Association of Chief Audit Executives of Banks in Nigeria

Design+printbyProwess08039221516

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

Eagle Eye

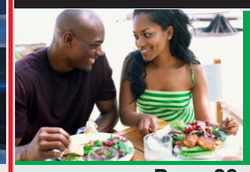
A Quarterly Publication of the Association of Chief Audit Executives of Banks in Nigeria (ACAEBIN) Q4, 2020

OPERATIONALIZING THE NEW 3 LINES OF DEFENCE

Security and Compliance: What to Expect in 2021

Page 10

Wellness



7 Diet Decisions You Can Make To Live Longer.

Page 28

The Role of IT Governance in Addressing Pandemic-Related Cyberrisk

Page 31

ACAEBIN EXCO MEMBERS

Yinka Tiamiyu
(Chairman)

Uduak Nelson Udoh
(1st Vice Chairman)

Felix Igbinosa
(2nd Vice Chairman)

Gboyega Sadiq
(Treasurer)

Aina Amah
(Auditor)

Prince Akamadu
(Chairman Research & Publication)

Adekunle Onitiri
(Chairman Payment & Systems)

Dele Dopemu
(Ex-officio I)

Samuel Ekanem
(Ex-officio II)

CONTENT

Editorial

It has been an interesting year to put it mildly but the fact that you are reading the fourth copy of your favourite quarterly professional magazine is testimony of God's faithfulness. Welcome to the final edition in year 2020.

In this publication, we have an article culled from ISACA on securing Work-From-Home (WFH) devices. The outbreak of the COVID-19 pandemic resulted in lockdown measures that were imposed to contain the spread of the virus, which included a freeze on commuting to the office to work in person for almost everyone but essential workers. This posed some challenges. While the author concedes that it is not humanly possible to exhaust all alternatives when planning for business continuity, there is a need to find a balance between available services and security. You may wish to read the full article for the author's recommended tips that can be considered as part of aligning objectives to security requirements:

Our article from IIA opines that during these unprecedented COVID-19 times, internal audit also faces challenges to modernize practices, processes, and methodologies amid today's digital age. As organizations continue to adjust their business models and operations with a digital mindset, internal audit must innovate and transform itself into an agile, multi-skilled, and technology-enabled function. The author is of the opinion that while many CAEs have amassed goodwill by demonstrating internal audit's value in response to COVID-19, they can enhance their standing further by adopting next-generation audit practices that include dynamic risk assessments. Finally, Chief Audit Executives (CAEs) need to respond to the emerging needs and new strategies of management and the board. When doing this, they must ensure the information they are communicating is timely and relevant.

Have you got what it takes to be a good auditor? This is the question that the author of the article on the 'the characteristics of a good auditor set out to answer even as he argues that attaining and maintaining the characteristics mentioned in the article require personal commitment which are crucial to the auditor's long-term success.

In this edition also is an article- **An Overview of IoT and the Audit Perspective** which chronicles the history and the risk associated with IoT, delves into ISACA's established process for Auditing IoT. The author concludes that such audits determine whether IT controls protect corporate assets, ensure data integrity and are aligned with the business's overall goals.

Modern organizations generally recognize the risk of employees having interests that conflict with the interests of the organization, itself. These conflicts not only affect internal auditors but all employees of the organization. We have an interesting article that addresses the challenge that conflicts of interest can be difficult to identify, manage, and audit.

As usual, we have other articles including those on lifestyles and health that you will find very educative.

Finally, permit me to wish us all great yuletide and Covid-free 2021 even as I express profound gratitude to the entire Research and Publications Sub-committee.

Thank you.

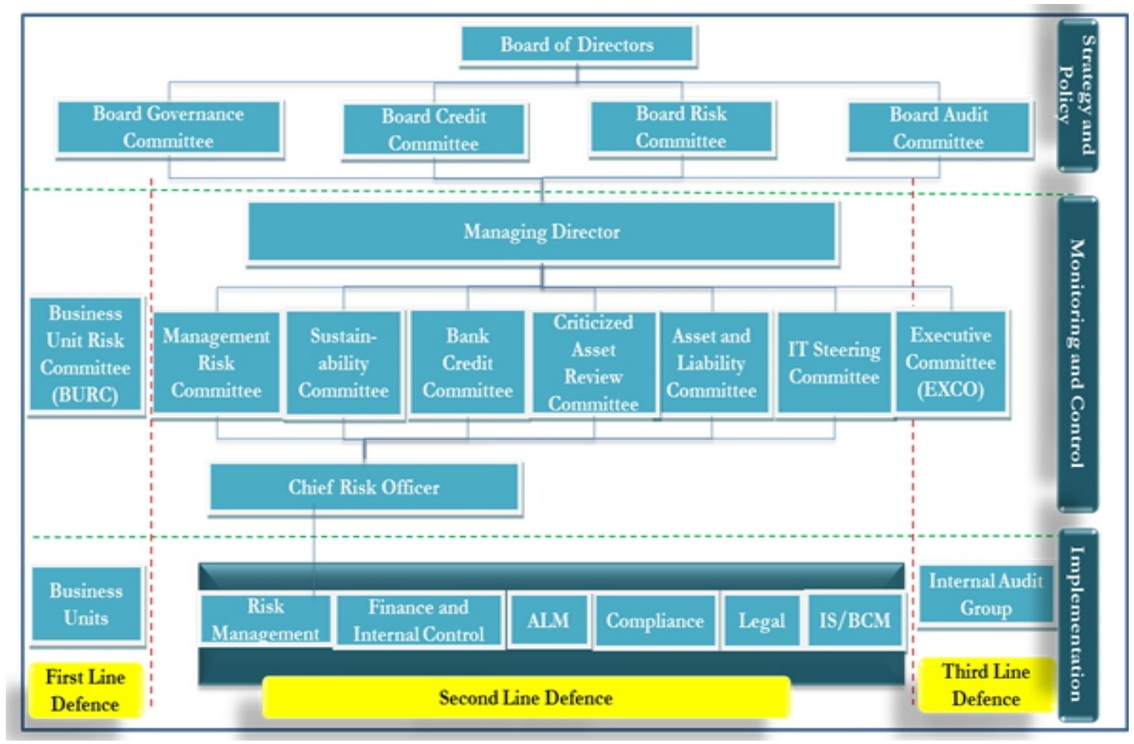
Prince Akamadu
Editor-in-Chief

OPERATIONALIZING THE NEW 3 LINES OF DEFENCE

Considering rapid changes, unprecedented new risks, and the growing complexity of organizations; the Institute of Internal Auditors (IIA) in collaboration with specialists in governance and risk management from around the world, introduced a major update to the widely accepted Three Lines of Defence Model in July 2020. The 3 lines model has been widely accepted over the years in organizing governance and risk management in organizations including interaction and responsibilities of key stakeholders. The update encourages organizations to determine appropriate, pragmatic structures for themselves, taking into account their objectives and circumstances against a backdrop of an ever-evolving risk landscape.

In the earlier Enterprise Risk Management model, the three lines of defense were represented by management control as the first line, risk and control monitoring as the second, and independent assurance through the internal audit function as the third. i.e **based on departmental functions.** A notable criticism of the model was its emphasis on defensive actions at the detriment of a more proactive approach to identification , analysis and preparedness for both opportunities and threats; as practiced in modern organizations.

Figure 1: Enterprise Risk Governance Structure



The new model emphasizes a **principles-based** approach and is designed to better identify and structure interactions and responsibilities of management, internal audit, and those charged with governance to achieve more effective alignment, collaboration, accountability, and objectives. It focuses on adapting the model to suit organizational objectives and circumstances. Roles are clearly defined in the new model for various leaders within an organization, including oversight by the board or governing body; management and operational leaders including risk and compliance (first- and second-line roles); and independent assurance through internal audit (third-line role). Its essence therefore is to broaden the scope of the model to include value creation.

The position of external assurance providers is also addressed. The new model emphasizes six principles related to governance, governing body roles, management and first- and second-line roles, third-line roles, third-line independence, and creating and protecting value. The new model applies to all organizations, which can optimize the new approach by:

- ✓ Focusing on the contribution risk management makes to achieving objectives and creating value, as well as to matters of "defense" and protecting value.
- ✓ Clearly understanding the roles and responsibilities represented in the model and the relationships among them.
- ✓ Implementing measures to ensure that activities and objectives are aligned with the prioritized interests of stakeholders.

The expected close collaboration should not result in blurring of the lines, conflicting roles or shirking of responsibilities by any of the roles. Given the new paradigm in which the responsibilities of Internal Audit extends from traditional provision of assurance (on governance, risk and controls) to engagement in consulting activities, it becomes imperative to instill checks so that Internal Audit would be able to fulfil its mandate.

Effective implementation

Those charged with governance can ensure that an organisation gets the full benefit of the 3 lines of defence by a well thought out implementation process. First, the organization should develop and ensure proper documentation of the risk framework. This should draw from regulatory standards and best

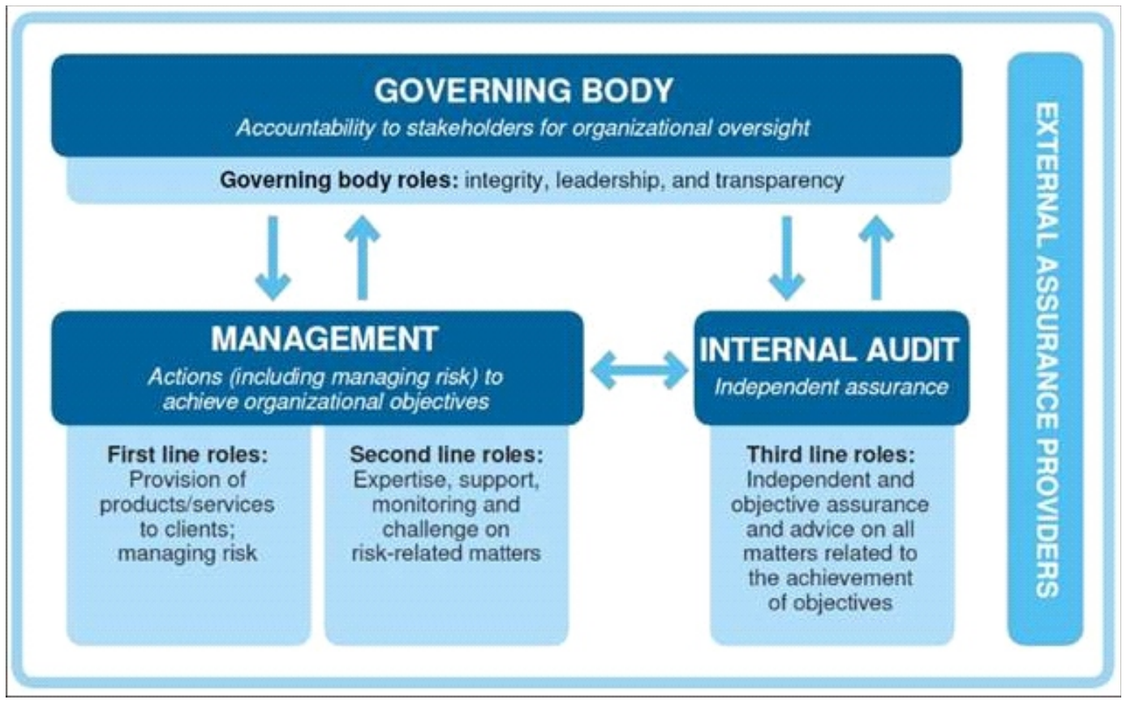
practices. The testing performed at each line of defence should be aligned with the risk framework. Care should be taken to identify any shortcomings and overlaps in responsibilities, for necessary corrections and optimality. It is important to ascertain the level of confidence that can be placed on a line of defence by the other lines. A proper analysis would also result in identification of opportunities and streamlining of responsibilities. Management would thus be able to deploy the most appropriate structure and resources within their organizations to preserve and enhance value.

It would be advantageous to minimize audit fatigue in the organization and enable the front lines of defence to concentrate on serving customers and improve the effectiveness of the 2nd and 3rd lines of defence. The other stakeholders/business units typically are unable to properly distinguish Audit's role from that of the other assurance services especially when similar requests are made from them or similar methodologies are applied in carrying out the different roles.

This underscores the need for painstaking development and testing of risk methodologies by Management.

The three lines should adopt a collaborative approach to governance, risk and controls. Internal Audit should take interest in the ability of the first two lines of defence to play their roles as well, and follow up on steps being taken to empower and fortify them. This would ensure that Internal Audit is noy bogged down with operational activities or with filling their roles due to incapacitation of operational and control functionalities.
In summary, please see the differences in the original one (ERM) and the new /IIA's model below: Internal Audit

Figure 2: IIA's 3 lines of defence



rather than standing next to the 2nd line of defence without indicating interaction with all other functionalities is now shown in the diagram as giving and receiving feedbacks across all functionalities; and adequately engaging them all. There is also a role for external assurance providers which is not in the traditional Enterprise Risk Management /Governance Framework. The 3 roles are now shown to operate **concurrently** rather than appearing **sequential**. It is worthy of note also that the new model summarizes the specific functions expected from each of the 3 lines, which is absent in the earlier one.

Michael Ajuyah
Internal Audit
Ecobank Nigeria Ltd

Adapting to the Dynamic Risk Environment

Internal audit needs to move beyond analogue processes to assess risks in a digital world.

