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+printbyProwess08039221516

Eagle Eye

A Quarterly Publication of the Association of Chief Audit Executives of Banks in Nigeria (ACAEBIN) Q1, 2024

The Role of the Internal Auditor in Promoting Stability in the Financial Services Sector and National Economic Growth

Continuous Auditing: Can It Supercharge Your Controls ... Page 12

Eating nuts, seeds improves brain health, lowers heart diseases risk Page 16

Common Vulnerabilities and Exposure (CVE)

ACAEBIN EXCO MEMBERS

Prince Akamadu
Chairman

Aina Amah
1st Vice Chairman

Mogbitse Atsagbede
2nd Vice Chairperson

Ugochi Osinigwe
Treasurer

Olusemore Adegbola
Auditor

Olusegun Famoriyo
Chairman, Research & Publication Sub-Comm.

Femi Fatobi
Chairman, Payment & Systems Sub-Comm.

Adeola Awe
Ex-officio I

Olurotimi Omotayo
Ex-officio II

CONTENT

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
Aina Amah
Olusemore Adegbola
Femi Fatobi
Ugochi Osinigwe
Adeola Awe

Editorial

Welcome to the first edition of Eagle Eye magazine for 2024, dedicated to shedding light on critical aspects of auditing, risk management, and data integrity. In this issue, our contributors delve into a spectrum of topics that hold paramount importance in today's dynamic business landscape and the internal audit in particular.

First on the docket is an exploration of "The Role of Internal Auditor in Promoting Stability in the Financial Services Sector and National Economic Growth." As financial ecosystems continue to evolve, understanding the pivotal role of internal auditors becomes imperative in fostering stability and contributing to broader economic prosperity.

In the effort towards address real-world challenges faced by field auditors, we have shared insights into overcoming on-the-job obstacles by Auditors in the course of performing their duties while providing pragmatic solutions to enhance audit efficiency in the article; "Common Challenges Faced by Field Auditors and Recommended Practical Solutions."

The spotlight then shifts to "Common Vulnerabilities and Exposures," addressing vulnerabilities that organizations may face in their audit processes and strategies to fortify against potential threats.

"Continuous Auditing" takes centre-stage, highlighting the importance of adopting continuous auditing practices for proactive risk mitigation and efficient financial oversight.

With the ever-growing threat landscape, we delve into "Cybersecurity: the role of the Board." Our contributor explored the responsibilities of boards in ensuring robust cybersecurity measures, emphasizing the crucial nexus between leadership and cybersecurity resilience.

"Sustainability Reporting Practice" provides a comprehensive overview of reporting practices that align with environmental, social, and governance (ESG) principles. As sustainability gains prominence, organizations must navigate the evolving landscape of responsible reporting.

In the realm of technology, we explore "The Integral Role of Clock Synchronization for Data Integrity and Compliance." The precision of time synchronization becomes a linchpin in maintaining data integrity and adhering to compliance standards while our article on how Eating nuts improves brain health and lowers hear diseases risk is a must read.

Lastly, we have dissected "The Nexus between Pareto Principle and Risk-Based Audit Methodology," exploring how the Pareto Principle can be harnessed to optimize risk-based audit approaches, maximizing efficiency and impact.

We trust that this compilation of articles will offer valuable insights, provoke thoughtful discussions, and equip our readers with the knowledge needed to navigate the intricate landscape of auditing and risk management. Thank you for joining us on this intellectual journey, and we look forward to continuing to be your trusted source for industry knowledge and expertise.

Olusegun Famoriyo
Editor-in-Chief

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

The Role of the Internal Auditor in Promoting Stability in the Financial Services Sector and National Economic Growth

Abstract

The financial services industry is a vital component of the economy that plays significant roles in national economic growth. It provides a range of financial products and services that facilitate economic activity. The financial service industry is continuously changing, and thus, the role of internal auditors in ensuring stability and contributing to economic growth is becoming increasingly significant. Internal auditors play crucial roles in financial institutions by offering impartial and objective evaluations of the institution's operations, risk management, and internal controls. The external auditors are responsible for improving the quality of an organization's governance by providing insights that can guide decision-making and improve the overall performance of the organization vis a vis helps to identify and manage risks to allow financial stability.

Keywords: Financial Services, Internal Auditors, Risk Management and Economic Growth.

Introduction

The financial services industry is one of the major contributors to any country's economic growth. It is responsible for allocating and managing funds, providing loans, and facilitating investments in various businesses and industries. This sector includes banks, investment firms, insurance companies, and other financial institutions. As the financial services sector continues to grow, it creates more job opportunities, fosters innovation, and promotes stability within the economy. Moreover, this sector helps individuals and businesses manage risks, access capital, and achieve their financial goals. In summary, the financial services industry is a vital component of any modern economy which plays a significant role in national economic growth.

The stability of the financial sector is a cornerstone of a nation's economic health, and internal auditors play a pivotal role in ensuring the robustness and integrity of financial institutions. In the face of economic uncertainties and global challenges, the role of internal auditors has become increasingly significant. This discussion explores the multifaceted contributions of internal auditors in fostering stability within the financial sector and, consequently, supporting national economic growth.

The role of an auditor is to evaluate financial records, statements, and processes of businesses, organizations, and government. To provide an independent and objective assessment of

information, to ensure the accuracy, compliance with regulations, adherence to accounting standards, and reliability of financial information. The verification process helps to maintain integrity in financial reporting and provides stakeholders with confidence in the accuracy of the information. The focus is on the overall system of organization, controls, rules, procedures, and regulations set up. Also, this function has been a mechanism for assuring the government, its ministries, and the legislature, that public funds are received, and spent in compliance with appropriations and other relevant laws.

Recently, there has been an increased interest and more emphasis placed on the internal auditors' function. In OECD (Organization for economic cooperation and development) countries, the demand for improved accountability and greater transparency within government has resulted in a call for more information about government programs and services.

According to the Institute of Internal Auditors (IIA), internal auditors are responsible for evaluating and improving the effectiveness of an organization's risk management, control, and governance processes. Their role is critical in maintaining stability by identifying potential risks and weaknesses within the organization and providing recommendations for management to address those issues. Furthermore, internal auditors also aid in ensuring that the organization is compliant with relevant laws and regulations, and financial statements are accurate and reliable. Without internal auditors, organizations may be more prone to fraudulent activities, errors, and other risks that could threaten their stability.

The Companies with a strong internal audit function are less likely to experience fraud. Dezoort et al. (2002).

The presence of internal auditors can positively impact the organization's financial performance. Krishnan et al. (2005).

Based on the foregoing, the importance of internal auditing in maintaining an organization's stability cannot be overemphasized.

Financial instability and economic downturns have been a persistent challenge in many countries across the globe. These crises are influenced by a country's unique historical context and factors specific to their economy. In Nigeria, the most significant economic downturn occurred in the 1980s when the economy of the country was solely relied on oil exports (Monocultural Economy). A sharp drop in oil prices led to a substantial decrease in government revenue and foreign exchange earnings, resulting in a severe economic crisis. This crisis resulted in astronomical inflation rates, high unemployment rates, and a significant decline in the standard of living.

The Nigerian economy has been characterized by structural imbalances, insufficient diversification, and a lack of fiscal discipline, which have contributed to the country's recurring economic crises. Ojo (2019).

The country's vulnerability to commodity price shocks, inadequate regulation, and weak institutions have contributed to Nigeria's economic instability. Other countries have also faced financial instability and economic downturns at various times in their history. Akinlo and Ibhagui (2019).

The Great Depression of the 1930s, for example, affected many countries worldwide, including the United States, Canada, and much of Europe. Similarly, the 2008 global financial crisis, which resulted from the collapse of the US housing market, affected many countries worldwide and led to significant economic challenges.

Financial instability and economic downturns are often caused by factors such as excessive borrowing and lending, inadequate regulation and oversight of financial markets, and economic shocks such as natural disasters or changes in global commodity prices. Understanding the historical context of these crises can help countries develop policies and strategies to mitigate their impact and prevent similar crises from occurring in the future. Helleiner (2014).

Internal Auditor

Internal auditor is an independent, skilled practitioner tasked with the responsibility of delivering quality assurance and consulting activity designed to add value and improve an organization's operations. He helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes through internal audit functions.

The primary role of Internal Auditor is to help the Board and Executive Management to protect the assets, reputation, and sustainability of the organization. He does this by ensuring that all significant risks are identified and reported appropriately to the Board and Executive Management; assessing whether they are adequately controlled; and by challenging Executive Management to improve the effectiveness of governance, risk management and internal controls.

Roles of Internal Auditor

Risk Assessment: To evaluate risks, internal auditors

scrutinize the organization's risk management processes, internal controls, and governance processes. After a detailed evaluation, auditors share the report with the management.

Monitoring Emerging Risks: Auditors are meant to understand the type of risks involved in the company's business dealings so that key risk indicators will be assigned to every business function of the organization; by so doing, emerging risk can be monitored and possibly prevented or worse, mitigate it impact accordingly. Internal auditors are saddled with the responsibility of identifying, assessing, and mitigating risks within financial institutions. By conducting thorough risk assessments, auditors contribute to the development of strategies that safeguard the financial sector from potential threats, ensuring stability in times of economic volatility.

Achieving Business Objectives: Internal auditors ensures that the company achieves excellence in its operations by complying with standard operating policies.

Fraud Prevention, Control, and Cost Management: Internal Auditors facilitate the detection of frauds, losses, and prevention of the same. An auditor is also responsible for checking the validity and authenticity of a company's accounting and statistical records, hence, failure to conduct regular internal audit can increase business exposure to unpredictable risks and potential deterrent.

Internal auditors are at the forefront of detecting and preventing fraudulent activities within financial institutions. By implementing robust internal controls and conducting regular audits, they contribute to the creation of a transparent and trustworthy financial environment, fostering confidence among stakeholders and the public.

