., 2012).

Challenges of Audit Follow-up

Audit follow-up can be challenging, and some of the common challenges include:

Lack of Resources: Audit follow-up requires significant resources, including time, personnel, and budget (Cohen & Simnett, 2015). Auditors may not have the necessary resources to perform effective follow-up.

Low Priority: Audit follow-up may be seen as a low priority task, especially when compared to other audit tasks such as planning and fieldwork (Institute of Internal Auditors, 2017).

Lack of Management Support: Audit follow-up may not receive adequate support from management, which can make it difficult to perform effective follow-up (Knechel et al., 2012).

Complexity of Audit Recommendations: Audit



recommendations can be complex and difficult to implement, which can make follow-up challenging (Institute of Internal Auditors, 2017, International Organization for Standardization, 2018).

Limited Auditor Training: Auditors may not receive adequate training on audit follow-up, which can make it difficult to perform effective follow-up (Cohen & Simnett, 2015).

Inadequate Follow-up Procedures: Audit follow-up procedures may be inadequate or non-existent, which can make it difficult to perform effective follow-up (Institute of Internal Auditors, 2017).

Lack of Accountability: There may be a lack of accountability for audit follow-up, which can make it difficult to ensure that follow-up is performed effectively (Knechel et al., 2012).

Competing Priorities: Auditors may have competing priorities, such as other audit tasks or administrative tasks, which can make it difficult to perform effective follow-up (International Organization for Standardization, 2018).

Limited Stakeholder Engagement: There may be limited stakeholder engagement in the audit follow-up process, which can make it difficult to ensure that follow-up is performed effectively (Cohen & Simnett, 2015).

Inadequate Technology: Audit follow-up may not be supported by adequate technology, which can make it difficult to perform effective follow-up (Institute of Internal Auditors, 2017).

Strategies and best practices for results-driven audit follow-up

Effective audit follow-up is crucial to ensuring that audit recommendations are implemented and that audit objectives are achieved. A results-driven audit follow-up process helps to verify that agreed-upon actions have been taken, and that the desired outcomes have been realized. Here are some strategies and best practices for results-driven audit follow-up:

Strategies

Clearly Define Audit Objectives and Recommendations: Ensure that audit objectives and recommendations are specific, measurable, achievable, relevant, and time-bound (SMART).

Establish a Follow-Up Plan: Develop a follow-up plan that outlines the steps to be taken, the responsible parties, and the timelines for completion.

Assign Accountability: Assign clear accountability for implementing audit recommendations and for conducting follow-up activities.

Use Technology to Facilitate Follow-Up: Leverage technology, such as audit management software, to facilitate follow-up activities, track progress, and

document results.

Conduct Regular Progress Updates: Conduct regular progress updates to ensure that agreed-upon actions are being taken and that the desired outcomes are being achieved.

Best Practices:

Verify Implementation of Recommendations: Verify that agreed-upon recommendations have been implemented and that the desired outcomes have been achieved.

Document Results: Document the results of follow-up activities, including any successes, challenges, or areas for improvement.

Communicate Results: Communicate the results of follow-up activities to stakeholders, including audit committees, management, and employees.

Continuously Monitor and Evaluate: Continuously monitor and evaluate the effectiveness of audit follow-up activities and make adjustments as needed.

Recognize and Reward Success: Recognize and reward employees and management for successfully implementing audit recommendations and achieving desired outcomes.

Conclusion

Audit follow-up is a critical component of the audit process, ensuring that audit recommendations are implemented and that audit objectives are achieved. Effective audit follow-up provides numerous benefits, including improved audit quality, increased accountability, enhanced risk management, and better decision making. However, audit follow-up can be challenging, and its effectiveness can be influenced by various factors, such as the quality of audit recommendations, the level of management support, and the level of auditor training.

To ensure effective audit follow-up, organizations should establish a formal audit follow-up process, provide training to auditors on audit follow-up, and use technology to improve the efficiency of the audit follow-up process. Additionally, organizations should ensure that audit follow-up is performed in a timely and effective manner, and that audit recommendations are implemented and verified. Effective audit follow-up is essential for ensuring that audits are effective and that organizations achieve their objectives. By prioritizing audit follow-up and ensuring that it is performed effectively, organizations can improve their governance, risk management, and overall performance.

Recommendations

Develop a Follow-up Plan: Auditors should develop a follow-up plan to ensure that audit recommendations are implemented and verified (Institute of Internal Auditors, 2017).

Provide Training to Auditors: Organizations should provide training to auditors on audit follow-up to ensure that they have the necessary skills and knowledge to perform effective follow-up (Cohen & Simnett, 2015).