COVID-19 has disrupted business operations worldwide. Offices sit empty as many employees continue to work remotely. Considering the fact, that many organizations may offer remote working as a permanent option for some employees, business would not return to the old normal anytime soon, if ever.

During these unprecedented times, internal audit also faces challenges to modernize practices, processes, and methodologies amid today's digital age. As organizations continue to adjust their business models and operations with a digital mindset, internal audit must innovate and transform itself into an agile, multi-skilled, and technology-enabled function. It must become a “next-generation” function that can recognize emerging risks and changes to the organization's risk profile quickly and efficiently and incorporate them into the audit plan timely. This requires a dynamic risk assessment process.

From Static to Dynamic

The risk management methodologies most organizations have in place today were developed before the turn of the century. In effect, risk management is frequently an analog approach being applied in what is now a digital world.

Organizations need to do more to embed deeper and more insightful risk information in strategy-setting, performance management, and decision-making processes. Twenty-first century advances of digital, cloud, mobile, and visualization technologies; exponential growth in computing power; and advanced analytics can help elevate organizations' risk management capabilities.

Internal audit can be part of the change by transitioning to a dynamic risk assessment model that enables the department to respond to risks quickly as

they change. Next-generation internal audit functions have moved beyond annual or quarterly risk updates to obtain a real-time view of changes to risk and their impact on the organization, as well as the effect on the assurance needed from internal audit.

A dynamic risk assessment approach enables organizations to:

- Identify changing risk trends in real time.
- Reprioritize coverage of risk as changing risk trends are identified.
- Develop an ongoing and common view of risk and the integrated assurance map across the Three Lines Model.

The dynamic risk assessment process must be agile, integrated, and aligned. From an integration standpoint, the risk assessment must closely align with other internal audit processes, leveraging Agile auditing and continuous monitoring practices. In addition, the view of risk across the Three Lines Model must be consistent and aligned to measure and monitor the achievement of the organization's objectives. Aligned assurance is the correlation of risk, controls, and a broader view of the control environment across the Three Lines Model. Facilitating governance and management of risk within an organization's risk appetite, aligned assurance seeks to maximize operating efficiency and provide clearer visibility of results to stakeholders.

This alignment relies on an Agile audit approach in which enterprise risk management and internal audit are aligned. Agile auditing uses a framework that is based on iterative and sustainable development, where requirements and solutions evolve through collaboration among cross-functional audit teams focused on quality. Internal audit and its stakeholders are focused on a common goal of risk mitigation by responding to changing and emerging business needs and directions, while simultaneously working to meet business and regulatory commitments. In Agile auditing, if a dynamic risk assessment model does not have an impact on internal audit's assurance plan, the full potential of the model cannot be realized.

A Call to Action

Internal audit departments should adapt their risk assessment approach to quantify risk more effectively in a rapidly evolving business environment, in real time, and execute relevant assurance work to align with key organizational risks and priorities. Organizations and internal auditors must not only consider urgent matters requiring attention now, but also determine what is coming next and what may happen eventually.

Now: The disruptions created by the pandemic are particularly challenging for internal auditors performing risk assessments. Auditors are illustrating the strengths of Agile and targeted risk assessments in an unanticipated and fluid environment.

Auditors have the task of uncovering immediate risks associated with the changes wrought by COVID-19. These threats span the breadth of organizations and include risks related to keeping systems secure while employees are working from home, employees' mental health and well-being, and meeting compliance obligations in a distributed environment.

Using targeted risk assessments to identify threats during a crisis can deliver more meaningful and valuable results to stakeholders. They can set the stage for discussions about regulatory changes or compliance, as well as emerging or heightened risks, and immediate actions to address them.

Next: To build a dynamic risk assessment, internal auditors can use flexible risk assessments to continuously monitor the organization's operations and identify matters requiring attention. This practice allows internal audit to more quickly and accurately determine where organizations should focus attention and resources to improve processes, address risks, make corrections, and launch goal-achieving initiatives.

Technology is pivotal in effective continuous monitoring. Organizations increasingly are adopting innovations to move toward a continuous monitoring approach, which can help pave the path for a dynamic risk assessment.

Many organizations are leveraging advanced data analytics to allow internal auditors to more effectively map out action plans; make better inquiries into the various owners of risks and processes; and improve how, when, and where audits are conducted. During the pandemic, internal audit functions have used such data to inform and test the value of key risk indicators and then recalibrate these indicators to better align with available data.

Process mining is becoming a key differentiator for internal audit programs, particularly in a work-from-home environment. Process-mining technology provides auditors with critical insight into how systems and processes are operating in these situations and identifies where deviations may be occurring. The data tells auditors what is actually happening and supports dynamic risk assessment activities by identifying hot spots, driving audit focus.

Eventually: At some point, the crisis will end, and a rebuilding phase will begin. As workers transition to a more familiar routine, internal auditors can use dynamic risk assessments to prepare relevant audit plans and ensure organizations remain responsive to the risks facing day-to-day operations. Internal audit also can enhance the success or repositioning of project delivery, an area impacted heavily by the pandemic. Most importantly, the audit plan needs to provide executives with confidence that internal audit can accurately assess the organization's financial sustainability and any underlying risk.

The Change Imperative

In today's rapidly changing world, every organization faces the same reality — improve continuously or be left behind. Internal audit is no exception.

Chief Audit Executives (CAEs) need to respond to the emerging needs and new strategies of management and the board. When doing this, they must ensure the information they are communicating is timely and relevant.

Many CAEs have amassed goodwill by demonstrating internal audit's value in response to COVID-19. They can enhance their standing further by adopting next-generation audit practices that include dynamic risk assessments.

Culled From: iia.org

Security and Compliance: What to Expect in 2021

There is little doubt that 2020 has been one of the most challenging years many security professionals have encountered. The turmoil created by the COVID-19 pandemic has tested security and compliance to its absolute limits. Cybercriminals have capitalized on these times of rapid change and confusion, using COVID-19 to bombard potential victims with phishing attacks, clickbait and persistent attempts to exploit.

Security and compliance teams face an uncertain 2021, and there will no doubt be increased regulation as a result of COVID-19. But there is also data compliance uncertainty between the US, Europe and the UK as a result of the UK exiting the European Union in January 2021. Organizations will need to adopt protective security arrangements to meet the changing threat landscape, including the challenge of managing a remote workforce at scale.

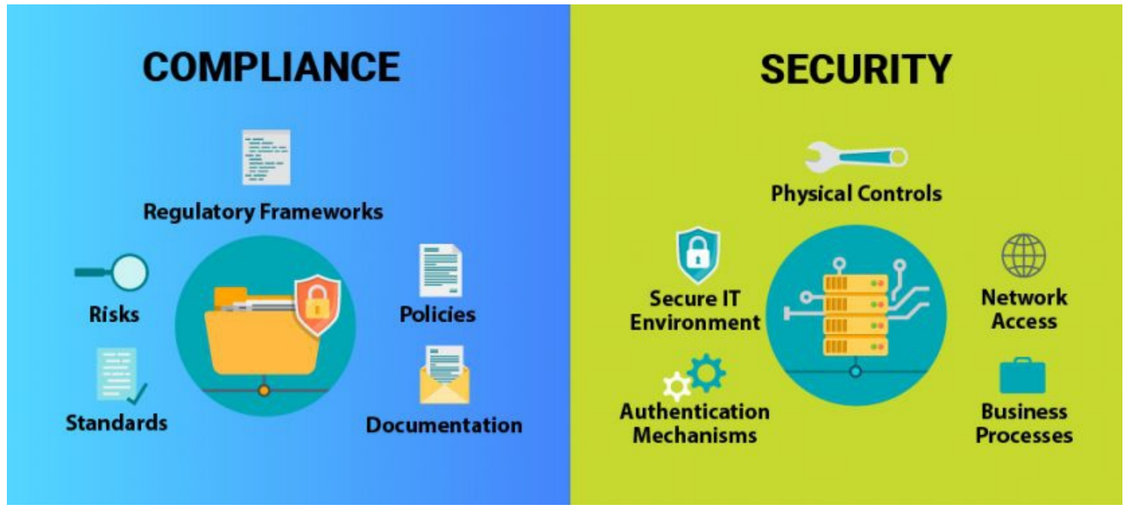
Securing a remote workforce

A sudden increase in remote working started in March 2020 for parts of the world, and businesses will continue to encourage this trend in a post-COVID era. Tech giants such as Microsoft, Google and Twitter have already announced such plans despite the challenges it introduces.

VMware Carbon Black reported a 148% increase in ransomware attacks in the first few weeks of lockdown, and the Verizon Data Breach Investigation Report has identified that the number of errors "made by the remote workforce" is increasing. Now that company data is inside people's homes, perhaps on personal laptops, any misconfiguration of newly acquired cloud services and questionable data security controls could be disastrous.

Proactive security teams will have already implemented mobile device management, mobile threat defense and endpoint device management software to minimize the risk of data from leaving authorized platforms. But the switch to mass remote working may have caught many businesses short.

Despite increased productivity and deeper employee engagement, inadequate controls over data will see auditors and regulators taking tougher action on businesses and employees as we move into 2021. Weak security controls will increase company exposure to external threats, and thorough risk analysis mitigation must continue into 2021. Remote worker habits must be monitored, and business preparedness must adapt as we hopefully enter a post-COVID dynamic.



Cloud agility and the shift to e-commerce

COVID-19 also has reinforced the necessity of business transformation and cloud migration. A cloud-first narrative was already prevalent in the majority of board rooms, but the pandemic has accelerated this desire. Businesses that already have some cloud services, such as video conferencing, telephony, and cloud-based productivity suites, have coped much better with the pandemic.

There has been a significant increase in the uptake of other cloud services. Traditional retailers have shifted focus to e-commerce, and the hospitality sector has quickly embraced table service ordering apps. This explosion in cloud uptake has increased the attack surface for cybercriminals.

There is simply a lot more infrastructure to target and more remote desktop connections to brute-force attack. It is imperative to keep training and sharing relevant knowledge into 2021. Awareness of the latest cybersecurity trends will likely reduce the chances of misconfiguration during this often-hasty transition.

Compliance and enforcement

2020 have been a difficult year for compliance. We have already seen the EU-US Privacy Shield being revoked. Any businesses that handle sensitive or personal data, such as HIPAA-compliant healthcare organizations, must take extra care during this pandemic.

Each legislation is still enforceable despite the occasional relaxation of enforcement by governing bodies like the Office for Civil Rights (OCR). Other data privacy acts, such as GDPR, CCPA, and PIPEDA, will continue to take action against businesses that suffer a data breach. EasyJet, a low-cost British travel company, is one such example. It was fined £180 million for a data breach of 9 million passenger and credit card records. EasyJet is also facing an £18 billion lawsuit from the passengers impacted.

Data breaches are expected to increase into 2021, and the use of ransomware is expected to spike. Large-scale phishing campaigns are targeting individuals, playing on the reader's emotions. Campaigns purport to have information about furlough schemes, government cash incentives for business support, or false information about vaccines.

Final thoughts

We have just scratched the surface of what to expect from security and compliance in 2021. Businesses and employees need a comprehensive security strategy, whether you use a dedicated server or cloud implementation, or use a managed cloud service to reduce the risk of misconfiguration. Remember that legislation is still enforceable, even if some of the guidelines have been relaxed.

Culled from: isaca.org

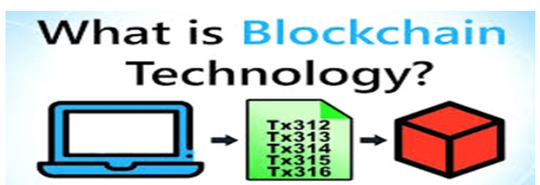
UNDERSTANDING THE AUDITABLE SCOPE WITHIN THE BLOCKCHAIN/STRUCTURED LEDGER TECHNOLOGY (SLT)?

AUDIT OVERVIEW AND EXPECTATIONS OF INTERNAL AUDITORS

It is no longer news that the globe is a common village, commodity exchanges amongst entities have gotten many means of settlements; currently on the top burner with difficulties in understanding by persons and entities within the Nigeria and indeed global business spectrum is the 'bitcoin' – a digital token built on a distributed ledger infrastructure otherwise known as distributed ledger technology (DLT).

This article is to set to provide readers most especially Internal Auditors who are charged with the responsibilities of providing assurances to those charged with governance, a quick insight into the world of bitcoin as a means of exchange as well as the accounting treatments/judgements expected of entities by the International Accounting Standards Board's (IASB); while aligning same with existing internal audit practice of structured processes before drawing conclusion on the structured ledger post audit review.

THE CONCEPT OF BLOCKCHAINS BY GREAT MINDS AT THEIR RESPECTIVE TIMELINES.



Blockchain is a form of distributed ledger, which uses independent computers known as nodes to record transactions, shares and ability to synchronizes databases in separate electronic ledgers instead of the usual traditional ledger where data is centrally stored. Thus, it aids audit trail and auditable history of information while making evidences (traces) visible to everyone within the network. A blockchain consists of records known as ''blocks'' that is used to record transactions on many active blocks which cannot be altered retrospectively without the alteration of all subsequent blocks.

A distributed ledger thus connotes a type of data base spread across multiple sites, regions or participants, the blockchain is in sequence of blocks which amounts to a type of distributed ledger.

WHO INVENTED DISTRIBUTED LEDGER?

Globally accepted innovator of the Blockchain Technologies which is today fast becoming an accepted medium of exchange across extensive business hubs of the world.