Internal auditor executes a systematic and objective approach to examine the books of accounts, statutory records, documents, and the current financial situation of an organization. The Auditors carry out their audit functions with the aim of ensuring both financial and non-financial disclosure of the company meet it true and fair view.

Internal Audit in Financial Services

Internal auditors play a critical role in financial institutions, offering impartial and objective evaluations of the institution's operations, risk management, and internal controls. Their primary objective is to ensure that the institution's systems and processes are effective and efficient while also identifying areas for improvement. Internal auditors have the responsibility of evaluating the adequacy and efficiency of the risk management policies and procedures, identifying, and assessing the risks that the institution faces, and ensuring that the institution's risk management processes are effective in mitigating those risks. Additionally, they also oversee compliance with laws, regulations, and internal policies and procedures and report their findings to top management and the board of directors.

Internal auditors have an essential role in corporate governance by providing reasonable assurance to stakeholders regarding the effectiveness of their organization's internal control systems. Internal auditors are responsible for improving the quality of the organization's governance by providing insights that can guide decision-making and improve the overall performance of the organization. Alzeban and Gwilliam (2014).

Internal auditors ensure the compliance of an organization with relevant laws, regulations, and internal policies and procedures. Ali and Al-Shammari (2016).

Regulatory Framework

The financial sector operates within a complex web of regulations and compliance standards. Internal auditors play a critical role in evaluating the extent to which financial institutions adhere to these regulations. Their diligence ensures that institutions operate ethically, mitigating the risk of legal issues and financial instability.

Regulatory requirements ensure the stability and growth of financial institutions. By laying down guidelines and rules for internal audits, regulatory bodies help financial institutions operate safely and soundly, reducing the probability of financial crises and increasing investor confidence. In Nigeria, for instance, the CBN's regulatory requirements for internal audits help ensure that financial institutions have a strong risk management system and internal control framework in place, which helps prevent fraud, misconduct, and other financial risks that could destabilize the financial system. Similarly, in the United States, the regulatory requirements of the SEC and PCAOB for internal audits of publicly traded companies help ensure that investors have access to trustworthy financial information, increasing investor confidence and promoting economic growth.

The Regulatory requirements have a positive impact on the quality of internal audits. They found that regulatory requirements are positively associated with the quality of internal audits, which in turn, improves financial reporting quality and reduces the likelihood of restatements. Gao et al. (2017).

The regulatory requirements for internal audits can lead to a decrease in fraudulent financial reporting and an increase in the quality of financial reporting, thereby increasing investor confidence and promoting economic growth. Knechel et al. (2016)

Regulatory requirements play a crucial role in preventing market failures and systemic risks that could potentially harm the economy. In the aftermath of the 2008 financial crisis, policymakers across the globe implemented several regulatory measures to prevent such crises from happening again. These measures were aimed at increasing transparency, promoting responsible behavior, and reducing the likelihood of financial institutions engaging in risky behavior that could be detrimental to the economy (Rosenblum, 2011). Furthermore, regulatory requirements are instrumental in promoting transparency and accountability in financial institutions. By mandating financial institutions to establish independent and effective internal audit functions, regulatory bodies ensure that institutions are accountable for their actions and those potential issues identified and addressed promptly (KPMG, 2021).

Financial Reporting Accuracy:

Accurate and reliable financial reporting is vital for maintaining trust in the financial sector. Internal auditors review financial statements to ensure accuracy and compliance with accounting standards. This process enhances the credibility of financial institutions, attracting investors and contributing to economic stability.

Operational Efficiency and Cost Reduction:

Internal auditors assess the operational efficiency of financial institutions, identifying areas for improvement and cost reduction. By enhancing operational effectiveness, auditors contribute to the financial stability of institutions and allowing them to weather economic challenges more effectively.

Strategic Planning and Decision Support:

Internal auditors provide valuable insights to senior management by offering objective assessments of the institution's performance. This information aids strategic planning, enabling financial institutions to make informed decisions that contribute to long-term stability and economic growth.

Technology and Cybersecurity Oversight:

In this era of digital finance, internal auditors are increasingly involved in evaluating technology risks and ensuring robust cybersecurity measures. By safeguarding financial institutions against cyber threats, auditors contribute to the overall stability of the financial sector.

Challenges Faced by Internal Auditors

Internal auditors encounter some hurdles in their efforts to ensure stability within an organization. One of the most common obstacles is maintaining compliance with laws and regulations, which can be challenging when regulations are frequently updated, and compliance requirements are complex and difficult to understand. Another major challenge is ensuring accuracy in financial reporting. Internal auditors must ensure that financial statements are precise and adhere to generally accepted accounting principles. This can be difficult when financial data is inconsistent or when there are issues with financial reporting software.

Lack of resources is one of the most significant potential barriers to achieving internal auditor objectives and maintaining economic growth. Internal auditors often have limited staff and budgets, which can make it challenging to address all the risks facing an organization. Additionally, internal auditors may encounter resistance from management or other stakeholders when attempting to implement changes or address issues. This can be especially difficult when the proposed changes are unpopular or when there are competing priorities.

Internal auditors face several challenges in ensuring compliance with laws and regulations, including the complexity of regulatory environments and the lack of clarity in compliance requirements. Boudreaux and Germane (2020).

Resource constraints can make it difficult for internal auditors to effectively address risks facing an organization. Cai, Zhu, and Wu (2018), likewise, resistance from management and other stakeholders can pose a significant obstacle to internal auditors' efforts to implement changes or address issues. Ruhnke, Schmidt, and Wilke (2017)

Best Practices in Internal Auditing

Effective strategies and best practices for internal auditors to contribute to economic stability and growth include maintaining a strong focus on risk management, especially in critical sectors such as the oil and gas industry and promoting transparency and accountability in government and business. Nigerian internal auditors have successfully implemented these strategies in several instances. For example, the Central Bank of Nigeria (CBN) saved over $3 billion in foreign exchange by implementing a new risk-based supervision framework, which was developed with the help of internal auditors (Okey and Nwosu, 2019).

The Nigerian National Petroleum Corporation

(NNPC) has made significant progress in enhancing transparency and accountability, largely due to the efforts of internal auditors in identifying and addressing financial mismanagement and corruption (Ezeani, 2019).

Another notable example is the Central Bank of Nigeria (CBN), which has an internal audit department.

At the Central Bank of Nigeria (CBN), these auditors play a critical role in ensuring that the bank's financial operations are efficient, effective, and comply with regulatory requirements. They also provide valuable insights into risk management practices and help identify areas for improvement (Igbinedion, 2017).

Access Bank, one of Nigeria's leading financial institutions, has a robust internal audit department

that promotes stability and growth by ensuring that the bank's operations are conducted safely and soundly. The department provides regular reports to the bank's management and board of directors, highlighting areas of concern and making recommendations for improvement (Adegbaju & Fakile, 2016). This is also the culture and practice in Heritage Bank.

Based on foregoing, the roles played by the internal auditors in ensuring the stability and growth of Nigeria's financial system cannot be overemphasized.

Contributions of Internal Audit to National Economic Growth

The financial services industry is an essential component of national economic growth as it provides a range of financial products and services that facilitate economic activity. The sector's stability is crucial for economic growth as it mobilizes savings, manages risk, and allocates capital. Over the past few decades, Nigeria's financial services sector has undergone significant reforms that have led to increased stability and growth. (Adesina & Olajide, 2018)

A stable financial services sector has many direct and indirect benefits for national economic growth. Direct benefits include increased access to credit, improved efficiency in capital allocation, and enhanced financial stability. Indirect benefits include increased investment, job creation, and improved living standards. These benefits are particularly significant for developing countries such as Nigeria, where access to credit and capital is often constrained. (Adegbite et al., 2018)

Internal auditors play a critical role in ensuring these benefits are achieved by providing independent assurance of the effectiveness of internal controls, risk management, and governance processes within financial institutions. Internal auditors help to ensure that financial institutions operate safely and soundly, which promotes financial stability. They also help to identify and manage risks, which is essential for effective capital allocation and financial management. (Adeyemi & Mgbame, 2018)

A study by Adetunji and Adeniji (2019) examined the role of internal audits in the Nigerian financial services sector and found that internal auditors play a critical role in ensuring compliance with regulatory requirements and promoting good corporate governance practices. The study also found that internal auditors help to identify and manage risks, which is essential for maintaining financial stability.

Collaboration with Other Stakeholders

Effective stability and economic growth can be ensured through collaboration between various stakeholders such as internal auditors, regulatory bodies, and others. To evaluate and improve company operations, internal auditors play a critical role, while regulatory bodies ensure compliance with laws and regulations. Working together, these parties can identify potential risks and implement measures to mitigate them. This collaboration can also lead to better decision-making, improved risk management, and increased efficiency, ultimately contributing to overall economic growth. Collaboration between internal auditors and regulatory bodies can also help to enhance transparency and accountability. This can help to build trust and confidence among stakeholders, which is essential for attracting investment and promoting economic stability.

Several Nigerian authors have also emphasized the importance of collaboration between stakeholders in promoting economic growth and stability. Collaboration between the government, private sector, and civil society can enhance economic development in Nigeria. Adeyemi and Opeyemi (2018) while collaboration between stakeholders can lead to better resource allocation, improved service delivery, and enhanced economic growth. Okpanachi and Aboje (2017).

Effective communication with stakeholders is essential for maintaining stability in the financial sector. Internal auditors facilitate transparent communication by providing accurate and timely information about the financial institution's performance, fostering trust among investors, regulators, and the public.

Future Trends of Internal Audit and Recommendations

The financial services industry is constantly changing, and thus, the role of internal auditors in ensuring stability and contributing to economic growth is becoming increasingly significant. In this sector, some noteworthy emerging trends in internal auditing include the utilization of data analytics, greater emphasis on risk management, and the need for auditors to adopt a more strategic mindset. To enhance the position of internal auditors in promoting stability and contributing to economic growth, it is crucial to invest in their professional development. This includes providing continuous training on emerging trends and technologies, as well as encouraging auditors to develop a strategic mindset that goes beyond traditional auditing duties. Additionally, it is necessary to ensure that internal auditors have the required resources and support to carry out their responsibilities effectively, such as access to relevant data and information, and the ability to collaborate with other departments within the organization.