Use Technology to Improve Efficiency: Auditors should use technology to improve the efficiency of the audit follow-up process, such as using audit management software to track and monitor follow-up activities (International Organization for Standardization, 2018).

Monitor and Report on Follow-up Activities: Auditors should monitor and report on follow-up activities to ensure that audit recommendations are implemented and verified (Cohen & Simnett, 2015).

Verify the Implementation of Audit Recommendations: Auditors should verify the implementation of audit recommendations to ensure that they are effective and operating as intended (International Organization for Standardization, 2018).

Communicate with Management and Stakeholders: Auditors should communicate with management and stakeholders to ensure that they are aware of follow-up activities and the implementation of audit recommendations (Knechel et al., 2012).

References:

Cohen, J., & Simnett, R. (2015). The role of audit follow-up in the audit process. *Auditing*: A Journal of Practice & Theory, 34(2), 147-164.

Institute of Internal Auditors. (2017). International standards for the professional practice of internal auditing. Institute of Internal Auditors.

International Organization for Standardization. (2018). ISO 19011:2018 - Guidelines for Auditing management systems. International Organization for Standardization.

Knechel, W. R., Salterio, S. E., & Ballou, B. (2012). The effects of audit committee expertise On audit quality. Auditing: A Journal of Practice & Theory, 31(2), 151-173.

Emuebie Emeke, Head, Branch & Services Audit, Union Bank Plc.

Urologists list reasons men with heart disease suffer erectile dysfunction

Male sexual reproductive experts have given reasons why men suffering from heart conditions may experience sexual problems, including erectile dysfunction.

The urologists explained that the ability to achieve an erection is closely linked to the flow of blood around the body, particularly to the penis.

According to them, when the arteries that bring blood to the penis are compromised, it could lead to erectile dysfunction.

Speaking exclusively with *PUNCH Healthwise*, the physician emphasised that heart conditions, such as high blood pressure and heart failure, could affect a man's ability to achieve an erection.

The experts advised men who are experiencing sexual problems to seek medical attention.

A consultant urologist, Dr. Emmanuel Eze, urged men to be more aware of the link between heart health and sexual function.

According to him, men with heart conditions such as coronary artery disease, high blood pressure, and heart failure are more likely to experience erectile dysfunction and other sexual problems.

He described erectile dysfunction as the inability to achieve or maintain an erection sufficient for satisfactory sexual performance.

"The relationship between heart health and sexual function is complex. Men with heart conditions may experience decreased blood flow to the penis, making it difficult to achieve and maintain an erection," he stated.

In addition to erectile dysfunction, the physician said men with heart conditions may also experience other sexual problems, such as decreased libido, premature ejaculation, and painful intercourse.

He noted that these problems can have a significant impact on a man's quality of life and relationships.

The urologist emphasised that the link between heart health and sexual function is not just physical, but also psychological.



He stated that men with heart conditions may experience anxiety, depression, and stress, which could further worsen sexual problems.

"The good news is that many of these sexual problems can be treated. Men with heart conditions should not hesitate to speak with their healthcare provider about their sexual health. With the right treatment and lifestyle changes, many men can improve their sexual function and overall quality of life," he advised.

The physician, however, recommended that men with heart conditions take steps to manage their condition, including making healthy lifestyle changes such as exercising regularly, eating a healthy diet, and quitting smoking.

On his part, a Senior Registrar in Urology at the Lagos State University Teaching Hospital, Dr. Akpo Edewor stressed that erectile dysfunction can be a symptom of an underlying health condition, and that seeking medical attention can help to identify and treat the underlying condition.

Edewor also identified diabetes as a potential cause of erectile dysfunction.

The urologist explained that diabetes can damage the blood vessels and nerves that control erection, leading to erectile dysfunction.

He added, "When the arteries that bring blood to the penis are compromised, it can lead to erectile dysfunction. So, men suffering from heart conditions need to be aware of this potential complication and seek medical attention if they experience any symptoms.

"Erectile dysfunction can be a symptom of an underlying health condition, and seeking medical attention can help to identify and treat the underlying condition. So, it's essential for men to seek medical attention if they experience persistent erectile dysfunction.

"Heart conditions, such as high blood pressure and heart failure, can affect a man's ability to achieve an erection. When the heart is not functioning properly, it can lead to a reduction in blood flow to the penis, making it difficult to achieve an erection.
"Diabetes can damage the blood vessels and nerves that control erection, leading to erectile dysfunction. So, men with diabetes need to be aware of this potential complication and work with their healthcare provider to manage their condition."