Various blockchains conceptualizations had taken place before year 2008 when the works of the famously anonymous innovator, known by pseudonym (SATOSHI NAKAMOTO) became globally accepted. However, history has it that the blockchain invention started since 1991, with an inventor improving on the works of the previous one.

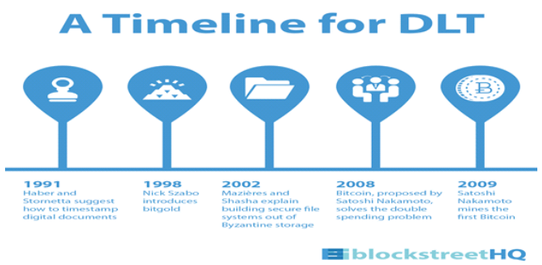
SATOSHI NAKAMOTO introduced a peer-to-peer version of electronic cash that allows direct online transactions between two parties without a third party. Nakamoto's paper proposed a solution to bit gold's double spending problem by implementing **distributed peer-to-peer timestamp servers, which generate computational proof for the chronological order of transactions.** Nakamoto's proposal became a reality in 2009 when he led the group that mined the first block, meaning a transaction was verified and added to the base of the chain, thus kicking off a chain of blocks, each containing information on verified transactions.

Transactions on cryptocurrencies are routed though e-wallets; these wallets are shown in the schedule below:

-		overall wallets as at
–		
–		
—		
—		
—		

BEFORE THE BLOCKCHAINS TECHNOLOGIES

The first ever bitcoin was known as ''genesis block'' mined in January 2009, most people had never known or heard about Blockchain; there were other concepts similar to the bitcoins, it evolved as a form of distributed ledger technology. However, not all distributed ledger technologies are blockchains, below is an excerpt of the highlights on blockchains before 2008.



STRUCTURED LEDGER TECHNOLOGY AND ITS ETHICAL CHALLENGES TO THE INTERNAL AUDITORS/ACCOUNTANTS

Distributed ledger technology (DLT) is a digital system for recording asset transactions in which the transactions and their details are recorded in multiple places at the same time. It is a digital database of records with information relevant to a group of participants. Unlike traditional databases, distributed ledgers have no central data store (CDS) or administration functionality. All participants are looking at a common, shared, view of the records which are updated at the same time for all participants.

The reliability of such a system is paramount as is the need to ensure that sensitive citizen data is not impaired or largely at risk. If anything went wrong, this may present ethical challenges to the Internal Auditors/Accountants. The Internal Auditors will therefore require a knowledge of distributed ledgers and be able to assess the risk of hacking to data.

Professional Accountants/professional accountants must be honest about whether they are comfortable with their knowledge of DLT and may need to consider the client's interests when they are dealing with large volumes of sensitive information.

WHAT IS THE ACCEPTANCE LEVEL OF CRYPTOCURRENCIES AS MEANS OF EXCHANGE ?

Increasing number of entities are accepting digital currencies as payment, digital currencies are not yet widely accepted as a medium of exchange and do not represent legal tender. Entities may choose to accept digital currencies as a form of payment, but there is no requirement to do so. Blockchains however comes into different forms; (1) permission-less and (2) permissioned blockchains; and it is exactly what the names connotes with both public and private keys being used by participants respectively on same.

HOW CAN BLOCKCHAIN OR STRUCTURED LEDGER TECNOLOGY (SLT) BE ACCOUNTED?

CRYPTOCURRENCY is an intangible digital token that is recorded using a distributed ledger infrastructure, often referred to as a blockchain. These tokens provide various rights of use (ROU). For example, cryptocurrency is designed as a medium of exchange. Other digital tokens provide rights to the use of other assets or services.

These tokens are owned by an entity that owns the key that lets it crease a new entry in the ledger. Access to the ledger allows the re-assignment of the ownership of the token. These tokens are not stored on an entity's IT system as the entity only stores the keys to the Blockchain (as oppose to the token itself). They represent specific amounts of digital resources which the entity has the right to control, and whose control can be reassigned to third parties.

ARE THERE TAILORED ACCOUNTING STANDARDS FOR CRYPTOCURRENCIES?

At first, it might appear that cryptocurrency should be accounted for as cash because it is a form of digital money; but looking it broadly, you will realise that cryptocurrencies cannot be considered equivalent to cash currency as defined in International Accounting Standards 7 -(statement of cashflows) and International Accounting Standard 32 (financial instrument – presentation) because they cannot readily be exchanged for any good or service.

IAS 7 defines cash equivalents as 'short-term, highly liquid investments that are readily convertible to known amounts of cash and which are subject to an insignificant risk of changes in value'.
Thus, cryptocurrencies cannot be classified as cash equivalent because they are subject to significant price volatility.

A relational table or schedule as shown below reflects on the various codes of IASs or IFRSs that have been directed at digital (cryptocurrencies) currencies.

	CODES OF IASs/IFRS WITH POSSIBLE IMPACTS	IMPACTS NARRATIVES	GLOBAL (IAS) PRESCIPTIONs
1	**IAS 7** **(STATEMENT OF CASHFLOWS)**	⌘ It does not appear that digital currencies represent cash or cash equivalents that can be accounted for in accordance with IAS 7. ⌘ It cannot be classified under any sub-headings within the statement of cashflows	⌘ Code cannot be adopted as a basis for accounting for cryptocurrencies.
2	**IFRS 9** **(FINANCIAL INSTRUMENTS)**	⌘ Intuitively, it might appear that cryptocurrency should be accounted for as a financial asset at fair value through profit or loss (FVTPL) in accordance with IFRS 9. ⌘ It does not seem to meet the definition of a financial instrument either because it does not represent cash, an equity interest in an entity, or a contract establishing a right or obligation to deliver or receive cash or another financial instrument. ⌘ Cryptocurrency is not a debt security nor an equity security (even though a digital asset could be in the form of an equity security)but it does not represent an ownership interest in an entity.	⌘ Cryptocurrencies cannot not be accounted for as a financial asset.
3	**IAS 38** **INTANGIBLE ASSETS**	⌘ Digital currencies or cryptocurrencies do appear to meet the definition of an intangible asset in accordance with IAS 38 – Intangible Assets. ⌘ The standard defines an intangible asset as an identifiable non-monetary asset (INMA) without physical substance. ⌘ IAS 38 further indicates that ''an asset is identifiable if it is separable or arises from contractual or other legal rights. ⌘ An asset is separable if it is capable of being separated or divided from the entity and sold, transferred, licensed, rented or exchanged, either individually or together with a related contract, identifiable asset or liability.	⌘ Given the characteristics of intangible assets, cryptocurrencies seem to have the closest alignments. ⌘ Entities are to adopt self-judgement in applying IAS 38 to the accounting treatment of cryptocurrencies.

4	**IAS 21** **THE EFFECTS OF CHANGES IN FOREIGN EXCHANGE RATES**	⌘ IAS 21 states that an essential feature of a non-monetary asset is the absence of a right to receive (or an obligation to deliver) a fixed or determinable number of units of currency. ⌘ For emphasis, it does not give the holder a right to receive a fixed or determinable number of units of currency.	⌘ It thus appears that cryptocurrency meets the definition of an intangible asset in IAS 38 as it is capable of being separated from the holder and sold or transferred individually and, in accordance with IAS 21, which is the opposite.

FINAL REMARKS:
Cryptocurrency holdings can be traded on an exchange and therefore, there is expectation that the entity will receive an inflow of economic benefits. However, cryptocurrency is subject to major variations in value and therefore it is non-monetary in nature. It is a form of digital money without physical substance. IAS 38 – Intangible assets has been accepted as the most appropriate classification; and as such Internal Auditors and Accountants are expected to apply the accounting treatment applicable to intangible assets to cryptocurrencies emanating from structured ledger technologies (SLT).

INTERNAL AUDIT/ACCOUNTANTS' RESPONSIBILITIES AT MITIGATING RISKS ASSOCIATED WITH BLOCKCHAINS' TRANSACTIONS

- ★ Examining transactions and verifying the existence of digital assets.
- ★ Attesting to consistency between information on a digital ledger and the real world
- ★ Review transactions' records (amounts, senders' codes etc) on blockchain technology
- ★ Develop IT proven approach to audit around data on multiple blocks on the blockchains
- ★ Offer assurance services by leveraging on industry knowledge and experience to offer advice for blockchain consensus protocols
- ★ Leverage on IT auditing to examine internal control of blockchain, including data integrity and security.
- ★ Reconciliation between records on a blockchain, other reports and physical existence.

ARE THERE CURRENT AND POTENTIAL FUTURE CHALLENGES

The challenges posed to both permission-less and permissioned blockchains are virtually the same. They include amongst others the following:

- ★ Potential information leakage to outsider, including business competitors and customers;
- ★ Repetitive and competition between an existing enterprise resource planning (ERP) and a blockchain.
- ★ No central archive or authority to verify the existence, ownership and measurement of items recorded on blockchain on the go.
- ★ Data retrieval due to clients' loss of private key.
- ★ No centralized authority to report cyber-attacks.
- ★ Learning curve timeline could be very high, as the blockchain technologies are gradually unfolding and awareness isn't that swift amongst members of the public.
- ★ Non-reversal of erroneous transactions.
- ★ Difficult to reach consensus rules amongst all participants when acting as agents to entities.
- ★ Power of override on information on blockchain.

CONCLUSION

Using both the public and private keys, miners solve mathematical functions to verify that the transactions senders and receivers match with the stated sources and that the transactions' contents have not been modified along the way.

With the aid of blockchain digital technology, we would have a world in which contracts are embedded in digital codes and stored in transparent, shared data bases, where they are protected from deletion, manipulations, dilution, distortion and possible theft. Every payment would have a digital record and signature that could be identified, validated, stored and shared. Interdependencies and frictions are eliminated, thus enabling algorithms to freely transact and interact with one another across the globe, thereby reducing its audit universe to a limited scope.

JULIUS OREYE A, AUDIT LEAD
HERITAGE BANK PLC

Growth Impact of Micro Small and Medium Enterprises (MSMEs) Financing by Deposit Money Banks in Nigeria

Globally, Micro Small and Medium Enterprises (MSMEs) play a major role in economic and social development in all countries, especially developing countries, accounting for 90% of private sector establishments and employing 50-60% of the labor force. In terms of employment generation, they contribute more, as they employ more than half of the entire workforce in the United States, and two-third in the European Union.

MSMEs can be likened to a propeller that powers the engine of a nation's economy for growth and development. MSMEs are businesses involved in different activities across Nigeria.

Their businesses include the production of local agricultural implements, bar owners, tailors, iron fabricators, vehicle mechanics, transporters, internet café owners, washmen, software development to mention but a few of them. MSMEs are also involved in producing for domestic and international markets. MSMEs can be found in rural, urban, regional, national, or international markets.

The Concept of Micro Small-Scale Enterprises (MSMEs)

MSMEs have a long history like every other part of the world. Historically, "small and medium enterprises has it origin in the eastern and Mediterranean", small and medium enterprises, all over the world is divergent arrays of business concerns involved in economic activities spanning from micro and rural enterprises to contemporary industrial organizations that uses sophisticated technologies. As a result of their relevance and contribution i.e., small, and medium enterprises to national economies, policy planners, academic and national government have shown interest in issues pertaining to small and medium scale enterprises (SMEs) all over the world. It was the means of survival for the people since ages, it has managed to save many poor homes that have the innovation to start a unique business but with different problems with establishment or survival. In Nigeria, there is no generally acceptable definition of SMEs, but it varies over time from organization to organization.

- Micro Enterprise: Any enterprise employing between one to nine people and having a capital base from one naira to ₦5 million excluding cost of land.

- Small Enterprise: Those that employ between 10 and 49 employees and having a capital base from ₦5 million to ₦50 million so once a business is within that confine, it is running a small enterprise.

- Medium Enterprise: Any enterprise that employs from 50 to 199 employees and having a capital base from ₦50 million to ₦500 million. If a business is within that confine it is running a medium enterprise and if it has anything above that, it is a large enterprise or a multinational. The National Policy on MSMEs adopts a classification based on dual criteria: employment and assets (excluding land and buildings), as follows:

The Central Bank of Nigeria (CBN) defines SME as an enterprise with a maxi-mum asset base of NGN200 million, without land and working capital, also the number of employees is not less than 10 and not more than 300. Due to the flexible nature, SMEs are quite able to withstand economically diverse situations. SMEs in Nigeria can be categorized into urban and rural enterprises, but in a more formal way they can be called Organized Private Sector.

According to history, SMEs in Nigeria have existed since the country's independence in 1960, probably before independence but since independence Nigeria has had series of seminars, studies and workshops, each of which appraise the excellence, importance and need to facilitate the establishment and sustainability of SMEs. All the National four-year development plans from 1962-63 to 1984-85 have laid strong emphasis on strategies of government-led industrialization mount on import as substitution. In addition, the Structural Adjustment Program (SAP) initiation in 1986, the state did not appreciate the Structural Adjustment Program active involvement in industrialization by a process of commercialization and privatization. Special attention was then shifted from large scale industries to Small and Medium Scale Enterprises, which has a prominent potential for developing domestic linkages for effective growth, sustainable industrial development. Bigger and greater leaning were then placed on the organized private sector (OPS) to head previous industrialization programmes.