Auditors' professional development plays a crucial role in ensuring effective and efficient internal audit practices in Nigeria's financial sector. Adediji, Adegbite, and Amao (2019).

Data analytics and modern technology have become essential tools for internal auditors to improve the audit processes and enhance the value proposition for Economic growth. Adeniji and Owojori (2020).

Conclusion:

The significant role played by internal auditors in promoting stability and contributing to the growth of the financial service sector and the national economy cannot be overemphasized. The financial services industry is responsible for allocating and managing funds, providing loans, and facilitating investments in various businesses and industries. It creates job opportunities, fosters innovation, and promotes stability within the economy.

Internal auditors are essential in maintaining stability within the financial service sector. They evaluate and enhance an organization's risk management, control, and governance processes. They identify potential risks and weaknesses within the organization and provide recommendations to management to address those issues. Additionally, they ensure that the organization complies with relevant laws and regulations and financial statements are accurate and reliable.

Without internal auditors, organizations may be more vulnerable to fraudulent activities, errors, and other risks that could threaten their stability. Internal auditors play a crucial role in financial institutions by offering impartial and objective evaluations of the institution's operations, risk management, and internal controls. They ensure that the systems and processes are effective and efficient while also identifying areas for improvement.

Internal auditors oversee compliance with laws, regulations, and internal policies and procedures and report their findings to top management and the board of directors. Their primary objective is to ensure that the institution's risk management processes are effective in mitigating those risks and promoting stability within the financial service sector and national economic growth.

The role of internal auditors in promoting stability in the financial sector is indispensable for national economic growth. By actively managing risks, ensuring compliance, detecting fraud, and enhancing operational efficiency, internal auditors contribute to the resilience and credibility of financial institutions. Their efforts go beyond financial reporting to encompass strategic decision-making, cybersecurity oversight, and transparent communication with stakeholders. In this way, internal auditors serve as guardians of stability in the financial sector, playing a vital role in fostering economic growth and prosperity.

References

Adediji, A. A., Adegbite, O. S., & Amao, O. I. (2019). The Impact of Professional Development on Internal Auditing Practice in Nigeria. *Journal of Accounting and Auditing: Research & Practice*, 2019, 1-17.

Akeem Amusa
Heritage Bank Internal Audit

Cybersecurity: The Role of the Board

A three-step process for board directors to start improving cyber- oversight.

In 2016, cybercrime cost U.S. firms more than US$17 million on average, based on a benchmark study of 237 global companies. According to a think- tank report, the global economic losses caused by cyberattacks total an estimated US$445 billion per year. The reason behind it is very simple.

Various studies have estimated that between 70 and 90 percent of organizations and companies around the world just don't have sufficient cybersecurity.

It is the board's problem.

The most common misconception is that cyberattacks are solely the IT department's responsibility. Whereas IT staff is indeed equipped with appropriate tools and experience to deter or mitigate an attack, it's up to the CEO to make the right decisions and take adequate actions. And for that to happen, cybersecurity has to be seen as a board responsibility, and discussions about this topic have to originate from the board.One major problem with boards, however, is that they often don't have sufficient knowledge, tools, and expertise. This is what is often referred to as one of the board's information gaps, prohibiting effective oversight. But directors' lack of knowledge doesn't absolve them of their fiduciary responsibility. In the face of board inaction, the CEO is confronted with a catch-22: In case of a successful cyberattack, the CEO will take the blame, whereas if the cyberattack is unsuccessful, the board will take credit for the proper decentralization of responsibility.

A three-step starting point.

Boards can begin taking ownership of organizational cybersecurity with a three-step process. The steps outlined below will work for nearly all organizations, but their difficulty will vary by sector. Though they may seem basic, very few boards I've come across have done all three.

1) Understand your organization's biggest risks.
2) Conduct a "fire drill".
3) Know what you own.

Understanding cyber risk

Board members usually have not discussed cyber risk with the management team. It is extremely important to have a dedicated discussion that ends with consensus and commitment. The conversation should go beyond the obvious. For example, leaders at manufacturing firms should consider all possible ramifications of supply chain interruptions and communication lapses. After the initial conversation, reassessments should take place on a semi-regular basis.

Here are some general points about cyber risks that may aid exploration:

Risks can stem from an organization's public profile. If a company's operations seem unethical for example, the firm appears to unjustly fire people or act improperly the probability of an attack increases.

Intellectual property is also often a reason for a hack. When a business is rich in R&D, unscrupulous actors competitors, hackers, etc. may mount a cyberattack to get at its secrets.

The top three industries targeted for cyberattacks are healthcare, manufacturing, and financial services. Sony Pictures, Anthem (aninsurance giant) and Target are only three of the better known companies that have been the victim of a cyberattack in recent years.

Fire drills.

One can compare testing a company's cybersecurity functionality to conducting fire drills. In-depth, live testing gives an accurate sense of the organization's vulnerability to, and ability to recover from, cyberattacks.

Phishing emails are still the most common starting point for data breaches. Most people are aware of phishing, but don't realize how easy it is to be taken in by these scams. A good way to signal commitment to cybersecurity is to test board members as a group to see how many of them fall victim to a simulated and targeted phishing attack. Sharing the results with management and employees spreads awareness and reduces embarrassment around the issue. It also makes everyone aware that cybersecurity is a top-level priority.

Over time, organisations can get tougher in enforcing vigilance. For example, Exxon Mobil frequently sends simulated phishing emails to employees. Those who take the bait can have their internet privileges revoked.

Knowing what you own

Often, board directors will unfairly blame IT for cybersecurity failures that actually originate from external sources (vendors, etc.). Boards that perform a cyber-exposure audit for the first time are usually shocked by how much risk resides outside the organization itself.

Exposure in cyberspace is defined by how connected your organization is and what its dependencies are. The more a company relies on third-party software, services, clouds and so on, the more vulnerable it becomes. Visible extranet solutions or integrations between companies are risk factors, too.

Essentially, cyber-exposure means that assets, services, and processes are somehow accessible through public (and not-so-trusted) networks. It is measured by an organization's attack surface. Examples of exposure points:

- Technical assets (networks, systems, online applications)
- People (email, social media, mobile)
- Information flows between systems
- Processes (maintenance, software development, banking transactions)
- Current security measures for each technical asset

Comprehending the sheer scale and dispersal of the risks should help banish the illusion that IT can manage cybersecurity entirely on its own. Directors should then realize that the final responsibility for an all-pervasive and potentially damaging issue rightly belongs with them.

Focusing on the most critical systems and most obvious findings gives you a jump-start. But remember, the only time a change in security happens is when a point of exposure is assessed, and action taken to address the risk.

Writing Excel spreadsheets listing the problems is not going to change anything, security-wise.

Final points to remember.

The consequences of cybercrime are not limited to a one-time financial hit. The fallout can include reputational damage, in-depth regulatory investigations, long and costly litigations, and of course theft of intellectual property, just to name a few. Each of these entails damage to the company that may take years to undo if the company is indeed able to fully recover.

To underline our point: No organisation is ever fully protected from cyberattacks, even those with the best possible safety measures. In 2016, hackers published private information on 20,000 FBI employees. Earlier this year, popular education platform Edmodo fell victim to hackers who obtained access to over 77 million user records. The list of such high-profile breaches is growing at a rate never seen before a trend which is likely to continue.

Culled from: https://knowledge.insead.edu

Continuous Auditing: Can It Supercharge Your Controls and Risk Assessment?

Continuous audit is emerging as an effective strategy for managing and minimizing organizational risk. A few years ago, the Journal of Accountancy noted that organizations "are investing time and money in continuous auditing," but what does this approach mean in practice?
How does continuous audit work? How does a continuous auditing help you mitigate risk, and how can audit management software support you?

What Is Continuous Auditing?

The internal audit process is crucial to an organization's risk management framework. Internal auditors are often known as the "third line of defense" against corporate risk because they provide independent assurance of risk management controls.

The internal audit usually follows a set timetable, a cyclical process to a specific schedule. An auditor or audit team collates data on the adequacy and effectiveness of risks and controls and publishes findings.

Continuous auditing, conversely, is an "always on" audit process.

How Does Continuous Auditing Work?

Rather than a person manually completing audit tasks, a continuous auditing is supported by technology, automatically assessing and delivering findings at very regular intervals. This enables constant risk awareness, auguring the traditional internal audit process and supporting internal audit teams in their work.

When Is Continuous Auditing Used?

Often, continuous audits are focused on repetitive and automated processes or procedures. The continuous auditing process provides a quick and early indication of the procedures' success, unlike traditional internal audits, which can occur months after a business process or activity.

Continuous auditing and monitoring can bolster internal audits in priority areas identified by the business, acting as a second layer of control and assessment for critical processes or functions.

What Are the Benefits of Continuous Audit?

It's worth exploring the advantages and disadvantages of continuous auditing. What are the benefits, and are there any downsides to implementing continuous audit techniques?
Benefits of a continuous audit include:

1. Errors, fraud, or non-compliant activity is immediately detected. Unlike a time-bound audit, the continuous audit process allows any errors, omissions, or fraud to be identified swiftly.
2. As a result, the potential for harm is minimized, making mitigation and remediation easier.
3. The chances of noncompliance are also reduced, minimizing the potential for reputational damage or financial penalties.
4. Audit work can be planned proactively, and auditors' time managed. A key advantage of continuous audits is that peaks and troughs of demand can be avoided, making the audit process more efficient. Besides, it allows for total review of dataset in a population instead of sampling.
5. Up-to-date data is always available. Whether to comply with external reporting requirements or for your internal audit reporting, continuous audit gives you instant access to accurate and current data. Accounts can be prepared faster, and you are assured that their content is watertight.
6. It positions the auditor as a valued business advisor. Continuous audit brings auditors close to business processes and enables the audit team to suggest improvements, tweaks, and remedial actions in a way that timetabled audit does not.