Culled from: healthwise.punchng.com

Cybersecurity Threat in The Financial Sector: The Role of Internal Audit Functions



The financial sector is increasingly vulnerable to cybersecurity threats, which can have devastating consequences for organizations, customers, and the economy as a whole (Deloitte, 2020). Cybersecurity threats, such as phishing, malware, and ransomware attacks, can compromise sensitive financial information, disrupt business operations, and erode customer trust (Verizon, 2020). As noted by the Institute of Internal Auditors (IIA) (2019), "cybersecurity is a critical concern for financial institutions, and internal audit functions play a vital role in helping organizations mitigate these threats" (p. 1).

The financial sector is a prime target for cyber attackers due to the sensitive nature of financial information and the potentials for significant financial gain (Ponemon Institute, 2019). According to the Identity Theft Resource Center (2020), the financial sector accounted for 24% of all data breaches in 2020, highlighting the need for effective cybersecurity measures.

Internal audit functions play a critical role in helping financial institutions mitigate cybersecurity threats. As noted by ISACA (2020), "internal audit functions can provide assurance that cybersecurity controls are operating effectively and identify areas for improvement" (p. 2). This paper will explore the role of internal audit functions in mitigating cybersecurity threats in the financial sector and provide guidance on best practices for internal audit functions in this area.

Cybersecurity Threats in the Financial Sector

As a hub for sensitive financial data and transactions, the financial sector is a prime target for cyber attackers seeking to exploit vulnerabilities for financial gain (Ponemon Institute, 2019). Cybersecurity threats in the financial sector can have devastating consequences, including financial loss, reputational damage, and compromised customer information (Deloitte, 2020). Cybersecurity threats in the financial sector are numerous and varied, including:

Phishing and social engineering attacks: These types of attacks involve tricking employees or customers into divulging sensitive information or clicking on malicious links (Verizon, 2020).

Malware and ransomware attacks: These types of attacks involve using malicious software to disrupt or disable computer systems, often with the goal of extorting money from the victim (Ponemon Institute, 2019).

Data breaches: These types of attacks involve unauthorized access to sensitive information, such as customer data or financial records (Identity Theft Resource Center, 2020).

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks: These types of attacks involve overwhelming a computer system with traffic in order to make it unavailable to users (Akamai, 2020)

Impact of Cybersecurity Threats on the Financial Sector

Cybersecurity threats can have a significant impact on the financial sector, amongst which are:

Financial loss: Cybersecurity breaches can result in significant financial losses, including the cost of responding to the breach, notifying customers, and providing credit monitoring services (Ponemon Institute, 2019).

Reputational damage: Cybersecurity breaches can damage the reputation of financial institutions, leading to a loss of customer trust and confidence (Deloitte, 2020).

Compromised customer information: Cybersecurity breaches can result in the compromise of sensitive customer information, including personal and financial data (Identity Theft Resource Center, 2020).

The Role of Internal Audit Functions in Cybersecurity

Internal audit functions play a critical role in helping financial institutions mitigate cybersecurity threats. Some of the key responsibilities of internal audit functions in this area include:

Risk assessment: Identifying and assessing the organization's cybersecurity risks, including vulnerabilities in systems, processes, and personnel (IIA, 2019).

Control evaluation: Evaluating the effectiveness of the organization's cybersecurity controls, including policies, procedures, and technology (ISACA, 2020).

Testing and assurance: Providing assurance that the organization's cybersecurity controls are operating effectively, through testing and other assurance activities (IIA, 2019).

Follow-Up and Verification: Internal audit functions should follow up and verify that agreed-upon actions have been taken to address cybersecurity risks and improve controls

Best Practices for Internal Audit Functions in Cybersecurity

As cybersecurity threats continue to evolve and become more sophisticated, internal audit functions play a critical role in ensuring the effectiveness of an organization's cybersecurity controls. The following are some best practices for internal audit functions in cybersecurity:

Staying up-to-date with emerging threats and technologies: Internal audit functions should stay current with the latest cybersecurity threats and technologies, to ensure that they are equipped to identify and mitigate risks (Deloitte, 2020).

Collaborating with other stakeholders: Internal audit functions should collaborate with other stakeholders, including IT, risk management, and compliance, to ensure that cybersecurity risks are identified and mitigated (IIA, 2019).

Risk-Based Approach: Internal audit functions should adopt a risk-based approach to cybersecurity auditing. This involves identifying and prioritizing high-risk areas, such as sensitive data storage and transmission, and focusing audit efforts on those areas

Audit of Cybersecurity Governance: Internal audit functions should audit the organization's cybersecurity governance framework to ensure that it is adequate and effective.