However, SMEs in Nigeria have not been able to play these important roles given the quantum of challenges they face which include inadequate capital, as they are not able to have access to finance from banks, poor operating environments as typified by poor state of infrastructure, low entrepreneurial skills and inconsistent government policies. To tackle the problem of inadequate finance, government at various times put in place schemes to ensure flow of investable fund into the sector. The focus of government shortly after independence was to ensure that indigenous entrepreneurs participated actively in the sector and efforts were made at channeling funds to improve the contribution of small and medium enterprises (SMEs).

Despite the intervention by government, this trend continued till the early 2000s when it became apparent that a system-wide approach was necessary to address this funding challenge of SMEs. This partly necessitated the banking sector consolidation of 2005 to ensure banks active participation in financing SMEs (Mordi et. al. 2014). MSMEs play a significant role in the economic development of nations as they play a prominent role in the private sector. MSMEs make up over 90percent of entrepreneurs of the world and are responsible for 50 to 60percent of employment generation. MSMEs occupy an essential position in almost every country or state, and they have been recognized by government and development experts as the main engine of economic growth and a significant force in the promotion of private sector development.

For any developing country to grow and develop economically, greater attention must be paid to the MSME sector. Financing had been identified in many business surveys and research as one of the main factors determining the survival and growth of MSMEs in both developing and developed countries. Banking sector help to make finance available to firms by mobilizing surplus fund from deposits and channel it in the form of credit to investors Finance remains one of the barriers to the growth of MSMEs in Nigeria.

Commercial bank credit to private sector is one of the leading businesses of deposit banks through which they generate income. Bank credit to private sector is an essential source of funds for most organizations. Access to finance is vital to business start-up, development, and growth for SMEs. Deposit money banks play a crucial role in economic resource allocation in many countries. Deposit money banks mobilize deposits and channel it to investors who need funds. For businesses in Nigeria looking for finance from banks to grow, the year 2020 look a bit brighter for them. Nigeria's Central Bank (CBN) has insisted that every bank must give out 65% of all deposits customers make in it as loans. Out of the 65%

of all deposits given out as loans, banks are further directed to give out 150% of it to startups and MSMEs. This however would only be applicable to commercial and merchant banks in the country.

Deposit Money Bank's Credit to Private Sector

Deposit money bank is a type of financial institution whose activities are based on accepting deposits and granting credit. The deposit money bank is considered an intermediary between those who have surplus funds and those who need them. deposit money banks are characterized by three important features distinguish them from other business enterprises namely liquidity, profitability and security, this importance is due to their significant impact on the formation of policies related to the main activities of the banks, which are the acceptance of deposits and the provision of loans and investment in securities.

Deposit money banks have almost one-third of the financial assets of all financial institutions in an economy, have the ability to generate funds from reserves generated by public deposits and have the ability to provide all credit needs for individuals, businesses and even governments. Since loans are the primary source of microfinance worldwide, and their source is mostly from commercial banks, these banks play an important role in the development of such projects.

Deposit money banks in developing countries have begun to view microfinance as not only a very important tool in public relations but also a profitable enterprise. The primary objective of deposit money banks is to maximize their profits with minimal risk, which leads them to seek high returns for granted loans and sufficient guarantees; and the fact that the loans granted to small projects are usually small and sufficient guarantees on project' assets, which are usually higher than the value of the loan and thus combine their objectives for profit and risk reduction. But this also makes it more difficult for small businesses to get loans from deposit money banks.

Credit is a major function that commercial banks perform. Deposit money banks in playing their intermediation role do give their deposits mobilized out to the deficit economic unit as loan, which may be on short, medium, or long-term basis. This assists them in achieving their profitability principles and other ends for which they are setup. A lot has been reviewed in terms of deposit money banks' credit activities of various deposit money banks. Some opinions deliberated on the factor responsible for banks willingness to extend many credits to some sector of the economy, while some discussed effect of such extension of credits on productivity and output. Most of these earlier studies agreed on the fact that it is logical for banks to have some basic credit principles or consideration to act as a check in their credit activities.

Since there are many studies in respect of bank's credit behavior, it is therefore imperative to highlight and consider some factor that economist and professionals alike have proposed as virtually significant in explaining the determinants of deposit money banks' credit behavior. Promoting access to finance is indubitably the heart of banking business. For that reason, its administration requires considerable skill and dexterousness on the part of the bank management. While a bank is irrevocably committed to pay interest on deposits, it mobilized from different sources, the ability to articulate loanable avenues where deposit funds could be placed to generate reasonable income; maintain liquidity and ensure safety requires a high degree of pragmatic policy formulation and application.

Banking in Nigeria witnessed an era of impressive profitability, characterized by high competition, huge deposits and varied investment opportunities; in an effort to make quick profits the banks relied essentially on self-liquidating loans and diversified their portfolio into less risky investments with safe margin. The current trend in Nigerian banking and finance sector, suggest that the days of cheap profits are now over and only banks with well-conceptualized lending and credit administration policies and procedures can survive the emerging competition.

Further, bank-credit decisions generally are fraught with a great deal of risks, which calls for a great deal of prudence and tact in this aspect of banking operations. The success of every financing activity largely hinges on the part of the credit analysts to carry out good credit analysis, presentation, structuring, and reporting., supported this view by stressing that" the days of armchair banking are over and that the increasing trend in bad debts and absence of basic business/corporate advisory services in most Nigerian deposit money banks, suggest an apparent lack of use of effective financing and credit administration techniques in these banks".

Emphasizing this assertion, Osayameh (1991), further stressed that "the major objectives of commercial banks' lending is to maximize profit". The staggering increase in volume of commercial banks credit in Nigeria, during the half of eighties alone, lends credence to this assertion. In 1980, aggregate commercial bank loan and advances was N6.4billion.

This increased to N113.6billion in 1986, a staggering increase of 94%. Management of such resources should therefore transcend the use of traditional techniques based mainly on the use of rule-of thumb, hunches, and experience.

The present volume and complexity of transaction in bank lending and credit administration in Nigeria call for the use of scientific techniques like those of management science and operations research to aid their lending and credit administration. in a study on roles and failure of financial intermediation by banks in Nigeria revealed that "commercial banks can lend on medium- and short-term basis without necessarily jeopardizing their liquidity. If they must contribute meaningfully to the economic development, the maturity pattern of their loans should be on a long-term nature rather than of short-term period".

Monetary Policy rate

The term monetary policy has been defined by experts from many perspectives. According to CBN (2006), monetary policy concept was defined as "Any policy measure designed by the federal government through the CBN to control cost availability and supply of credit. It also referred to as the regulation of money supply and interest rate by the CBN in order to control inflation and to stabilize the currency flow in an economy. Also, CBN (1997), defined monetary policy as combination of measures designed to regulate the value, supply, and cost of money on an economy in consonance with the expected levels of economic activities.

A close observation of these definitions of monetary policy shows that monetary policy boils down to adjusting the supply of money in the economy to achieve some combination of inflation and output stabilization. Most economist agree that in the long run output usually measured by gross domestic product (GDP) is fixed, so any changes in the money supply only cause prices to change. But in the short run, because prices and wages usually do not adjust immediately, changes in money supply can affect the actual production of goods and services.

Monetary Policy is the deliberate use of monetary instruments (direct and indirect) at the disposal of monetary authorities such as central bank in order to achieve macroeconomic stability. Monetary Policy is essentially the tool for executing the mandate of monetary and price stability. Monetary policy is essentially a programme of action undertaken by the monetary authorities generally the central bank, to control and regulate the supply of money with the public and the flow of credit with a view to achieving predetermined macroeconomic goals (Dwivedi, 2005).

Monetary policy is one of the tools of controlling money supply in an economy of a nation by the monetary authorities in order to achieve a desirable economic growth. Monetary policies are effective only when economies are characterized by well-developed money and financial markets like developed economies of the world. This is where a deliberate change in monetary variable influences the movement of many other variables in the monetary sector.

The performance of monetary policy has improved greatly in recent times- inflation has remained at moderate levels accompanied by high growth of domestic output. To sustain the efforts, there is need for appropriate collaboration with the fiscal authorities as well as the development of confidence in inter-bank market and the necessary financial market infrastructure is still relevant.

Deposit money bank credits to MSMEs

Deposit money Bank credit refers to loans, advances, and discounts of specific sums, which are normally with terms and other conditions available to individuals, small and medium sized business to start, grow or sustain any economic activity (John and Onwubiko, 2013).

A widespread concern is that, the deposit money banks attitude towards the subsector; which supposed to be the major source of funding to small and medium sized businesses are not providing enough aids and therefore limiting the potentials that could be taped from the subsector. The deposit money banks in their mode of operations most of the time call for more sure form of financial security, if they are to grant credit facility to small or medium sized business that need funds for business activities. However, due to the nature of small and medium sized businesses, in most cases, they tend not meeting up the requirements for the granting of the facilities. This has become a major challenge to the small and medium sized business operations in Nigeria. Robinson and Victor (2015) assert that most SMEs growth was hindered as a result of inability to access fund from financial institutions.

Characteristics of Deposit Money Bank Credit

Some characteristics of deposit money bank credits are of prime importance while extending credit to an individual or to a business enterprise.

Confidence: Confidence is very important for granting or extending any credit. The person or authority must have confidence on debtor.

Capacity: Capacity of the borrower to repay the debt is also very crucial thing to be considered. Before granting or extending any advance, creditor should evaluate the borrower's capacity.

Security: Deposit money banks are the main source of credit. Before extending credit, deposit money bank ensures properly about the debtor's security. The availability of credit depends upon property or assets possessed by the borrower.

Goodwill: If the borrower has good reputation of repaying outstanding in time, borrower may be able to obtain credit without any difficulty.

Size of credit: Generally small amount of credit is easily available than the larger one. Again, it also depends on above factors.

Period of credit: Normally, long term credit cannot easily be obtained because more risk elements are involved in its security and repayments.

Principles of Sound Credits

Credit is the most important function of the bank and profitable as well. On the contrary it is a risky business too. Loans always have the credit risk. So, a banker should manage the loan business in a profitable and safe manner. All the necessary precautions should be taken by a banker to minimize credit risk. Every borrower has different nature and functions of business. While considering a loan proposal, certain general principles of lending should be kept in mind that can help establishing some credit standards. Bank lending is an art as well as a science. These techniques, tools and methods are mostly mechanical. With a little practice, it can be learnt. Principles guide to action.

Safety: This is the most important guiding principle of a banker. Bank's business deals with the public deposits. Bank has to ensure the safety of the funds lent. Safety means the borrowers should be in a position to repay the loan along with interest. Otherwise, the banker will not be in a position to repay the deposits and bank may lose the public confidence. Bank follows lending policy to maximize earnings, but it has always to be defensive at the same time because it cannot afford to lose the people's money. The advance should be granted to reliable borrower.

Security: Security means any valuable given to support a loan or advance. A large variety of securities may be offered against loans from gold or silver to immovable property. The security accepted by a banker as a loan cover must be adequate, easy to handle, readily marketable. A banker must realize it only as a cushion to fall back in case of need.

Liquidity: Liquidity means a bank's ability to meet the claims of its customers. Banks should ensure that the money lent is not locked up for a long time. A bank would remain liquid with liquid advance. This is an important aspect of banking, which distinguishes it from insurance finance or industrial finance. It is the capacity of a bank to honor its obligations. A banker does the business on borrowed funds; it should ensure liquidity while lending money. At the time of need, a banker should be able to convert assets into cash to meet the demand of depositors, because depositors have faith in a bank on the basis of its liquidity.

Suitability: Banker should concentrate lending activity on purpose desirable from the point of view of economic health of the nation. Finance to gambling is not a part of banking business. Due consideration should be given to control inflation and raising the standard of living of the people.

Risk diversification: Every loan has its own risk. So, it is better to give an advance for different purposes and segments to spread the risk. For safety of interest against contingences, the banker follows the principle of "Do not keep all the eggs in one basket." Bank should avoid concentrating the funds in a few customers or segments. The advances should be spread over a reasonably wide area, number of borrowers, number of sectors, geographical area, and securities. Another form of diversification is maturity diversification. Under this, the loan portfolio is concentrated over different maturity periods. So that, a certain amount of loans matures at regular intervals which can be utilized to meet the depositor's demand.

Profitability: Commercial banks are profit earning concerns so bank must earn sufficient income to pay interest to the depositors, meet establishment charges, salaries to staff, earn income for the future, and distribute dividends to the shareholders etc. The difference between the lending and borrowing rates constitutes the gross profit of the bank. A bank should possess liquidity, with surety of profit; banks should not ignore the safety or liquidity.

Purpose: A banker should inquire the purpose of the loan. Safety and liquidity of loan depend on the purpose of loan. Loan may be required for productive purposes, trading, agriculture, transport, self-employment etc. Loan for productive purpose would increase the chances of recovery. On the other side, loan for non-productive purpose would have lots of uncertainty about recovery. After nationalization, the purpose of a loan has assumed more significant.

Nature of business: There may be innumerable types of businesses and the repaying capacity of a borrower depends on the nature of the business. So, banker should consider this while granting the loan.

Margin: The security offered against advance must be judged from the aspect of economic value and legal aspect. The market value of the security must be higher than the value of advances proposed. It should give enough margins for fluctuation in prices and interest rates.

National policies: In a developing country like Nigeria, banks are also required to fulfill some social responsibilities. Government policies and national interests impose certain social responsibilities on commercial banks. Sometimes to cater social responsibility, advances are given at concessional rate to the weaker and neglected sectors. The lending policies of banks are to be modified from time to time to suit the needs of the economy.