There are significant benefits to implementing a continuous audit process. Are there any disadvantages? Setting up costs can be an obstacle. And as with any technology-led approach, a human overlay will ensure the continuous audit process isn't over-reliant on technology at the expense of common sense. Another disadvantage is that error in system design implementation may not be noticed timely, hence there is need to perform robust quality assurance testing during implementation.

7 Steps to an Effective Continuous Auditing

It's generally accepted that there are six steps to an effective continuous audit process, as recognized in this paper from Rutgers University. In our analysis, we've added a seventh that will help make your continuous monitoring audit more rigorous, robust, and easier.

1. Establish priority areas like KRIs. Look at new procedures and any other processes critical to your business strategy, maybe carrying out a materiality assessment to determine key priorities.
2. Determine the rules for your continuous audit process; the parameters that guide your monitoring. These rules must consider factors like legal or external reporting requirements alongside internal compliance controls.
3. Decide how regular your monitoring will be. "Continuous" is slightly misleading; monitoring is rarely genuinely continuous. The cadence of your monitoring is something you will need to decide. A cost-benefit analysis, and an assessment of how frequently new data is available, will help to determine your monitoring frequency.
4. Monitor and tweak your parameters. Your continuous audit frequency and rules need to be determined before you start. But they should also be revisited once you've continuously audited for a set period. Consider whether your triggers are set at the proper levels; are you overreacting to risks with few costs?
5. Determine your follow-up process. What happens when an error is identified, or an alarm is triggered during the continuous audit process? Who does the alarm flag to? What do they need to do in response? How does the communication process work? Are there steps that should be taken, for instance, to cross-check and verify data before a trigger is acted on? What is the escalation process?
6. Share the results of the continuous audit process. How will you communicate the ongoing findings? At what intervals and via what means?
7. Identify the tools and technologies that can support you. Artificial intelligence, machine learning and robotic processes transform data collection and analysis. Explore their potential to supercharge your data analytics and continuous audit process.

Harness Continuous Audit to Future-Proof Your Audit Process

Internal audit teams must step up as organizations' risk profiles grow more complex and challenging. Moving from time-bound reactive audit processes to at-your-fingertips data and insight means capitalizing on continuous audits' benefits.

Doing this and making the best use of the technologies that can support you, enables internal auditors to play a valued role in corporate governance, acting as a partner to the C-suite and board and proactively tackling emerging risks.

Saliu Braimah
Tajbank Limited

The Integral Role of Clock Synchronization for Data Integrity and Compliance

The synchronization of clocks plays a fundamental role in ensuring seamless operations, accurate record-keeping, and effective collaboration. From multinational corporations to small enterprises, the precision of timekeeping has become a critical aspect of organizational success.

Definition of Clock Synchronization:

Clock synchronization, in a broad sense, refers to the process of aligning the timekeeping of various devices or systems to a common reference point. This ensures that the clocks across the network or organization show consistent and accurate time. The goal is to maintain temporal harmony and eliminate discrepancies between devices.

Importance and Applications:

For internal auditors, understanding the importance of clock synchronization is paramount as it directly impacts various sectors:

1. **Data Integrity and Security**: In sectors like finance and healthcare, accurate timestamping is crucial for maintaining data integrity and ensuring the security of transactions and records.
2. **Network Coordination**: In large-scale enterprises and telecommunications, synchronized clocks facilitate effective communication and coordination, particularly in distributed systems.
3. **Legal Compliance**: Various industries, such as legal and regulatory services, require precise timestamping for compliance purposes and to meet legal obligations.
4. **Log Management and Forensics**: In cybersecurity, synchronized clocks are vital for accurate log management, enabling efficient forensic analysis and investigation of security incidents.
5. **Industrial Automation**: Industries relying on automation, such as manufacturing and energy, depend on synchronized clocks for precise timing of processes and events.

Types of Institutions and Businesses that Require It:
Auditors should recognize the diversity of institutions and businesses that rely on clock synchronization:

1. **Financial Institutions**: Banks, trading platforms, and financial institutions rely on synchronized clocks for accurate transaction timestamps and compliance with regulatory requirements.
2. **Healthcare Organizations**: Hospitals and healthcare providers use synchronized clocks for accurate patient recordkeeping, medication administration, and compliance with healthcare regulations.
3. **Telecommunications**: Telecommunication networks require precise synchronization for the efficient functioning of network elements, ensuring seamless communication.
4. **Manufacturing and Industrial Plants**: Industrial automation processes, including robotics and production lines, depend on synchronized clocks to maintain precise control over manufacturing operations.
5. **Global Enterprises**: Multinational corporations and global enterprises with distributed teams and operations benefit from synchronized clocks for efficient collaboration and data consistency.

Process or Methodology:

Internal Auditors should be familiar with the processes and methodologies employed for clock synchronization:

1. **Network Time Protocol (NTP)**: NTP is a widely adopted protocol for clock synchronization over a network. It utilizes a hierarchical structure of time servers to provide accurate time information to devices. NTP is suitable for a wide range of business scales.
2. **Precision Time Protocol (PTP)**: PTP is designed for applications requiring extremely precise time synchronization, such as industrial automation and financial trading systems. It operates at the microsecond or even nanosecond level.

Best Methods Suited to Business Enterprises:

For internal auditors, recommending the best methods involves considering the specific needs and scale of the business:

1. **Large-Scale Enterprises**: For large-scale enterprises with complex network architectures, a combination of redundant NTP servers and PTP for critical systems may be suitable. This ensures both accuracy and resilience.
2. **Medium-Scale Enterprises**: Medium-scale businesses can benefit from a robust NTP setup with multiple time servers to ensure redundancy and reliability. Regular monitoring and maintenance are essential to uphold accuracy.
3. **Small-Scale Enterprises**: Small-scale enterprises may find a simplified NTP setup

sufficient for their needs. Utilizing reliable NTP servers and configuring devices to synchronize regularly can provide accurate timekeeping.

Conclusion:

In the digital age, where precision and efficiency are paramount, clock synchronization emerges as a foundational element for the smooth functioning of businesses and institutions.

Whether ensuring compliance, facilitating global collaboration, or enhancing data security, synchronized clocks play a pivotal role in shaping the operational landscape of the modern business world.

As technology continues to evolve, businesses of all scales will find that investing in effective clock synchronization is not just a matter of accuracy but a strategic imperative for success.

References:

ISO/IEC 27002: Information security, cybersecurity, and privacy protection Information security controls
https://en.wikipedia.org/wiki/Clock_synchronization
https://www.tfp1.com/blog/the-essence-of-time-importance-of-clock-synchronization-in-buildings-industries/

Fetuga Adekunle
Sterling Bank Plc

Eating nuts, seeds improves brain health, lowers heart diseases risk

Eating more nuts and seeds is good for the brain and lowers the risk of heart diseases as they contain omega-3 fatty acids, powerful antioxidants and anti-inflammatory benefits that help remove toxins from the body and neutralize free radicals effectively, nutritionists say.

They explained that while omega-3 helps curb inflammation in the blood vessels and the rest of the body, the antioxidants protect cells from oxidative stress caused by free radicals.

A 2014 study found that a higher overall nut intake was linked to better brain function in older age, saying that nuts and seeds are also a rich source of the antioxidant, Vitamin E.

A registered Dietician Nutritionist, Olusola Malomo, said adding nuts and seeds as part of one's diet has been linked with a lower risk of heart disease.

He said, "Although high in fats, nuts and seeds are good sources of healthy fats such as monounsaturated and polyunsaturated fats, which are low in unhealthy saturated fats.

"Research has found that frequently eating nuts lowers levels of inflammation related to heart disease and diabetes.

"Nuts like almonds, walnuts, or cashews and seeds such as sunflower seeds, chia seeds, or flaxseeds are great sources of protein, fibre, and healthy fats."

He noted that these classes of food boost the levels of good cholesterol while lowering the bad cholesterol, known to help reduce blood pressure.

"Regularly eating a healthy diet that includes nuts may improve artery health and reduce inflammation related to heart diseases," he added.

Describing antioxidants as compounds in foods that scavenge and neutralise free radicals, Friday Asuqo said, "As a person ages, their brain may be exposed to oxidative stress and vitamin E may support brain health in older age."

He noted that vitamin E in the nuts and seeds may also contribute to improved cognition and reduced risk of diseases that have to do with memory loss.

"The nuts and seeds with the highest amounts of vitamin E include sunflower seeds, almonds and walnuts," he said.

He noted that oxidation in humans damages cell membranes and other structures, including cellular proteins and lipids.

"When oxygen is metabolised, it creates unstable molecules called free radicals, which steal electrons from other molecules, causing damage to DNA and other cells," he added.

Speaking in the same vein, a study published in the *National Library of Medicine*, titled, 'Long-Term Intake Of Nuts In Relation To Cognitive Function In Older Women,' by Okereke Okereke and team, the authors state that higher nut intake may be related to better overall cognition at older ages, and could be an easily-modifiable public health intervention.

The study partly read, "Higher total nut intake over the long term was associated with modestly better cognitive performance at older ages across all three of our cognitive outcomes in this cohort.

"There was a suggestion that walnut intake may be related to better cognitive performance, although it is difficult to draw conclusions since very few women consumed walnuts more than one to three times per month."