Assessment of Cybersecurity Controls: Internal audit functions should assess the design and operating effectiveness of cybersecurity controls, including firewalls, intrusion detection systems, and encryption technologies.

Identification and Reporting of Cybersecurity Risks: Internal audit functions should identify and report on cybersecurity risks to management and the board of directors.

Follow-Up and Verification: Internal audit functions should follow up and verify that agreed-upon actions have been taken to address cybersecurity risks and improve controls.

Use of Cybersecurity Frameworks and Standards: Internal audit functions should use recognized cybersecurity frameworks and standards, such as the NIST Cybersecurity Framework and the ISO 27001 standard, to guide their audit work.

Continuous Monitoring: Internal audit functions should continuously monitor the organization's cybersecurity controls and report on any

changes or updates.

Communication and Reporting: Internal audit functions should communicate and report on cybersecurity audit findings and recommendations in a clear and concise manner, using language that is easily understood by non-technical stakeholders.

Providing assurance and advisory services: Internal audit functions should provide assurance and advisory services to help the organization improve its cybersecurity posture (ISACA, 2020).

Conclusion

The financial sector is a prime target for cyber attackers, and the consequences of a successful attack can be devastating. As the threat landscape continues to evolve, it is imperative that financial institutions prioritize cybersecurity and leverage the expertise of internal audit functions to identify and mitigate potential vulnerabilities.

Effective internal audit functions play a critical role in ensuring the financial sector's resilience to cybersecurity threats. By providing assurance on the design and operating effectiveness of cybersecurity controls, internal audit functions can help financial institutions identify and address potential vulnerabilities before they can be exploited.

To stay ahead of the evolving threat landscape, financial institutions must adopt a proactive and collaborative approach to cybersecurity. This includes investing in advanced technologies, fostering a culture of cybersecurity awareness, and leveraging the expertise of internal audit functions to ensure the effectiveness of cybersecurity controls.

The financial sector's ability to withstand cybersecurity threats will depend on its ability to adapt, innovate, and collaborate. By prioritizing cybersecurity and leveraging the expertise of internal audit functions, financial institutions can help protect their customers, reputation, and bottom line



References

Akamai. (2020). 2020 State of the Internet Security Report. Akamai.

Deloitte. (2020). 2020 Global Cybersecurity Survey. Deloitte.

Identity Theft Resource Center. (2020). 2020 Data Breach Report. Identity Theft Resource Center.

Institute of Internal Auditors. (2019). Cybersecurity: A Guide for Internal Auditors. IIA.

International Organization for Standardization. (2013). ISO/IEC 27001:2013. ISO.

ISACA. (2020). Cybersecurity Audit/Assurance Program. ISACA.

Ponemon Institute. (2019). 2019 Cost of a Data Breach Report. Ponemon Institute.

Verizon. (2020). 2020 Data Breach Investigations Report. Verizon.

Emuebie Emeke, Head, Branch & Services Audit, Union Bank Plc.