Types of Credit Facilities Granted

However, it is common knowledge that getting financial support from deposit money banks has been grossly inadequate for budding indigenous entrepreneurs and even for those who have been in the SME business for a long term. Three types of credit are usually required by small scale enterprises. They include:

Short Term Credit: This type of credit is used to finance yearly operation until the product or proceeds from the industry are sold. The amount which is involved in this type of credit is usually small but lack of this type of credit is most accurately felt by small scale entrepreneurs who have little or no saving upon which to withdraw as they are mostly beginners.

Medium Term Credits: This type of credit is for more than one-year maturity period but not exceeding three to five years. This credit is mostly required for acquisition of inexpensive equipment with relatively short life span.

Long Term Credits: This type of credit is necessary for acquisition of major industrial machines, improvement in industrial equipment, building and land: It is a type of credit that the maturity period is for quite a longer duration.

Small scale enterprises therefore can be a powerful instrument in bringing about a revolution in industrial practices and in firms' productivity especially if supplied in sufficient quantity and used effectively. The study therefore identifies small scale entrepreneurial financing by commercial banks as a major role to entrepreneurial development because finance is just one of the major factors of production. The problem of credit to small scale industries may not necessarily be as a result of financing insufficiency but rather for some other reasons among which are.
Insufficient preparation on the part of small-scale entrepreneurs in their request for credit assistance. Information gaps as to range of funding institutions and scope of services available in these institutions. Moreover, servicing of small business accounts is relatively experience, risky and difficult to monitor with low turnover of account.

However, the parishioners in the sector small scale industry do not display competence in preparing justification for their project. It is are to see most of them coming up with cash flow projections, projected balance sheets, among others. They are based on personal rudimentary in formation and speculation. At times when they seek the advice of consultants, the outcomes that are made figures project based on assumptions which are most of their time unrealistic. As a result, such proposals are out rightly rejected by banks. There are suitable when credit demands in this sector are not in compliance in this government monetary policy and credit guidelines which must be adhered to by banks.

Nigeria Experience on SMEs Financing and Economic Growth

SMEs are made up of indispensable components in the growth of any economy. The story makes no exceptional difference in Nigeria as Small and Medium Scale Enterprises control the economy. Over the years, government has articulated a number of policies which are aimed at growing SMEs. Most policies literally failed due to poor performance, others however, succeeded. Attempts have been made in the past to recognize the role of SMEs to the growth of Nigeria's economy, its challenges and prospects which generated a space on the role of deposit money banks in the financing of Small and Medium Scale Enterprises.

This is as a result of government support programmes that create significant environmental conditions which ease the capacity of Small and Medium Scale Enterprises in order to contribute to development through the exhibition of goods and services thereby creating employment. It would not be out of place to have funds that target sectors that generate

significant wealth in a short period of time. Sectors such as creative industry, technology, mechanized agriculture, light manufacturing as viewed in the planned $500m FG fund, provided by the African Development Bank. The Nigerian federal government has set aside over ₦500 million for Ease of Doing Business initiatives in the 2019 Budget.

The Government Enterprise and Empowerment Programme (GEEP) is inventiveness by the Federal Government of Nigeria in order to allow financial literacy and access to micro-credit for Nigerians at the basal of the economic pyramid. The aim of GEEP is to provide capital to receivers in an easily available way to grow their business and on-board these beneficiaries into formal financial system with provision of bank accounts, mobile wallets, and formal identities.

TraderMoni is a loan programme of the Federal Government of Nigeria, created specifically for petty traders and artisans all over the country. It remains part of Federal Government Enterprise and Empowerment Programme (GEEP) scheme that is being executed by the Bank of Industry. TraderMoni gives an interest free loan to small businesses in Nigeria starting from N10,000 and grows all the way to N100,000 on the condition that the beneficiaries pay back. As the small businesses pay back the first loan, it automatically qualifies them for the second loan of #15,000. The entrepreneurs qualify for the next loan of #20,000 as soon as the #15,000 loan is paid back. This continues up to #50,000 and then #100,000. The Nigerian government wishes to support small businesses through the provision of continuous loans thereby making each loan bigger in order to encourage growth.

MarketMoni (also known as Government Enterprise and Empowerment Program or GEEP) is a business and empowerment programme of the Federal Republic of Nigeria that provides financial aid to small businesses that otherwise lack access to mainstream financial services and products in Nigeria. MarketMoni is part of the Government Enterprise and Empowerment Programme (GEEP), one of the Social Investment Programmes (SIPs) of the Nigerian Government. MarketMoni provides loans to traders with no interest except its 5% administrative fee.

FarmerMoni is a Government Enterprise and Empowerment Programme (GEEP) initiative created to boost economic growth through access to finance for farmers. This initiative is designed to help petty traders in order to expand their trade through the provision of collateral free loans. The loans are made repayable over a period of six months. The initiative allows beneficiaries to get access to a higher credit ranging from N300,000 to N2,000,000 when they repay within the stipulated time period. The scheme is to provide 1.66 million micro lending for businesses, women cooperatives, and market women: enterprising youth, farmers and agricultural workers, no collateral or interest element

In March 2020, the Federal government of Nigeria granted a three-month repayment moratorium for all government funded loans as part of government efforts to cushion the economic effects of Coronavirus pandemic on Small and Medium Scale Enterprises. The moratorium covers the Tradermoni, Marketmoni, Farmermoni and all loans issued through the Bank of Industry, Bank of Agriculture, and the Nigeria Export Import Bank.

The N-Power Graduate Programme is another Nigerian Federal Government's direct intervention to stop youth unemployment and re-activate public service delivery in four key sectors namely, education, agriculture, health, and tax. The endorsement will be realized by training and providing jobs for 500, 000 young Nigerian graduates across the 774 local government areas of the federation. In a way to continue and expand the N-power programme in Nigeria the Federal Government of Nigeria will now begin enrolment of a new batch of beneficiaries, starting from July 26, 2020.

SMEs and Economic Development Small and Medium Enterprises (SMEs) play vital role in the economic development of Nigeria and are known to be the main engine of economic growth and a key factor in promoting private sector development and partnership.

SME are generally responsible for the availability of goods and services, credits, motivating entrepreneurial spirit and repairs of second handed products. They create employment and a high standard of living, provide competition and fill needs of society and other firms has expanded these roles to include:

a) Aiding in the development of local technology.

b) Providing effective way of stimulating indigenous entrepreneurship.

c) Mobilization and utilization of domestic savings.

d) Ensuring a structural balance in terms of large- and small-scale industrial sector, as well as urban areas.

e) Ensuring the supply of high-quality parts and components, and intermediate products, thereby strengthening the international competitiveness of manufactured foods.

f) Producing specialized items in small quantity to meet current and diverse demands.

g) Mitigating rural-urban migration. They contribute to employment of the teeming unemployed youths and also strengthen the manufacturing sector of the economy.

COVID-19 and intervention measures to keep MSMEs afloat in Nigeria.

In a bid to support the growth of MSMEs, the federal government has established a number of schemes geared towards providing finance at low-interest rates. These include a special intervention fund managed by the Bank of Industry (BOI) to provide subsidized loans to MSMEs at a rate of 9% per annum.

Agri-Business/Small and Medium Enterprise Investment Scheme (AGSMEIS) is another intervention funding scheme anchored by the CBN specifically for enhancing agricultural businesses of MSMEs.

The latest of this move is the MSMEs Guaranteed Offtake Simulation Scheme which is aimed at providing bridge financing in supporting the payroll costs of MSMEs that are currently grappling with severe cash flow problems due to the disruptions induced by the global pandemic.

The vulnerable Nigerian MSME sector has been one of the sectors that have been badly hit by the current economic weakness brought about by the COVID-19 pandemic. Several businesses have been affected by supply chain disruptions and low demand for their products and services due to the weakened consumer purchasing power, leading to substantial loss in revenue. In a survey carried out by FATE Foundation in conjunction with BudgIT, of the 1943 MSMEs surveyed, 94.3% reported being negatively impacted by the pandemic particularly in the areas of Cashflow (72.1%), Sales (67.7%) and Revenue (59.2%).

Despite the negative impacts of the pandemic, 47.1% of respondents were positive that their businesses will survive the pandemic with 22.8% being unsure while 30% indicated that their businesses will not survive the pandemic. Most of the businesses reported needing support with Cashflow (72.1%) and Sales (67.7%) and will like the Government to provide support in the area of funding (89.4%) and access to markets (33.8%).

Globally, MSMEs are considered the critical engines of economic growth due to their potential to create jobs, boost economic output, generate income, and reduce poverty. In Nigeria, MSMEs have always struggled to play these essential roles given tough challenges in the business environment. Prior to the onset of the pandemic, many MSMEs were still reeling under the impact of the recent recession and were still struggling to get back on their feet. With the onset of the pandemic, the situation appears to have worsened for many. Given the importance of these MSMEs to the country's economic recovery post-pandemic, an effective support scheme should be a top priority. That said, it is essential that efforts should be deepened in improving accessibility and timely disbursement of such funds.

COVID-19 & EndSARS Lock down: How CBN policies helped prevent the collapse of the Nigerian economy:

Decisions taken in the next few days will determine how soon the issues surrounding the #EndSARS protests will be resolved. The past five to seven days in Nigeria have been nothing short of fictional for the Nigerian people. One would be hard-pressed to describe the events without seeming to take sides with either part of the standoff as emotions, euphoria and sometimes, unfounded principles have seemed to become the order of the day. Logic, accountability, and common sense being on vacation as they often are in such matters.

If there were negotiations (of which there are none presently), parties involved may likely disagree on a couple of things ranging from the sincerity of the other party, approach to a peaceful resolution, what amounts to a peaceful resolution and how to forge ahead.

Various initiatives and policies of CBN prevented the Nigerian economy from major setbacks before, during, and after the peak of the COVID-19 pandemic and EndSARS Lock down. Nigerian economy, like every other economy was severely hit by the impact of the pandemic, which was evident by the volatility in different markets. Therefore, in response to these harsh economic consequences, the CBN designed a lot of policies to help mitigate the effect of the pandemic.

Investors are generally reacting to policy changes as economies open up and world economies enter a recovery mode. Some of the policy changes he referred to, include CBN policy that domestic institutional investors should stop participating in the OMO market.

This policy has driven significant funds into the Nigerian Treasury Bills market, some of the funds have also trickled down to the equity market.

i) Cut in interest rate: This policy is a significant move in support of equities as an "asset class" because most investors are driven by yield. Due to the fact that the Nigerian economy has shifted into a negative real interest rate environment, these types of cuts will tilt investment preference to assets class that will generate higher yields and returns.

CBN's initial policy response to COVID-19 ranging, from granting of a further moratorium of one year on all principal repayments to the reduction of interest rates, the establishment of N500 billion targeted credit facilities, among others.

In the first quarter of the year 2020, the Nigerian Federal Government through the Central Bank of Nigeria (CBN) and the Federal Ministry of Finance, Budget, and National Planning have announced some monetary and fiscal measures to help mitigate the impact of the corona virus pandemic on the economy and Nigerian businesses.

The apex bank introduced a N50 billion Targeted Credit Facility (TCF) as a stimulus package to support small and medium enterprises (SMEs) that are affected by the corona virus pandemic. The TCF was designed to cushion the adverse effects of COVID-19 on MSMEs whose economic activities have been significantly disrupted by the COVID-19 pandemic, and to stimulate credit to MSMEs to expand their productive capacity through equipment upgrade and research and development. The scheme shall be funded from the Micro, Small and Medium Enterprises Development Fund (MSMEDF) and the eligible participating financial institution for the scheme is NIRSAL Microfinance Bank (NMFB). This means the CBN will be sourcing the fund from its MSME development fund which will be administered through NIRSAL Microfinance Bank. Thus, while the CBN will be providing the funds, applicants will have to apply for the loan through NIRSAL Microfinance Bank. The loan amount shall be determined based on the activity, cash flow and industry/segment size of beneficiary subject to a maximum of N25 million for SMEs. The guideline for this credit states that the loan for working capital shall be for a maximum of one year, with no option for rollover.

ii) MSME Survival Fund and Guaranteed Off Take Schemes (GOS): The federal government of Nigeria has just released the sum of N75 billion to MSME survival fund and support initiatives which is part of the N2.3 Trillion stimulus package of Nigerian Economic Sustainability plan to cushion the effect of COVID-19 & EndSARS Lock down

Conclusion and Recommendations

It is evident from my article that SMEs contribution is considerably high in economic development. Not only financially subsidized promotion is essential, but the strategic implementation becomes vital for sustainable development of the MSME sector.
Strategic implementation takes care of financial aspects, human resource, marketing, research and development, technology, and corporate governance in the MSME sector. It is critical for Policymakers to create an enabling and sustainable environment as a bedrock for MSMEs to flourish. Great to recall the words of Richard Branson; "A business star

Sunday Onwuemele
Team Member Forensic Investigations
United Bank for Africa Plc

How to Audit for Conflicts of Interest

Internal auditors can draw on several aspects when designing a plan for auditing this common risk.

Modern organizations generally recognize the risk of employees having interests that conflict with the interests of the organization, itself. These conflicts not only affect internal auditors - who are expected to follow The IIA's Code of Ethics and uphold the principles of integrity, objectivity, confidentiality, and competency - but all employees of the organization.

The challenge is that conflicts of interest can be difficult to identify, manage, and audit. Furthermore, there are various types of actual, potential, and perceived conflicts of interest. Some conflicts may involve an outside job or serving in another organization. Others may result from having personal and other types of relations with different stakeholders, which could influence decision-making.