Culled from: healthwise.punchng.com

Happy Birthday Distinguished CAEs

Keystone Bank — Jan. 01

Abiodun Okusami

WEMA BANK — Jan. 14

Oluwole Esomojumi

FEDERAL MORTGAGE Federal Mortgage Bank of Nigeria — Feb. 16

Rakiya Bello Umar

FCMB — Feb. 27

Adebowale Oduola

citibank — Feb. 27

Emeka Owoh

POLARIS BANK — March 05

Rotimi Omotayo

RMB — March 07

Femi Fatobi

Optimus Bank — March 22

Adeyinka Oladepo

THE INFRASTRUCTURE BANK PLC — March 23

Sadiku O. Kanabe

Images of the 57th Quarterly General Meeting of the Association held at Four Point by Sheraton, Victoria Island Lagos on December 13th 2023 and hosted by Rand Merchant Bank Nigeria

Images of the 57th Quarterly General Meeting of the Association held at Four Point by Sheraton, Victoria Island Lagos on December 13th 2023 and hosted by Rand Merchant Bank Nigeria

The Nexus between Pareto Principle and Risk Based Audit Methodology

The Nexus between Pareto Principle and Risk Based Audit Methodology

The Pareto Principle, also known as the 80/20 rule, and Risk-Based Audit Methodology are two concepts that can be connected in the context of auditing and risk management. The Pareto Principle is a general principle that suggests that, in many situations, roughly 80% of the effects come from 20% of the causes. In the context of risk-based audit methodology, this principle can be applied to optimize audit efforts and resources. According to Goodwin-Stewart and Kent (2006), internal audit is crucial for tracking a company's risk profile and pinpointing opportunities for better risk management. Through constructive feedback, internal audit aims to improve the organization's performance and efficiency. The risk-based technique establishes a connection between internal audit and the organization's overall risk management structure. Internal auditors use risk-based to verify that all organizational risk management procedures have been followed to properly manage risk. Erlina *et al.* (2020).

The Pareto Principle is a fundamental concept that underscores the uneven distribution of inputs and outputs, with a focus on the vital few elements that have a disproportionately large impact on outcomes. It provides valuable insights for decision-making, resource allocation, and continuous improvement in a wide range of fields and situations. Risk-Based Methodology is a systematic and strategic approach to managing risks within organizations. It allows for the proactive identification, assessment, and mitigation of risks to enhance decision-making, protect organizational objectives, and ensure a more resilient and adaptive approach to challenges and uncertainties.

The Pareto Principle and Risk-Based Audit Methodology should be used as tools in conjunction with other approaches and tailored to the specific needs and circumstances of an organization. When using them, one should take into account their limits as they are not universally applicable solutions.

Concept underlying Pareto Principle

Vilfredo Pareto, an Italian economist, noted in the late 19th Century that 20% of the country's wealth belonged to 80% of its citizens. This observation led to the creation of the Pareto Principle. In verifying this theory, he also discovered that 20% of the population held 80% of the wealth and land in practically all nations (Pareto, 1906). When he looked at his garden, he saw that 20% of the pea pods produced 80% of the peas, further supporting his theory.

The psychologist Joseph Juran developed this theory in the early 1950s, claiming that it might be used in management and even as a "universal principle". He thought that 20% of a company's clients would account for 80% of its revenue, and that 20% of all potential sources of error would account for 80% of production issues. He introduced the words "trivial many" and "useful many" to describe the many contributions that have a minor impact and the few that produce the majority of the effect. Juran (2005).

The 80/20 rule is a concept that is rooted in the observation of unequal distribution of resources and outcomes in various aspects of life. The idea behind the Pareto Principle is that in many situations, a small number of causes are responsible for a large percentage of the effects. In other words, a few key factors contribute most of the impact or results. The Pareto Principle is based on the inequality of inputs and outputs, focus on the vital few, non-linear relationships, applicability in diverse fields, decision-making and resource allocation, continuous improvement, adaptation and context sensitivity.

This principle has been applied to many different fields, from economics to business, from personal productivity to time management. One way to use the Pareto principle in the workplace is to identify the 20% of tasks that are responsible for 80% of the results. This allows individuals and teams to focus their efforts on the tasks that are most important, rather than wasting time on less important tasks. For example, if a sales team determines that 20% of their sales efforts lead to 80% of their revenue, they can prioritize those efforts and allocate resources accordingly. Another way to use the Pareto principle in the workplace is to identify the 20% of employees who are responsible for 80% of the productivity. This allows managers to focus on developing and supporting those high-performing employees, while also addressing any performance issues with the remaining 80% of employees.

The effectiveness of the Pareto Principle in the workplace depends on how it is applied. If used correctly, the principle can help a company prioritize its resources and focus on the areas that will have the greatest impact on its success. However, if used improperly, the principle can lead to a narrow focus on a few key areas while neglecting other important aspects of the business.

To use the Pareto Principle effectively, it's important to first identify the key areas that drive the most value for the organization. Then, the company can focus its resources on those areas while still maintaining a broader perspective on other important aspects of the business. Additionally, the principle can be used to continually evaluate and refine the company's strategies and priorities over time.

The key to applying the 80-20 rule effectively is to understand that it's not just about identifying the 20% of inputs that generate the most results, but also about eliminating or minimizing the other 80% of inputs that don't contribute as much. This requires a focus on priorities and a willingness to let go of activities or tasks that are not as important.

Idea Behind Risk Based Audit Methodology

It is well known that the auditing methodology has changed over the past few years, moving from a system-based audit to a process-based audit and finally to a risk-based audit. Numerous studies on risk-based internal auditing have been conducted in response to the change in auditing methodology. Research by Eshikhati (2012), Kirogo *et al.* (2014), and Nyarombe et al. (2015) are a few among them. Risk-Based Methodology, often referred to as Risk-Based Approach or Risk-Based Thinking, is a

fundamental concept that is widely applied in various fields, including auditing, project management, quality control, and risk management. This methodology is rooted in the principle of identifying, assessing, and managing risks in a systematic and proactive manner.

The core concepts underlying the Risk-Based Methodology include

- **Risk Assessment and Prioritization:** Risk-Based Methodology begins with the identification and assessment of risks associated with a particular activity, process, project, or objective. Risks are evaluated based on their potential impact and likelihood, and then prioritized according to their significance

- **Focus on critical Risks:** The methodology emphasizes focusing resources and efforts on the most critical or high-impact risks. This ensures that attention is directed toward the areas that have the potential to cause the greatest harm or disrupt the achievement of objectives

- **Informed decision making:** The identification and assessment of risks enable organizations to make informed decisions. By understanding the risks involved, they can develop strategies to mitigate, transfer, accept, or avoid these risks, depending on the context and the organization's risk appetite

- **Proactive approach:** Risk-Based Methodology promotes a proactive approach to risk management. Instead of reacting to risks as they arise, organizations anticipate and plan for risks in advance. This helps prevent issues from becoming major problems

- **Continuous monitoring, and adaptability:** Risk management is an ongoing process. The methodology stresses the importance of continuous monitoring and reassessment of risks as circumstances change. This allows for timely adjustments to risk management strategies

- **Integration into processes:** In many cases, Risk-Based Methodology is integrated into various processes and activities within an organization. It becomes part of the organizational culture, ensuring that risks are considered at every stage of decision-making and planning

- **Compliance and regulations** In some industries and sectors, regulatory authorities require organizations to adopt a risk-based approach to ensure compliance with relevant laws and regulations. This is particularly important in fields such as finance, healthcare, and aviation

- **Accountability and Ownership:** The methodology often assigns clear ownership and accountability for the management of identified risks. This ensures that specific individuals or teams are responsible for monitoring and addressing risks

- **Risk tolerance and risk appetite:** Organizations establish risk tolerance and risk appetite levels, which define the degree of risk they are willing to accept. The methodology aligns risk management practices with these established levels

- **Stakeholder involvement:** Engaging stakeholders in the risk assessment and management process is a key element of Risk-Based Methodology. This helps in capturing a broad perspective and considering diverse viewpoints.

Risk-Based Audit Methodology is a widely adopted approach in the field of auditing and risk management, and it is applicable to a variety of organizations and industries. The applicability of risk-based audit methodology is particularly valuable in internal audits, financial audits, compliance audits, IT audits, Operational audits, project audits, fraud audits, non-profit and government audits, supply chain audits, environmental and sustainability audits, health care audits, manufacturing audits etc. Risk-Based Audit Methodology is widely applicable across various industries and types of audits. It helps organizations and auditors prioritize their efforts, allocate resources effectively, and address the most significant risks, ultimately enhancing their ability to achieve their objectives while managing and mitigating potential threats

Nexus between the Pareto Principle and Risk-Based Audit Methodology

The Pareto Principle and Risk-Based Audit Methodology are related in several ways, as they share common principles and objectives, particularly when applied in the context of audit and risk management:

1. **Identifying High-Risk Areas**: The Pareto Principle suggests that roughly 80% of effects come from 20% of causes. In the context of risk management, this means that a small number of risks often account for the majority of potential negative impacts on an organization. Risk-based audit methodology aims to prioritize audit efforts based on the significance and impact of risks. It involves identifying and assessing the most critical risks that can affect an organization's objectives and operations.

2. **Risk Assessment**: The 80/20 rule can guide auditors in identifying the most critical risks that require immediate attention, thereby reducing the likelihood of overlooking significant risks. Risk-Based Audit Methodology involves assessing and prioritizing risks to determine the audit scope.

3. **Resource Allocation:** The Pareto Principle implies that organizations should focus their resources and efforts on the most significant areas or risks to achieve the maximum impact. In a risk-based audit approach, resources are allocated to areas with higher risk exposure. This ensures that audits are focused on areas where the potential consequences of risks are most severe and that resources are used efficiently.

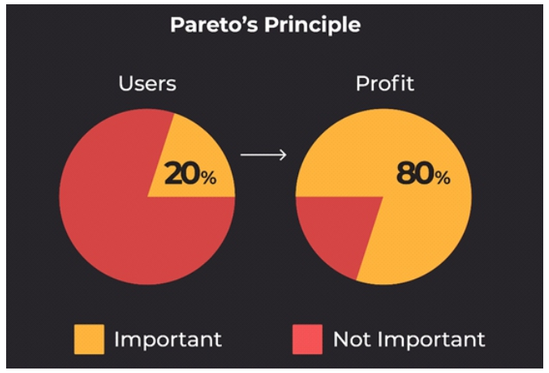
4. **Focus on Materiality**: The Pareto Principle highlights that not all issues or risks are of equal importance. Some have a more significant impact than others. In risk-based audit, materiality is a key concept, and a risk-based approach considers the materiality of risks to prioritize the audit scope and testing. Auditors focus on areas where the potential misstatements or risks are material to financial statements or organizational objectives.