4TH QUARTER 2024 & 1ST QUARTER 2025 CBN CIRCULARS

S/N	DATE PUBLISHED	TITLE OF CIRCULAR	REFERENCE	DEPARTMENT
1	25/11/2024	Guidelines for the Electronic Foreign Exchange Matching System (EFEMS)	FMD/DIR/CON/OGC/038/151	Financial Markets Department
2	25/11/2024	Implementation of the Bloomberg Bmatch System for Foreign Exchange Trading	FMD/DIR/CON/OGC/038/150	Financial Markets Department
3	29/11/2024	Revised Guidelines for the Nigeria Foreign Exchange Market (NFEM)	FMD/DIR/CON/OGC/040/0012	Financial Markets Department
4	29/11/2024	Superseded Circular - Operationalisation of the Standing Deposit Facility (SDF) Asymmetric Corridor: Post 298th Meeting of the Monetery Policy Committee (MPC)	FMD/DIR/PUB/CIR/001/022	Financial Markets Department
5	29/11/2024	Cash Availability over the Counter in Deposit Money Banks (DMBs) ans Automated Teller Machines (ATMs)	COD/DIR/INT/CIR/001/023	Currency Operations Department
6	13/12/2024	Updated Penalty on Inappropriate Cash Disbursement Practices by Deposit Money Banks (DMBs)	COD/DIR/INT/CIR/001/025	Currency Operations Department
7	17/12/2024	Circular on Cash-out Limits for Agent Banking Transactions	PSM/DIR/PUB/CIR/001/057	Payment Systems Management Department
8	19/12/2024	Sales of Foreign Exchange to BDCs to meet Retail Market demand for eligible invisible Transaction	TED/FEM/PUB/FPC/001/030	Trade and Exchange Department
9	8/1/2025	Suspension of Extension of Export Proceeds on behalf of Exporters	TED/FEM/FPC/GEN/001/001	Trade and Exchange Department
10	10/1/2025	Introduction of Non-Resident Nigerian Ordinary Account and Non-Resident Nigerian Investment Account	TED/FEM/PUB/FPC/001/002	Trade and Exchange Department
11	24/1/2025	Waiver of Non-Refundable Annual Licence Renewal Fee for Existing Bureaux De Change	FPR/DIR/PUB/CIR/001/001	Financial Policy and Regulatory Department
12	3/2/2025	Sales of Foreign Exchange to BDCs to meet Retail Market demand for eligible invisible Transaction	TED/FEM/PUB/FPC/001/003	Trade and Exchange Department
13	5/2/2025	Sales of Foreign Exchange to BDCs to meet Retail Market demand for eligible invisible Transaction	TED/FEM/PUB/FPC/001/004	Trade and Exchange Department
14	19/2/2025	Review of Automated Teller Machine Transaction Fees	FPR/DIR/PUB/CIR/001/002	Financial Policy and Regulatory Department
15	17/2/2025	Guidelines on Management OF Dormant Accounts, Unclaimed Balances and other Financial Assets in Banks and other Financial Institutions in Nigeria	FPR/DIR/PUB/CIR/001/004	Financial Policy and Regulatory Department

ACAEBIN DIRECTORY

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



Alpha Morgan Bank Limited.
Funmilola Adelokun,
54, Adetokubo Ademola Street,
Victoria Island,
Lagos.
funmilayo.adelokun@alphamorganbank.com
08023596393



Bank of Agriculture Limited
Baba Musami Marte
1, Yakubu Gowon Way
Kaduna.
b.marte@boanig.com
08036910864



Bank of Industry Limited
Onome Agorua
23, Marina
Lagos.
oagorua@boi.ng
08186963837,
DL: 01-2715087



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



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



Coronation Merchant Bank Limited
10, Amodu Ojikutu Street,
Victoria Island, Lagos

Development Bank of Nigeria
Joshua Ohioma
The Clans Place, Plot 1368A,
Tigris Crescent, Maitama, Abuja.
johioma@devbankng.com
08129145586



Ecobank Nigeria Ltd
Bisi Bello
Ecobank Pan African Centre (EPAC)
270, Ozumba Mbadiwe Street,
Victoria Island, Lagos, Nigeria
bibello@ecobank.com
07036515349



FBNQuest Merchant Bank Limited
Leslie Gumut
2, Broad Street, Marina
Lagos
leslie.gumut@fbnquestmb.com
08036450808



Federal Mortgage Bank of Nigeria
Ibrahim N. Ahmed
Plot 266, Cadastral AO, Central Business District
P.M.B 2273, Abuja
ibrahim.nafada@fmbn.gov.ng
08023157410,
01-4602102



Fidelity Bank Plc
Ugochi Osinigwe
Fidelity Bank Plc.
Adeyemo Alakija Street, V/I,
Lagos.
ugochi.osinigwe@fidelitybank.ng
08023030298,
08092147012



First Bank of Nigeria Ltd.
Mufutau Abiola
9/11, McCarthy Street, Lagos
Mufutau.Abiola@firstbanknigeria.com
08129145605



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



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



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



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



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



JAIZ BANK PLC
Musefiu A. Olalekan-Rasidi
No. 73 Ralph Shodeinde Street,
Central Business District,
P.M.B. 31 Garki Abuja,
Nigeria.
musefiu.olalekan-rasidi@jaizbankplc.com
080 5978 6222



Keystone Bank Limited
Abiodun Okusanmi
1, Keystone Crescent
Victoria Island, Lagos.
Nigeria.
biodunokusami@keystonebankng.com
08033534920



Lotus Bank Ltd
Saheed Adeluola Ekeolere
39C, Ahmed Onibudo,
Victoria Island,
Lagos.
Saheed.ekeolere@lotusbank.com
08033050015



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 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 Island, 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 Odukomaiye
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.
Yousuph.edu@suntrustng.com
08037274559



TajBank Nigeria Limited
Sabiu Muhammed Ibrahim
Plot 72, Ahmadu Bello Way,
Central Business District Abuja,
Nigeria.
sabiu.ibrahim@tajbank.com
08065436622



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