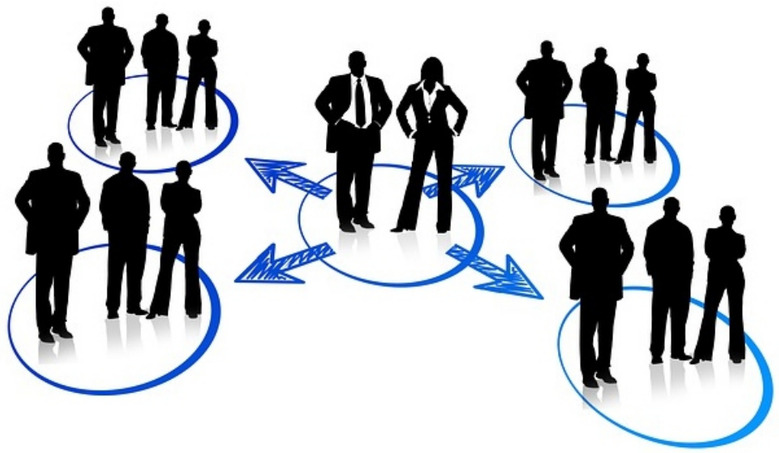
In the course of business, conflicts of interest are likely to arise. This does not automatically mean that the organization and its employees are doing something wrong. The issues are whether the organization is mature enough to recognize these situations and has developed mechanisms to address them. Internal auditors should consider several aspects when designing their approach to conflict-of-interest audits.

Clear Guidance

Organizations need to define what constitutes a conflict of interest and communicate that such conflicts are not allowed. Organizations can do this by adopting an ethics policy, defining organizational values, establishing behavioural principles, or simply notifying employees. Although such actions might appear trivial, organizations are expected to inform their employees about what is appropriate behaviour. Providing guidance on conflicts of interest and how to adequately communicate expectations to employees can be a good starting place for internal auditors to build their audit approach.

Organizational Setup

Businesses can organize duties related to managing conflicts of interest in different ways, as they can take various forms. In some organizations, the human resources (HR)



department will take the lead. However, additional departments, such as the ethics, compliance, or legal functions, are commonly involved in managing conflicts of interest. This approach creates complexity, because it requires the organization to clearly define roles and responsibilities, maintain adequate segregation of duties, exchange relevant data and information, and collaborate across functions.

Preventive Controls

It is important for internal auditors to identify which controls exist around conflicts of interest. Some generally applicable controls include:

- ***Processes for obtaining information from potential new employees and business partners.*** Organizations often ask new employees and business partners to provide information on any existing relationships with current employees. Such requests provide information before any relationship is established.
- **"Know your business partner" procedures.** Checking on business partners their business, organizational, and ownership structure can help identify conflict-of-interest risks.
- **Conflict-of-interest clauses in employment agreements.** Such clauses require employees to disclose their side activities with other companies.
- **Non-compete clauses.** These clauses in agreements and contracts should apply to employees, customers, business partners, and other stakeholders during the time they are associated with the organization or a specified time beyond that.
- **Conflict-of-interest management.** This process should include mechanisms, roles, and responsibilities for addressing reported or identified conflicts.
- **Prescribed response measures.** The organization would take these actions in case of a breach of conflict of interest-related agreements and clauses.
- **Gift register and policy.** A gift register should include both gifts given and received by employees. The gift policy should include an approval process for gifts of high value.
- **Conflict-of-interest reporting.** This process encourages employees to report conflict-of-interest relationships that may develop over time, including employees' relationships with other employees, managers, business partners, and stakeholders.
- **Outside employment approval.** Such a process requires employees to report and receive approval to have second jobs or freelance work.
- **Documentation.** The organization should have confidential, complete, and documented records on conflicts of interest.
- **Training.** The organization should train employees on conflicts of interest and how to deal with them.
- **Past lessons.** The organization should communicate and promote the lessons learned from past events.

Risk Acceptance

Organizations also should consider establishing a risk acceptance process to determine whether some conflicts of interest are acceptable. Some conflicts may be acceptable because of lack of other alternatives, organizational issues, resource availability, and evolving relationships. In each case, the organization needs to assess if the risk is acceptable from a risk appetite point of view.

Highly sensitive and confidential risk acceptance topics could be dealt with by an organizational body. For example, the organization could establish a committee comprising experts from HR, ethics, compliance, legal, risk management, and internal audit, with other participants invited, when necessary. This committee's work should be communicated and applied throughout the organization, as well as documented.

Post-transaction Controls

Certain conflict-of-interest controls could be exercised to trace issues after business transactions have taken place. Such controls include:

- Tools and records for obtaining information on how the reported conflicts of interest were addressed.
- Documented background checks on employees.
- Documentation of design changes from previous controls.
- Effectiveness assessment of new, additional, changed, and compensating controls to mitigate conflict-of-interest risks.
- Documented follow-up of any compensating measures taken for cases of risk acceptance.

These controls could provide auditors insights on how conflicts of interest were identified, as well as the recognition and management process steps taken, outcomes achieved, and follow-up results.

A Corporate Culture Matter

Managing conflict-of-interest situations is not just a formal question, but rather an integral part of the much broader concept of corporate culture. An important aspect of auditing conflicts of interest will be the willingness of the organization's employees to recognize it and their ability to report it. This awareness requires an open, transparent, and trustworthy work environment. Internal auditors can contribute with the results of their audits.

Corporate behaviour and decision-making related to conflict-of-interest issues send a strong message to employees about what is acceptable. Those messages are built into employees' perceptions and their execution of everyday business activities, which can result in significant consequences for organizations.

Culled from: iia.org

7 Diet Decisions You Can Make To Live Longer.

If you are to ask many people to make one wish, it is certain that quite a number would wish for long life. However, we already know that if wishes were horses, beggars would ride.

You don't have to rely on wishes to live long when there are conscious diet decisions you can make to live longer.

These 10 diet changes can help you add years to your life.

Imbibe some wine

The occasional drink of red wine is good for your health according to the American Heart Association (AHA). AHA believes the antioxidants and other components found in red helps to reduce heart disease risk. For women, moderate consumption means no more than one glass each day. For men, no more than two.

Go meatless on occasion

A study from Loma Linda University found that people who eat very little meat live longer. Not only do vegetarians eat less saturated fat, they eat more whole grains, fruits, and vegetables, which are chock-full of vitamins, minerals, and antioxidants.

Eat some watermelon

Known for being a good fruit to fight cancer and heart disease thanks to its high lycopene content, watermelon is a good fruit to include in your diet.

Eat more (good) fats

That may not sound like the most health-conscious advice, but replacing saturated and trans fats with the good-for-you variety of fat (namely monounsaturated) can help lower bad cholesterol, raise good cholesterol, and cut your risk of atherosclerosis.

Eat fruits and vegetables

Eating fruits and vegetables regularly or multiple times each day has several health benefits. Eating fruits can protect the body's cells from harmful free radicals

Increase fibre intake

Research from 2008 found that the more fibre you eat, the lower your risk of coronary heart disease.

Go fish

Heart-healthy omega-3s have been shown to lower bad cholesterol, help the body combat inflammation, and reduce the risk of cancer and heart attack.

Culled from: guardian.ng

Important Things To Know About Heart Attacks

The heart is a pump responsible for distributing blood to the entire body. All of our cells, including those of the heart, require oxygen and nutrients which the blood supplies and a break in the supply of blood to them can cause cell death.

Myocardial infarction (MI) or commonly known as a heart attack, is the interruption of blood supply to the heart, usually by a blood clot, causing some heart cells to die. A heart attack is a serious medical emergency and can be life-threatening.

According to the World Health Organization, heart attacks led to over 9 million deaths in 2016 alone, making it the world's leading cause of death. A heart attack differs from a cardiac arrest (when the heart malfunctions and stops working).

How does a heart attack occur?

Most patients who suffer a heart attack have atherosclerosis, a condition where the inner walls of major blood vessels that carry oxygenated blood to the heart (called arteries) are lined by cholesterol or fat (called plaques). This leads to the narrowing of the area that blood passes through. The process of atherosclerosis is gradual and has no symptoms.

One of the plaques formed in the blood vessels typically breaks off right before a heart attack (referred to as plaque rupture) causing a blood clot to form at the site it once was. This clot causes the stoppage to the supply of the areas after the blockage, triggering a heart attack.

Although the blood supply can be restored to the areas affected, complications may arise causing the affected heart wall muscle to work sub-optimally or not to work at all.

What are the risk factors for a heart attack?

Risk factors are conditions that increase one's chances of developing a certain condition. For heart attacks, risk factors are as listed below:

1. Age: Heart attacks are commoner in men older than 45 years of age and women older than 55
2. Hypertension
3. Diabetes mellitus (and impaired glucose tolerance)
4. High cholesterol levels
5. Smoking
6. Family history of heart attacks or heart disease
7. High-fat diet
8. Drug misuse. Examples are cocaine and crystal meth
9. Obesity and physical inactivity

10. Ethnicity: South Asians are thought to have a 40-60% higher risk of CHD-related mortality compared to other populations

What are the signs and symptoms of heart attacks?

A heart attack is a medical emergency as it can be fatal. While most heart attacks cause symptoms, one may not have symptoms in some cases, especially if you are diabetic. The commonest symptoms seen include:

- A squeezing, choking or smothering severe chest pain or heaviness. The chest pain feels like great pressure on the chest that may cause breathlessness, and it can be felt in the neck, left arm, jaw and back
- Typically, the chest pain lasts for longer than 15 minutes and is not relieved by rest or changing positions
- Nausea and Vomiting
- Excessive sweating
- Coughing or wheezing
- Generalised weakness and light-headedness

How is the diagnosis of a heart attack made?

Doctors make the diagnosis of a heart attack from the history of complaints and the physical findings. In addition to these, blood, imaging and other physical tests, chief of which is the Electrocardiogram or ECG (which measures the electrical activity of your heart), are carried out to ascertain the type and location of the heart attack (the part of the affected). These investigations also indicate if there are other medical conditions or concerns.

How are heart attacks managed?

Once the diagnosis of a heart attack is established, immediate stabilisation and resuscitation begin. This typically involves pain management, oxygen delivery, and the administration of medications to help the heart cope better.

Thereafter, treatment is dependent on the type of heart attack you have had (based on the findings on the electrocardiogram or ECG).

Restoration of the blood supply to the affected parts of the heart is carried out via medications (aptly named clot busters) or surgical intervention (via a procedure called percutaneous coronary intervention).

While waiting for an ambulance or transfer to the hospital, it is helpful to chew and then swallow a tablet of Aspirin, if the person having a heart attack is not allergic to Aspirin.

Once the supply is restored, and treatment is completed, medications are offered to reduce the risk of developing another heart attack, and lifestyle modifications (examples are increased physical fitness or smoking cessation) are prescribed.

Complications from a heart attack may also happen after recovery. These may occur immediately after the attack or as late as six weeks after a heart attack, typically causing death or a reduction in quality of life.

How can you prevent a heart attack?

Preventing heart attacks is tied to reducing your risks. These steps are simple and effective. However, they cannot eliminate the chances of developing a heart attack. These steps include:

1. Quit smoking
2. Reduce your alcohol intake
3. Exercise regularly: Do around 30 minutes of aerobic exercises daily or around 150 minutes weekly
4. A healthy balanced diet: Eat low fat, high fibre diet
5. Lose weight, especially if you are overweight or obese
6. Manage any health conditions optimally. Examples are hypertension, kidney disease and diabetes.

Culled from: guardian.ng

The Role of IT Governance in Addressing Pandemic-Related Cyberrisk

The entire world is now grappling with the COVID-19 pandemic, which is turning out to be not only a massive health challenge, but also one of the most enormous economic challenges in recent history. With every passing day, thousands of positive cases are added to the already huge number of active cases. This one pandemic has taken scientists, researchers, politicians and policy makers the world over by surprise. Despite the many advancements in medical/clinical research and biotechnology, even the world's most advanced countries are struggling to find effective treatments and a vaccine to combat this deadly virus.

The pandemic has brought about several changes in lifestyles, work lives and the way people do business. The importance of IT governance in keeping the world's information systems on track has once again come to the fore. Top critics of IT have realized the importance of technology during these most challenging times.

Nearly everyone has embraced technology in some form or another:

- Conducting webinars/virtual meetings (official/personal), using CISCO Webex/Zoom/Google meeting platforms
- Placing shopping orders on Amazon
- Engaging in a virtual medical consultation with a physician
- Using a fitness app to remain active and healthy during lockdown
- Making mobile payments for services

Now schools, offices, even entertainment and dance classes, have gone virtual. Technology is now impacting all walks of life, directly or indirectly, in a real sense.

The proliferation of the use of technology has posed greater risk to people in all spheres of their lives. This

has created gold mines of opportunities for cybercriminals. India alone witnessed a 51% rise in the use of spyware and stalkerware in the period between March 2020 and June 2020, compared to January and February 2020, according to one report.1

> *"The appropriate adoption of IT governance becomes an inevitable solution to safeguard the interests of organizations, governments and individuals."*

In addition to individuals and society as a whole, organizations and financial institutions are more prone to cyberattacks. Some of the factors exacerbating the risk to IT systems and devices due to the spread of the pandemic include:

- **Poor security architecture** Because some applications (apps) and software have been hurriedly developed to meet the urgent demand created by the lockdown (e.g., apps developed by schools and universities for taking online exams), the necessary security aspects might have not been properly tested. This leaves some of these apps vulnerable to cyberattacks. Cybercriminals may try to exploit any vulnerabilities available in these rapidly developed systems

- **Dilution in security protocols** The COVID-19 pandemic has sparked the need to dilute some security protocols, particularly physical access controls, such as those used in biometric access systems, to avoid direct touch and maintain social distancing. This makes organizations more vulnerable to physical access penetration and uninterrupted intrusion to IT infrastructure (i.e., server rooms, data centers, desktops devices, printers). In addition, intruders are able to hide their identity by wearing masks that are not often objected to now.