5. **Continuous Monitoring**: The Pareto Principle can also be applied to continuous monitoring and reporting of key areas to maintain effective control and management. A risk-based audit methodology often includes continuous monitoring of risks and controls, particularly those that are most critical. Auditors can continuously track the most critical risks (20%) and report on them more frequently to ensure that timely actions are taken to mitigate those risks.

6. **Focus on Root Causes**: The 80/20 rule encourages organizations to dig deeper into the root causes of significant issues or risks to address them effectively. In a risk-based approach, auditors not only identify high-risk areas but also investigate the root causes and contributing factors behind those risks. This allows organizations to implement corrective actions that address the underlying issues.

Limitations of the Pareto's Principle and Risk Based Audit Methodology

While the Pareto's Principle and Risk-Based Audit



Methodology are valuable concepts in various contexts, they also have limitations. It's important to be aware of these limitations to use them effectively and understand their constraints. Here are some limitations for each.

Limitations of the Pareto Principle (80/20 Rule)

1. **Situational variability**: The actual distribution of inputs and outputs may not always follow an 80/20 ratio. In some cases, it might be 90/10, 70/30, or different proportions. The specific ratio can vary depending on the context.

2. **Context dependency**: The Pareto Principle may not be applicable to all situations. In some cases, there might not be a clear distinction between vital few and trivial many factors. It might not work well in complex, multidimensional systems.

3. **Overlooking less obvious factors**: Focusing solely on the vital few factors can lead to neglecting less obvious or long-term factors that could become critical in the future.

4. **Static view**: The Pareto Principle provides a snapshot view of a situation. It doesn't consider changes over time or the dynamics of evolving circumstances.

5. **Lack of guardian**: It doesn't provide specific guidance on how to address or manage the identified vital few factors, leaving that aspect open for interpretation.

Limitations of Risk-Based Audit Methodology

1. **Subjectivity**: The assessment of risks can be subjective and influenced by the judgment of those conducting the audit. Different auditors may assess the same risks differently.

2. **Data availability**: The effectiveness of risk-based audit methodologies is highly dependent on the availability and quality of data. In some cases, it may be challenging to gather sufficient data for

risk assessments.

3. **Complexity:** Risk assessments in risk-based audits can become complex, particularly in large organizations with diverse operations. Managing the complexity of multiple risks and audit processes can be challenging.

4. **Resource intensive:** Implementing a risk-based audit methodology can require significant resources, including time, personnel, and financial investments. Smaller organizations may find it more challenging to allocate these resources.

5. **Overlooking emerging risks:** The methodology might not adequately address emerging or unknown risks that were not considered in the risk assessment process.

6. **Limited known risk:** It focuses on known risks and may not account for "unknown unknowns" or risks that have not yet been identified.

7. **Risk mitigation effectiveness:** Successfully

identifying risks doesn't guarantee that the risk mitigation strategies will be equally effective. The effectiveness of mitigation measures is contingent on various factors.

Steps to Implementing the Pareto Principle and Risk Based Audit Methodology

Implementing the Pareto Principle and Risk-Based Audit Methodology in an organization requires a structured approach to prioritize efforts, allocate resources effectively, and manage risks efficiently. Here are suggested steps to help you implement these principles:

1. **Understand the organization's objective** - Before implementing these principles, it's crucial to have a clear understanding of the organization's goals, objectives, and key performance indicators (KPIs). This will provide the context for applying the Pareto's Principle and Risk-Based Audit Methodology.

2. **Identify and analyze risks** - Begin by conducting a comprehensive risk assessment. Identify and assess risks that could impact th organization's objectives. Use tools such as risk matrices and risk heat maps to quantify the likelihood and potential impact of these risks.

3. **Apply the Pareto Principle** - Determine which risks are the most critical by applying the Pareto Principle. Typically, you will find that a small percentage of risks have a disproportionate impact on your objectives. Focus on these vital few risks.

4. **Set risk tolerance objective** - Establish clear risk tolerance levels and objectives. Define the acceptable level of risk for each critical risk area to guide decision-making and resource allocation.

5. **Develop a risk-based audit plan** - Based on the risk assessment and the critical risks identified, create a risk-based audit plan. The plan should specify the scope of each audit, objectives, and methodologies to be used.

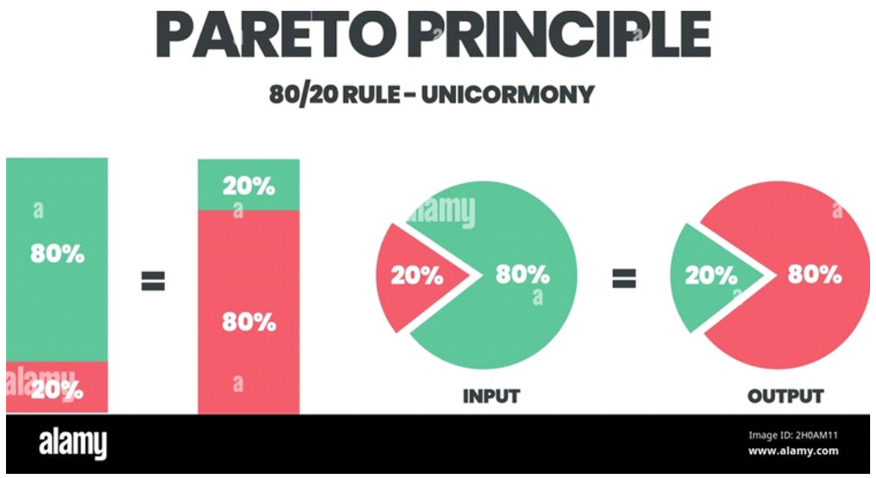
6. **Allocate Resources** - Allocate audit resources and

efforts according to the risk-based audit plan. Concentrate resources on areas with the highest risk exposure, as identified by the Pareto Principle and risk assessment.

7. **Perform Audits** - Conduct audits following the risk-based audit plan. During the audits, focus on the high-impact risks and potential issues that could significantly affect the organization's objectives.

8. **Root cause analysis** - For high-impact risks or issues, perform root cause analysis to understand the underlying factors contributing to the problems. This helps in developing effective corrective actions.

9. **Continuous monitoring** - Implement continuous monitoring and reporting mechanisms to stay up-to-date with changes in risk profiles. Regularly reassess risks and adjust the risk-based audit plan as needed.



10. **Mitigate Risks** - Develop and implement risk mitigation strategies for the identified high-impact risks. Ensure that corrective actions address the root causes and reduce the likelihood and impact of risks.

11. **Communication and reporting** - Effectively communicate audit findings and risk management progress to relevant stakeholders, including management, board members, and employees. Provide recommendations for improvement.

12. **Review and adjust** - Periodically review the effectiveness of the risk-based audit methodology and the application of the Pareto Principle. Adjust the methodology and priorities as needed to align with changing organizational objectives and risk profiles.

13. **Training and skill development** - Invest in the training and skill development of audit teams and employees to ensure they have the knowledge and competencies required for risk-based auditing and risk management.

14. **Stakeholder involvement** - Engage key stakeholders, including senior management, in the risk assessment and decision-making processes. Their input and buy-in are essential for successful implementation.

15. **Compliance and documentation** - Ensure that the implementation aligns with regulatory requirements and is well-documented for transparency and audit trail purposes.

Conclusion and recommendation

Pareto Principle and Risk-Based Audit Methodology are interconnected in the way they can help auditors prioritize and allocate resources, identifying and addressing the most significant risks and promoting efficient and effective management of critical areas. By identifying the 20% of risks that contribute to 80% of the impact, auditors can create a more focused and efficient audit plan that addresses the most critical issues, ultimately enhancing the overall effectiveness of the audit process.

Implementing the Pareto Principle and Risk-Based Audit Methodology should be an ongoing and dynamic process. It should require a cultural shift towards a proactive, risk-aware organizational mindset. By consistently applying these principles, an organization can better manage risks, optimize resource allocation, and enhance its ability to achieve its objectives, while minimizing potential threats. However, it is important to note that Pareto Principle and Risk-Based Audit Methodology are not one-size-fits-all solutions, and their limitations should be considered when applying them.

Emeke Emuebie, Internal Audit department, Union Bank of Nigeria PLC

Common Challenges Faced by Field Auditors and Recommended Practical Solutions

Field auditors face various challenges in their work, and addressing these challenges requires practical solutions. Here are common challenges faced by field auditors along with recommended practical solutions:

1 **Limited Access to Information:**

Challenge: Difficulty accessing relevant information in real-time.

Solution: Implement mobile auditing tools that allow auditors to access data on-site.

2 **Inadequate Training**

Challenge: Lack of proper training on auditing tools and methodologies.

Solution: Provide regular training sessions and workshops to keep auditors updated on best practices and tools.

3 **Time Constraints**:

Challenge: Limited time for field audits, leading to rushed assessments.

Solution: Optimize audit processes, focus on critical areas, and provide adequate resources to streamline the audit timeline.

4 **Communication Barriers**:

Challenge: Difficulty in communicating findings and recommendations effectively.

Solution: Use clear and concise language in reports, and provide training on effective communication skills.

5 **Data Accuracy Issues**:

Challenge: Inaccurate or incomplete data affecting audit results.

Solution: Implement data validation checks and ensure auditors verify information at the source.

6 **Lack of Technology Integration**:

Challenge: Outdated or inefficient technology tools.

Solution: Invest in modern audit management software and ensure seamless integration with other systems.

7 **Resistance from Auditees**:

Challenge: Resistance or lack of cooperation from the entities being audited.

Solution: Establish positive relationships, communicate the benefits of the audit, and involve auditees in the process.

8 **Risk Assessment Challenges**:

Challenge: Difficulty in accurately assessing and prioritizing risks.

Solution: Implement a robust risk assessment framework and collaborate with risk management experts.

9 **Regulatory Changes**:

Challenge: Keeping up with constantly changing regulations.

Solution: Establish a system to monitor and adapt to regulatory changes promptly.

10 **Inadequate Resources**:

Challenge: Limited resources, including staffing and budget constraints.

Solution: Prioritize audits based on risk, allocate resources efficiently, and advocate for increased budget when necessary.

11 **Document Management Issues:**

Challenge: Inefficient documentation processes leading to errors.

Solution: Implement a centralized document management system and provide training on proper documentation practices.

12 **Remote Auditing Challenges**:

Challenge: Difficulty conducting audits remotely.

Solution: Utilize video conferencing tools, secure data transmission methods, and establish clear remote auditing protocols.

13 **Audit Trail Security**:

Challenge: Ensuring the security of audit trails and evidence.

Solution: Implement encryption, access controls, and regular security audits of the audit trail system.

14 **Fraud Detection Challenges**:

Challenge: Identifying and detecting fraudulent activities.

Solution: Utilize data analytics tools and collaborate with forensic experts for advanced fraud detection.

15 **Language Barriers**:

Challenge: Language differences impacting communication.

Solution: Provide language training or use translation services as needed.

16 **Audit Report Quality**:

Challenge: Producing comprehensive and clear audit reports.

Solution: Develop standardized report templates and conduct quality reviews before finalizing reports.

17 **Insufficient Follow-up**:

Challenge: Lack of follow-up on audit recommendations.

Solution: Establish a monitoring system to track the implementation of audit recommendations and report progress.

18 **Cultural Sensitivity**:

Challenge: Cultural differences impacting the audit process.

Solution: Train auditors in cultural sensitivity and adapt audit approaches accordingly.

19 Scope Creep:

Challenge: Expanding scope without proper assessment.

Solution: Clearly define and communicate the audit scope, and obtain approval for any scope changes.

20 Data Privacy Concerns:

Challenge: Ensuring compliance with data privacy regulations.

Solution: Implement strong data protection measures, including anonymization and encryption, and stay informed about evolving privacy laws.

21 Inadequate Sampling Techniques:

Challenge: Inaccurate sampling leading to unreliable results.

Solution: Train auditors in statistical sampling techniques and ensure adherence to best practices.

22 Audit Independence:

Challenge: Maintaining independence from the entities being audited.

Solution: Establish and enforce policies to ensure auditors' independence and objectivity.

23 Resource Allocation:

Challenge: Allocating resources effectively across multiple audits.

Solution: Prioritize audits based on risk and allocate resources proportionally.

24 Lack of Continuous Monitoring:

Challenge: Relying solely on periodic audits.
Solution: Implement continuous monitoring tools and processes to detect issues in real-time.

25 Environmental Challenges:

Challenge: Weather and environmental conditions affecting on-site audits.

Solution: Plan audits considering environmental factors and provide necessary equipment and support.

26 Technology Reliability:

Challenge: Dependence on technology with potential technical glitches.

Solution: Have backup systems in place, conduct regular technology audits, and provide technical support.

27 Knowledge Transfer:

Challenge: Difficulty transferring knowledge within the audit team.
Solution: Establish knowledge-sharing sessions and documentation processes to ensure information is passed on effectively.

28 **Stakeholder Communication**:

Challenge: Ineffective communication with key stakeholders.

Solution: Develop a communication plan, including regular updates and feedback sessions with stakeholders.

29 **Audit Evidence Collection**:

Challenge: Difficulty in collecting sufficient and relevant evidence.

Solution: Standardize evidence collection procedures and provide training on effective evidence gathering.

30 **Ethical Dilemmas**:

Challenge: Facing ethical dilemmas during the audit process.

Solution: Establish a code of ethics, provide ethics training, and create a reporting mechanism for ethical concerns.

Conclusion

Addressing these challenges requires a combination of technology, training, communication, and process improvements. Regularly reviewing and updating strategies based on evolving circumstances will contribute to the effectiveness of field audits.

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

Common Vulnerabilities and Exposure (CVE)

CVE Background

Before Common Vulnerabilities and Exposure (CVE) was started in 1999, it was very difficult to share data on vulnerabilities across different databases and tools. Each vendor maintained their own database, with their own identification system and different sets of attributes for each vulnerability. CVE ensures that every tool can exchange data with other tools, while also providing a mechanism by which different tools, such as vulnerability scanners, can be compared.

While some may question whether publicly disclosing vulnerabilities makes it easier for hackers to exploit those vulnerabilities, it is generally accepted that the benefits outweigh the risks. CVE includes only publicly known security exposures and vulnerabilities. This means that hackers could get their hands on data related to the CVE whether it is in the CVE list or not. Additionally, details of a CVE are often withheld from the vulnerability list until the corresponding vendor can issue a patch or other fix, ensuring that enterprises can protect themselves once the information is made public. Additionally, information sharing across the cybersecurity industry can help speed mitigations, as well as ensure that all organizations are protected more quickly than if left to identify and find resolutions to CVEs on their own.

What Is a CVE?

Common Vulnerabilities and Exposures (CVE) is a database of publicly disclosed information security issues that has been assigned a CVE ID number. A CVE number uniquely identifies one vulnerability from the list. CVE provides a convenient, reliable way for vendors, enterprises, academics, and all other interested parties to exchange information about cyber security issues. CVEs help IT professionals coordinate their efforts to prioritize and address these vulnerabilities to make computer systems more secure. Enterprises typically use CVE, and corresponding CVSS scores, for planning and prioritization in their vulnerability management programs.

CVE was launched in 1999, and is managed and maintained by the National Cybersecurity FFRDC (Federally Funded Research and Development Center), operated by the MITRE Corporation. CVE is sponsored by the US Federal Government, with both the US Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA) contributing operating funds. CVE is publicly available and free for anyone to use.

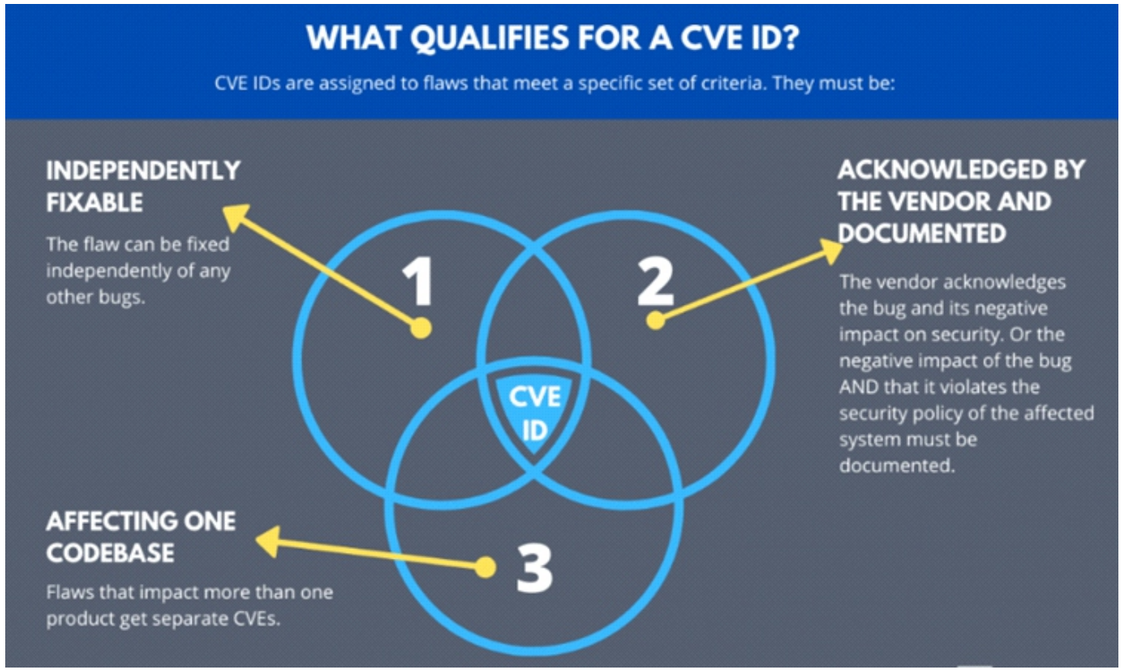
Understanding CVE Identifiers

Every CVE is assigned a number known as a CVE Identifier. CVE identifiers are assigned by one of around 100 CVE Numbering Authorities (CNAs). CNAs include IT vendors, research organizations like universities, security companies, and even MITRE themselves.

A CVE identifier takes the form of CVE-[Year]-[Number]. Year represents the year in which the vulnerability was reported. The number is a

sequential number assigned by the CNA.

For example, CVE-2019-0708, corresponds to a flaw in Microsoft's Remote Desktop Protocol (RDP) implementation. While CVE-2019-0709 might not sound familiar, you might recognize the common name given to this CVE, BlueKeep. Infamous CVEs, like BlueKeep, that get a lot of enterprise (and press)



attention commonly get an informal nickname as an easy way to remember the vulnerability in question. A select few CVEs even get their own cool custom logo or graphic (often designed by the marketing teams at the vendor or organization looking to publicize information on the vulnerability to attract journalist interest).

Difference Between a Vulnerability and an Exposure

A vulnerability is a weakness which can be exploited to gain unauthorized access to or perform unauthorized actions on a computer system. Vulnerabilities can allow attackers to get direct access to a system or a network, run code, install malware, and access internal systems to steal, destroy, or modify sensitive data. If it goes undetected, it could allow an attacker to pose as a super-user or system administrator with full access privileges.

An exposure is a mistake that gives an attacker access to a system or network. Exposures can allow attackers to access personally identifiable information (PII) and exfiltrate it. Some of the biggest data breaches were caused by accidental exposure rather than sophisticated cyber attacks.

How Are CVEs Determined?