- **Scalability.** The sudden surge in usage of apps/software is also posing a risk of scalability, as they would have been developed to accommodate an estimated number of users/activities in the normal course of events. However, due to the significant increase in hits on these apps/websites, there is extra load on servers, which might make them prone to a denial of service or crashing. For example, now more people have shifted to Internet and mobile banking. According to one report, consumer mobile app use increased 40% during lockdown.

- **Load on networks** As more people shift to a digital lifestyle, the load on networks/bandwidth has suddenly increased, posing the risk of breakdown or clogging of networks. According to a World Economic

- Forum article, between the first and second quarters of 2020, health and fitness app downloads increased by 46% worldwide.

- The regional breakdown is shown in figure below.

Health and Fitness App Downloads (Q1-Q2, 2020) by Region

Region	Download Growth
India	157%
Middle East and North Africa (MENA)	55%
Europe	25%
Asia-Pacific	47%
Rest of the world	43%
Americas	21%

Source: Ang, C.; "Fitness Apps Grew by Nearly 50% During the First Half of 2020, Study Finds," World Economic Forum, 15 September 2020, Visual Capitalist. Reprinted with permission.

- **Newer avenues** The pressing need to embrace technology has forced almost every industry, organization and individual use technology in some form or the other. This has opened new avenues for cybercriminals to exploit. For example, new phishing emails in the name of COVID-19 have started spamming many inboxes with subject lines such as "Know the COVID Status of Your City/Country," "Access Authorized COVID Labs/Hospitals in Your City" or "Claim Your COVID Subsidy by Clicking a Link." Calls are being placed by fraudsters, informing individuals of a government COVID subsidy having been credited to their bank account, which they can access if they share their automated teller machine (ATM) card details. Furthermore, it is possible that software developers who lost their jobs may get into the unethical business of hacking due to their lack of employment.

- **Video call apps** The current crisis has mandated that most individuals work from home and use technology as much as possible when performing their duties. This has provided office headquarters direct entry into employees' homes when they are connected through video calls. If these video calling apps are hacked, bad actors can peer into employees' homes, thereby directly infringing on their privacy.

- **Unemployment** The pandemic has led to a drastic reduction in economic activities, at almost all levels across economies, leading to a significant rise in job losses. This has rendered many people unemployed. It is not outside the realm of possibilities that some who are unemployed may explore ways to make money illegally. They may try new ways of committing fraud, cyberfrauds in particular, due to the more fertile and conducive environment available now as a result of the pandemic.

- **Lack of public awareness** From the user's standpoint, an unprecedented increase in the use of IT systems/devices is a serious risk. The uninformed public is now forced to adopt these technologies, to which they may have previously been oblivious, due to restrictions imposed on the physical world. Many of them are first-time users in the virtual world and may not have been trained on cyber- and other-related risk issues these devices/systems bring. Making the public aware in a short period of time of the risk involved in using these devices/systems is challenging, which may render more people easy targets of cyberattackers.

IT Governance During the COVID-19 Pandemic

Although it will be difficult to contain the mounting risk arising from the enhanced use of technology by individuals and organizations, there is a need to respond to the governance challenges posed by the pandemic with the same vigor as health professionals and governments have responded to the health issues.

The appropriate adoption of IT governance becomes an inevitable solution to safeguard the interests of organizations, governments and individuals. There are several governance and security frameworks (e.g., COBIT, ITIL, International Organization for Standardization [ISO]/International Electrotechnical Commission [IEC] ISO/IEC 27002, ISO/IEC 38500) available in the IT space and it is up to organizations and governments to select the appropriate ones for them and determine the extent to which they adopt them. These governance frameworks provide globally acceptable standards, principles, practices and tools that create trust in and value from IT and can protect not only organizations, but also individuals.

COBIT 2019, the latest version of COBIT, is one such framework that provides effective principles and appropriate tools for leveraging multiple frameworks and standards under a single integrated framework. COBIT is now widely accepted and practiced by IT organizations worldwide for the governance of enterprise IT.

Conclusion

During these times, organizations cannot afford any laxity. They must strengthen their existing IT governance frameworks or adopt new ones, if they have not already done so. These frameworks enable organizations to manage their IT risk effectively and ensure that their IT processes are well aligned with the overall business objectives.

Organizations should see this as an opportunity and a reason to convince their boards and senior management to align their IT governance framework with risk management and compliance frameworks, within the overall governance framework of the organization, before it is too late.

Culled from: isaca.org

Internet of Things (IoT) - An Overview of IoT and the Audit Perspective

The Internet of things (IoT) is any physical device internet enabled. They can also be referred to as Smart devices. They are the various devices around the globe now connected to the internet, collecting and sharing data. This is made possible by the availability of wireless networks and computer chips. Hence, it is possible to turn anything even as tiny as a pill to something as big as an Airplane, being an IoT. The connecting of different objects and adding sensors adds another level of digital intelligence to the devices, thereby enabling them to communicate real time data. This makes the world connected in a smarter and simpler way.

The term IoT is mainly used for devices that wouldn't usually be generally expected to have an internet connection, and that can communicate with the network independently of human action. For this reason, a PC isn't generally considered an IoT device and neither is a smartphone, even though the latter is crammed with sensors. A smartwatch or a fitness band or other wearable device might be counted as an IoT device.

History of IoT

The idea of adding sensors and intelligence to basic objects was discussed throughout the 1980s and 1990s (and there are arguably some much earlier ancestors), but apart from some early projects-including an internet-connected vending machine-progress was slow simply because the technology wasn't ready. Chips were too big and bulky and there was no way for objects to communicate effectively.

Processors that were cheap and power-frugal enough to be all but disposable were needed before it finally became cost-effective to connect up billions of devices. The adoption of RFID (Radio Frequency Identification) tags; low-power chips that can communicate wirelessly and solved some of this issue, along with the increasing availability of broadband internet and cellular and wireless networking. The adoption of IPv6-which, among other things, should provide enough IP addresses for every device the world (or indeed this galaxy) is ever likely to need was also a necessary step for the IoT to scale.

Kevin Ashton coined the phrase 'Internet of Things' in 1999, although it took at least another decade for the technology to catch up with the vision.

"The IoT integrates the interconnectedness of human culture; our 'things' and the interconnectedness of our digital information system -- 'the internet.' That's the IoT," as explained by Ashton to ZDNet.

How Secure is the Internet of Things?

Security is one the biggest issues with the IoT. These sensors are collecting in many cases extremely sensitive data; what you say and do in your home, for example. Keeping that secure is vital to consumer trust. Hitherto, IoT's security track record has been extremely poor. Too many IoT devices give little thought to rudimentary security issues, like encrypting data in transit and at rest.

Flaws in software, even in old and well-used codes are discovered on a regular basis, but many IoT devices lack the capability to be patched, which means they are permanently at risk. Hackers are now actively targeting IoT devices such as routers and webcams because their inherent lack of security makes them susceptible to compromise and roll up into giant botnets.

Flaws have left smart home devices like refrigerators, ovens, and dishwashers open to hackers. Researchers found 100,000 webcams that could be hacked with ease, while some internet-connected smartwatches for children have been found to contain security vulnerabilities that allow hackers to track the wearer's location, eavesdrop on conversations, or even communicate with the user.

Governments are growing worried about these risks . The UK government has published its own guidelines around the security of consumer IoT devices. It expects devices to have unique passwords, that companies should provide a public point of contact so anyone can report a vulnerability (and that these will be acted on), and that manufacturers should explicitly state how long devices will get security updates. It's a modest list, but a start. When the cost of making smart objects becomes negligible, these problems will only become more widespread and intractable.

Connecting industrial machinery to IoT networks increases the potential risk of hackers discovering and attacking these devices. Industrial espionage or a destructive attack on critical infrastructure are both potential risks. That means businesses will need to make sure that these networks are isolated and protected, with data encryption with security of sensors, gateways and other components a necessity. The current state of IoT technology makes that harder to ensure, however, as does a lack of consistent IoT security planning across organizations. That's very worrying considering the documented willingness of hackers to tamper with industrial systems that have been connected to the internet but left unprotected.

The IoT bridges the gap between the digital world and the physical world, which means that hacking into devices can have dangerous real-world consequences. Hacking into the sensors controlling the temperature in a power station could trick the operators into making a catastrophic decision; taking control of a driverless car could also end in disaster.

Internet of Things and the cloud

The huge amount of data that IoT applications generate means that many companies will choose to do their data processing in the cloud rather than build huge amounts of in-house capacity. Cloud computing giants are already courting these companies: Microsoft has its Azure IoT suite, while Amazon Web Services provides a range of IoT services, as does Google Cloud.

Procedures for Auditing IoT

ISACA established a process for Auditing IoT and explained in five steps:

1. **Determine the Audit Subject**
   It is necessary to determine the Audit Subject by answering the key question of -What are you Auditing?

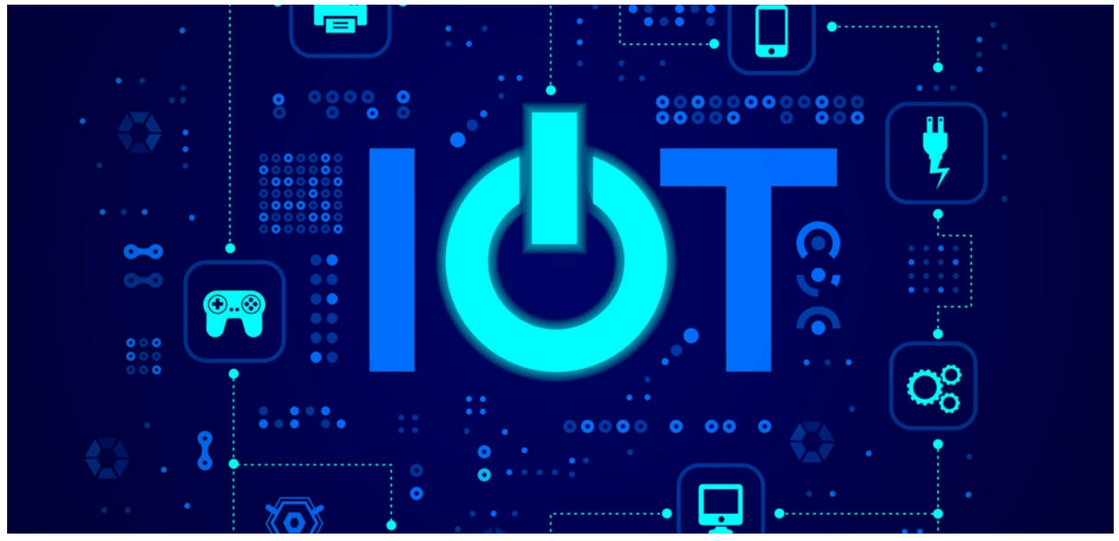
2. **Define the Audit Objective**
   Once you determine the Audit Subject, we need to establish the objective of the audit. Why are we auditing it? From an auditor's perspective, it is advisable to adopt a Risk-based approach (Figure 1) and define the objective for the Audit

Figure 1: IoT Risks

Risk Category	Examples
Business	Health and Safety Regulatory Compliance User Privacy Unforeseen Costs
Operational	Unauthorized Access Performance Authorization and Controls
Technical	Device Vulnerabilities Device Updates Device Management

3. Set Audit Scope

The Audit scope should identify the actual IoT device that is meant to be audited. Hence, we must be able to determine the limits of the Audit. This involves identifying the supporting infrastructure such as the connectivity and data collection methods, the cloud or other storage means, and the algorithms used for processing the data.



4. Perform Pre-Audit Planning

This involves Risk Assessment based on the Scope of the Audit. It involves answering questions such as:

How will the Device be used from a business perspective?

What threats are the device exposed to?

How is access to the device established and if identity will be proven?

What is the process of updating the device in case of an attack on the vulnerabilities?

Who monitors the device?

Have we established all risk scenarios?

What personal information is obtained by the device?

Do the users know that their information is stored by the device?

With whom will the data be shared?