CVE IDs are assigned to flaws that meet a specific set of criteria. They must be fixed independently of any other bugs, they must be acknowledged by the vendor as having a negative impact on security, and they must be affecting only one codebase. Flaws that impact more than one product get separate CVEs.

Who Reports CVEs?

Anyone can report a CVE to a CNA. Most commonly, researchers, white hat hackers, and vendors find and submit CVE reports to one of the CNAs. Many vendors actively encourage people to seek out vulnerabilities as a "free" way to improve upon the security posture of their products. In fact, many even offer bug bounties and other forms of contests and prizes to encourage the community to test, and find the flaws in, the security of their products.
The full list of CNAs includes many household names, including MITRE, Adobe, Apple, CERT, Cisco, Dell, Facebook, Google, IBM, Intel, and more.

Benefits of CVEs

- The program's main purpose is to standardize the way each known vulnerability or exposure is identified, allowing security administrators to access technical information about a specific threat across multiple CVE-compatible information sources.
- Sharing CVE details is beneficial to all organizations it allows organizations to set a baseline for evaluating the coverage of their security tools. CVE numbers allow organizations to see what each tool covers and how appropriate they are for your organization.
- By using the CVE ID for a particular vulnerability or exposure, organizations can quickly and accurately obtain information about it from a variety of information sources and coordinate their efforts to (prioritize and address these vulnerabilities to their organizations more secure.

wallarm

Common Vulnerabilities and Exposures

- Security advisories can use CVE vulnerability details to search for known attack signatures to identify particular vulnerability exploits.

What are the Limitations of CVE?

CVE is not meant to be a vulnerability database, so (by design) it does not contain some of the information needed to run a comprehensive vulnerability management program. In addition to the CVE identifier, the CVE entry includes only a brief description of the security vulnerability, and references to more information about the CVE, such as vendor advisories.

Additional information on each CVE can be found directly on vendor websites, as well as in the National Institute for Standards and Technology (NIST) National Vulnerability Database (NVD). The NVD provides CVSS Based Scores, fix information, and other important details often needed by information security teams that want to mitigate the vulnerability or assess its overall priority.

Additionally, CVE represents vulnerabilities in unpatched software only. While traditional vulnerability management programs viewed unpatched software as the primary issue for resolution, modern, risk-based approaches to vulnerability management recognize that there are many types of "vulnerabilities" introducing risk to an organization, all of which need to be identified and mitigated. Many of these do not fit the definition of a CVE and cannot be found in the CVE security list.

Three key takeaways

Know your deployments. Just because a CVE exists doesn't mean the risk applies to your specific environment and deployment. Be sure to read each CVE and understand if it applies to your environment by validating that it applies (or partially applies) to the operating system, application, modules, and configurations of your unique environment.

Practice vulnerability management. Vulnerability management is a repeatable process to identify, classify, prioritize, remediate, and mitigate vulnerabilities. This means understanding how a risk would apply to your organization so you can properly prioritize any outstanding vulnerabilities that need to be addressed.

Be ready to communicate. CVEs will impact your organization's systems, both because of the vulnerabilities themselves and any potential downtime required to address them. Communicate and coordinate with your internal customers and share the vulnerabilities with any central risk management function within your organization.

References

https://www.balbix.com/insights/what-is-a-cve/

https://www.redhat.com/en/topics/security/what-is-cve

Contributed by: Oluwasegun Onasanya (ProvidusBank Ltd)

Oluwasegun Onasanyan
ProvidusBank Limited

Emerging Trends In Audit Quality Assurance: What Auditors Need To Know

In the dynamic landscape of financial reporting and regulatory requirements, auditors play a crucial role in ensuring the reliability and accuracy of financial information. With the ever-evolving business environment, auditors need to stay abreast with emerging trends in audit quality assurance to maintain the highest standards of professionalism and effectiveness. This article, enumerate some of the key trends shaping the future of audit quality assurance.

In January 2022, several emerging trends in audit quality assurance were noted. However, the landscape keeps evolving even after then. Here are some key emerging trends observed:

I. Technology Integration:

Data Analytics and Artificial Intelligence: Auditors were increasingly incorporating data analytics and artificial intelligence into processes to enhance the efficiency and effectiveness of audits.

Blockchain Technology: As blockchain gained prominence, auditors continue to explore and leveraging on the use of Blockchain Technology to further support transparency and traceability on financial transactions.

ii. Remote Auditing:

The COVID-19 pandemic accelerated the adoption of remote auditing practices. Auditors were leveraging on technology to perform audits remotely, leading to a shift in traditional audit approach to system base.

iii. Focus on Cybersecurity:

With the increasing frequency and sophistication of cyber threats, auditors now pay more attention and greater emphasis on cybersecurity on client systems and financial data.

iv. Regulatory Changes:

Regulatory bodies continue to update standards and requirements to keep pace with the evolving business environment and the associated emerging risks. Auditors needs to stay informed and adapt processes mandated by the regulators t through circulars, pronouncement, and guidelines.

v. Audit Quality Indicators (AQIs):

There was a push towards developing and using audit quality indicators to measure and monitor the effectiveness of audit processes. These indicators aimed to provide insights into the quality of audits performed by firms.

vi. Environmental, Social, and Governance (ESG) Considerations:

Auditors continue to incorporate ESG factors into audit processes. This involved assessing the impact of environmental, social, and governance issues on the financial performance of reporting entities.

vii. Focus on Professional Development:

Continuous professional development and training were crucial for auditors to stay updated on industry trends, technological advancements, and regulatory changes.

viii. Audit Firm Culture and Governance:
There was a heightened focus on the culture and governance within firms. Strong ethical culture and effective governance structures were seen as essential for maintaining audit quality.

ix. Extended External Reporting (EER):

Auditors were extending their focus beyond traditional financial reporting to include a broader range of information in their audits, such as non-financial and sustainability reporting.

It's important to check for latest developments in the area of audit quality assurance, as the industry is dynamic, and new trends continue to be emerged.

x. Data Analytics and Continuous Monitoring:

The traditional audit model involved periodic assessments of financial data. However, the emerging trend emphasizes continuous monitoring through the use of data analytics. Auditors are now leveraging advanced on analytics to analyze vast datasets in real-time, enabling the auditors to detect anomalies and potential risks promptly. Continuous monitoring enhances audit quality by providing a more comprehensive and up-to-date picture of an organization's financial health.

xi. Focus on Cybersecurity:

As businesses become more reliant on digitalization and cloud computing, the cybersecurity threats have escalated. Audit quality assurance now extends to assessing an organization's cybersecurity controls. Auditors must be well-versed in evaluating the effectiveness of cybersecurity measures put in place and understand the potential impact of cyber threats on financial reporting. This trend reconfirmed the fact that cybersecurity is an integral part of the overall business integrity.

xii. Enhanced Professional Skepticism:

Professional sceptical is one of the fundamental aspects of auditing, and recent trends highlight the importance of professional scepticisms. Auditors are encouraged to critically evaluate management representations, assess the reasonableness of estimates, and challenge assumptions. This heightened skepticism is crucial for uncovering potential misstatements and ensuring the reliability of financial statements.

xiii. Regulatory Changes and Global Harmonization:

The regulatory landscape for auditing is constantly evolving, with regulatory bodies around the world updating standards and requirements. Auditors need to stay informed about these changes to ensure compliance and uphold audit quality. Furthermore, there is an increasing emphasis on global harmonization of auditing standards, with efforts to create a consistent framework that transcends national boundaries. Auditors must be aware of these global initiatives and adapt the practices accordingly.

Conclusion:

The audit profession is undergoing a transformative phase with emergence trends in audit quality assurance. Auditors must continue to embrace these changes in other to stay relevant and effective in an increasingly complex business environment. By integrating technology, focusing on continuous monitoring, addressing cybersecurity risks, maintaining professional skepticism, and staying abreast of regulatory developments, auditors can contribute to the enhancement of audit quality and, ultimately, the reliability of financial information. In this rapidly evolving landscape.

In summary, auditors need to be at breast with emerging trends, leverage on technology, and maintain highest standards of professional conduct, continuous training, and adopt proactive approach to audit processes, adopting of new methodologies and tools are essential in the ever-evolving field of auditing.

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

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

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

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

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

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

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

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

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

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

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

Fidelity Bank Plc
Ugochi Osinigwe
Fidelity Bank Plc.
2, Adeyemo Alakija Street, 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
081291456605

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 Akinnoye
Niger House (6/7 foors)
1/5 Odunlami St, Lagos
dakinnuoye@fsdhgroup.com
08022017090

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

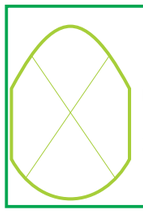
Greenwich Merchant Bank Ltd
Rasaq Alawode
Plot 1698A Oyin Jolayemi Street,
Victoria Island, Lagos
rasaq.alawode@greenwichbank
group.com
08083248797

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

Heritage Bank Ltd
Kikanwa Akpenyi
130, Ahmadu Bello Way,
Victoria Island, Lagos
kikanwa.akpenyi@hbng.com
08023184022

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

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



Lotusbank

Adeola Hopewell Street,
Victoria Island, Lagos.

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

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

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

Nova Merchant Bank
Sele Gyang
23, Kofo Abayomi Street
Victoria Island, Lagos.
Sele.gyang@novambl.ocm
08033228437

Optimus Bank
Adeyinka Oladepo
55, Bishop Oluwole Street,
Victoria Island, Lagos
adayinka.oladepo@optimusbank.com
07035316372

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

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

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

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

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

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

Standard Chartered Bank Nig. Ltd.
Prince Akamadu
142, Ahmadu Bello Way
Victoria Island, Lagos
Prince.akamadu@sc.com
08037649757

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

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

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

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

Union Bank of Nigeria Plc
Victor Ikeneku
36 Marina,
Lagos.
Voikeneku@unionbankng.com
08033338100

United Bank for Africa Plc
Mercy Okwara
UBA House
57 Marina, Lagos
Mercy.okwara@ubagroup.com
08039165569

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

Wema Bank Plc.
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