5. Determine the Audit Procedures and Information Gathering Steps

At this stage, enough information and data must have been gathered to select an Audit approach or strategy to develop the Audit program

General baseline controls- Minimum controls that need to be applied to all aspects of the technology

Data-related controls- Such as controls that apply to the data forming a key part of IoT

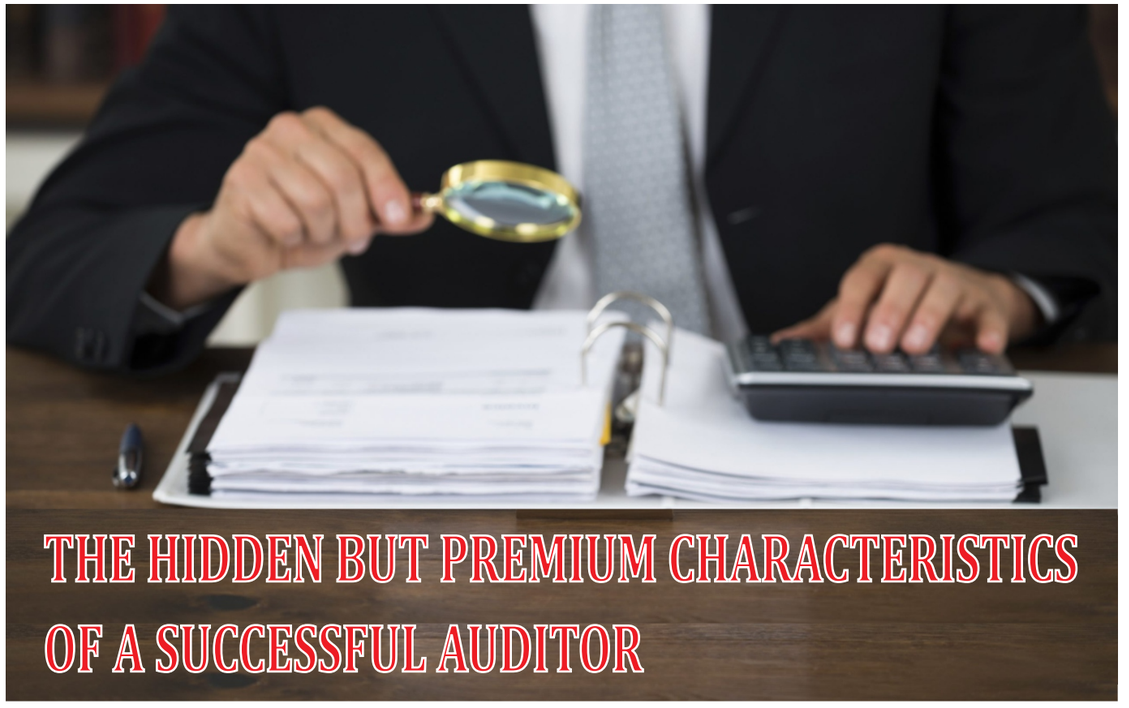
Analysis and learning-related control- Applied to ensure that the analysis is ethical and enables trusted use of the data and that outcomes of analysis can be applied to business decision-making

Business and process alignment - Related aspects which ensure that the IoT implementation is aligned to business needs and that business benefits are delivered as required

Conclusion

As will be the objective of any Audit to provide Assurance for any business decision, Information technology audits determine whether IT controls protect corporate assets, ensure data integrity and are aligned with the business's overall goals.

Francis Uzoewulu
Keystone Bank Limited



THE HIDDEN BUT PREMIUM CHARACTERISTICS OF A SUCCESSFUL AUDITOR

Have you got what it takes to be a good auditor? The required skills go beyond learning debits and credits and completing checklists.

The today's auditor must display dynamism, high technical capacity, and empathy in the discharge of his expected duties but should also not let any irregularity fly across without any form of escalation.

In order to be precise and concise, some key characteristics which yesterday's auditor saw as inconsequential have been itemized below.

THE CHARACTERISTICS

A) Vision and Instinct

Working as an auditor enables such a person gain experience particularly when he/she works with numerous clients in multiple industries. Such experience allows a good and willing auditor gain the ability to instinctively understand what the client's business is about. While carrying out the audit, he/she can identify issues within the business and also interpret what they could mean in the future. There is an anonymous quote that states that "instinct is the nose of the mind." The good auditor does not settle when a client's answer or transaction does not seem right.

Instinct causes him or her to dig deeper to arrive at a conclusion that fits with the vision of the business. To develop instinct and vision, the auditor must develop an inquiring mind and strive to learn from all experiences encountered in client situations throughout his or her career.

B) Being able to see the BIG picture

This defines that auditor's ability to quickly frame a picture of the client's business, the organization, and key attributes within it. A good auditor is able to sort out connections and linkages within the organization to focus the audit approach. The ability to see this big picture is very important to the planning stages of the audit. Putting the audit plan together requires an appreciation and an understanding of the organization and what constitutes a logical approach to the audit.

The audit checklist approach tends to cloud the big picture because of the large number of questions that are asked. Many auditors in their attempt to get all the questions completed typically do not take to time to step back and ask, "What does all this mean." Good auditors will have a much shorter list of targeted or strategic questions that are developed specifically for their client which allows him or her to focus on the big picture.

C) People Skills

The audit profession is not all about ticking and

tying; it is about people. Auditors need to have exceptional people skills. They need to have the ability to deal with all types of clients in all types of clients' diverse situations. In certain cases, client personnel have a fear of the auditor because they do not like someone looking over their shoulders. So, the auditor must have the ability to put client personnel at ease and be able to empathize from the client perspective. It is also important for the auditor to show respect for the client. After all, it is the client who is paying for the audit. The most often overlooked people skill is listening. Listening seems like a simple concept, but few do it well.

Many auditors listen to hear the answer they want to hear rather than to listen for understanding. Most audit checklists ask closed-ended questions which prevent the client from elaborating on a situation. When the client does expand their answer, the auditor must "hear" the client's answer completely; missing one small piece of the answer can cause them to miss the message entirely. Lastly, people skills are also very important within the audit team. Auditors need to be team players as the entire team is working toward a common goal.

D) Decision making ability

Once the audit evidence is accumulated, the auditor needs to determine what is relevant and what is not. Making these decisions is, at times, not easy as there is so much different information accumulated or clustered together and review them to bring out value might be challenging. Decision making can be hard. Most decisions involve some conflict or tradeoff. The challenging part is to select the best decision given the information that you have gathered to assist with the decision. There is a tendency to put off the decision by concluding that you need more information, only to again later conclude that you need even more information.

This decision paralysis can cause the audit to drag on and on and can ultimately cause the auditor to feel pushed to the wall as they now must decide because the client needs their financial statements immediately. Clients want their auditor to be strong and effective decision makers without prejudices or cowardice. Waffling around on a decision causes the client to lose confidence in their auditor.

E) Leadership

Great leaders have the desire to help others succeed. A famous producer once said, "Don't celebrate a fault, but celebrate the remedy." This statement is a classic in the context of leadership; leaders find solutions, they do not place blame. An auditor that is a leader finds solutions to complex problems and has the ability and skill to assist in getting the solutions implemented. A good auditor must strive to become a successful leader. Leadership characteristics can be taught but leadership must be earned day in and day out. Leadership is seen by the client as the auditor being a teacher and/or a trusted confidant. An audit staff member sees a leader as a mentor and coach. No single audit or audit firm, for that matter, can rise above the quality of its leadership. A common theme on every well-run audit or well-run audit firm can be directly linked to leadership.

F) Superior Communication Skills

This skill enables the auditors to have connection and rapport with others on the staff, managers, partners, and clients. The technological world in which we live today can negatively impact the audit staff's ability to become an effective communicator, especially when e-mail becomes a substitute for face-to-face communication with audit clients. A good auditor recognizes the importance of face-to-face communication and strives to make it the primary mode of communication. It is essential that all auditors work to make verbal communication a priority rather than a last resort.

In most cases, e-mail should be the last resort rather than the first resort. Clients want to talk to the auditor, and the better the auditor is at effective communication, the better the conversation is with the client. Effective communication occurs when the client understands exactly what you are saying. Achieving this is not easy but once achieved, it will set you apart from the rest.

Conclusion

The characteristics of a good auditor start with the basics of sound technical ability and solid ethical foundation. A good auditor considers those as baseline and work to grow beyond the "rules and regulations" mindset of the profession. Attaining and maintaining the characteristics mentioned in this article require personal commitment which are crucial to the auditor's long-term success. Have you

Bolanle Alalade
(ProvidusBank Ltd)

Security Tips for Working Remotely over VPN in the New Normal

With the advent of COVID-19, millions of employees around the world now work from home. In this new normal, organizations have capitalized their Virtual Private Network (VPN) requirements to meet the high demands of remote working and connectivity. This development makes VPNs crucial as one of the entry points to accessing office networks. A poorly developed VPN could have far reaching consequences such as the introduction of malware to the network and unfettered access to corporate and confidential data.

Virtual Private network (VPN) allows individuals to access a private network (e.g. a corporate network) from a public or shared network through a secure tunnel. For instance, an employee could access data resources and applications hosted on the employer's server directly over the internet from the comfort of their home. Generally, VPNs provide a safe connection, encrypt data between the sender (client) and the receiver (server), enable a user bypass web/ location-based filters and also allow for anonymity while surfing the internet.

While VPNs are advantageous, they increase the points of possible failure hence they are less reliable, they can reduce connection speed depending on the size of resources being transferred by various individuals, they do not also provide absolute anonymity as logs may be recorded. VPNs could also be expensive, with the cost increasing with the number of connections. They may also allow the transmission of malware such as Dialers, Worms, Keystroke loggers, Trojan horses and Hacker tools to the private network.

Two common types of VPNs include Personal or Home and Corporate VPNs. Personal or Home VPNs are very easy to install, users do not require specialized

technical expertise to use them. They allow users to bypass web or location-based filters, prevent Internet Servers Providers (ISPs) from tracking personal online activity and protect the privacy of individuals by not logging user activities (although there are exceptions depending on the VPN service providers). On the other hand, Corporate or Businesses VPNs are precisely meant for business use and allow employees secure encrypted connections to a corporate network.

Unlike Personal VPNs, they require specialized technical skills for setup and maintenance; they could be used to restrict threats by whitelisting Internet Protocols (IP) and allowing static IP addresses; they allow for global administrations such as users management and policy settings tuning.

In this new era of remote working, most corporate organizations use Remote Access VPNs which allows employees in remote locations establish secure online connections. Remote Access VPNs sometimes include:

a. Administration tools, such as VPN dashboards and Security management server.

b. Certificate management center or Trust entities, such as Internal Certificate Authority.

c. Endpoints such as Security Gateways and remote client's devices

Some important considerations when reviewing Corporate VPNs include:

1. Ensure that the latest vendor recommended patches are applied on all edge/gateway appliances and all VPN infrastructure and products.

2. Confirm that VPN infrastructure are configured in line with vendor recommendations/organization policy and that the vendor is easily reachable for support issues.

3. Check if organization approved procedure is followed before VPN access is granted.

4. Ascertain that periodic review of the list of devices with VPN installation is done.

5. Ensure that only trusted terminals can access corporate resources via VPN and checks are done to confirm the endpoint's identity and security posture.

6. Ensure that VPN access is granted only after inputting multi-factor authentication such as passwords and randomly generated one time passwords from a hardware token device.

7. Confirm that appropriate logging of user activities is done during remote access; logging of all events on VPN infrastructure.

8. Check that monitoring of VPN infrastructure for system utilization, temperature and unauthorized activity is being done.

9. Ensure that VPN users are trained on safe ways to use VPN access in the line with the organizations policy.

10. Review that configuration is done at the backend that ensures users can be connected to VPN on one device per time or from a known Mac address.

11. Confirm that when using VPN remote access, role based restrictions to organizational resources are enforced.

12. Ascertain if all vendor default VPN accounts are disabled on all infrastructure before connecting to the internet.

Adaeze Ugwu, CISM, CISA, CEH, OCJP, MCTS, ITIL.
Union Bank of Nigeria Plc

LEADING AN EFFECTIVE VIRTUAL TEAM

Many managers are used to seeing their subordinates in the office on a weekly basis but due to the recent COVID-19 pandemic, a lot of people now work remotely. Many studies have shown that employees are more productive when they have to skip commuting and work from home or a conducive place around. As a result, there has been a rise in the popularity of remote work, hence, leading virtual teams effectively has never been more important.

Irrespective of the location of the team (onsite or offsite) the leadership principles are the same. Managers are to reduce the virtual distance by establishing an environment where members of the team feel psychologically and emotionally connected to the business and to one another.

Tips for leading a virtual team:

There are tested and working leadership strategies that are effective in leading employees. Managers have to adapt this leadership approach when it comes to leading a virtual team.

1. Team Operating Agreement.

A team operating agreement should be established for a virtual team. This is a document written by the members of a team and it defines the team's purpose, results, and goals. It includes the agreements for managing work procedures, methodologies, and communication protocols. This will assist the team to know the nitty-gritty of working remotely and decrease challenges as they occur.

2. Leverage on technology that encourages communication

In a remote environment, employees do not have the opportunity to walk up to other colleagues to ask questions. Also, a virtual team does not have the environment that closely support building a team and strengthening friendship. When it comes to leading a virtual team with the use of technology, the best thing to do is to keep it simple while equipping the team members with the appropriate tools that encourage communication.

One of the main reasons technology is underutilized is because some people do not have the skills required to use them. A few tools should be selected and used constantly. Chat tools such as WhatsApp and video tools such as Teams should be implemented.

In getting across with one another in a team, chat tools are much easier than having to send an email or make a call. Also, video tools are used by some employers to organize virtual meetings and virtual company parties. Virtual meetings are more engaging with video conferencing due to the face-to-face aspect of it. Members using video conferencing are to ensure that their faces are distinctly visible and well-lit on the screen.

3. Check-in, but do not micromanage

Micromanaging has been argued to be the least motivational thing that can be done for an employee. Only few employees feel that their performance is supervised in a motivating way. Innovation begins when there is freedom which is how mutual respect is formed. Virtual team members are to be managed in a non-toxic way by avoiding their disengagement and frustration. There should be short standups at the begin of the day which is a way to check-in without micromanaging. Doing this will help to ask and know what employees are doing and also give tips on the way to do it.

4. Streamline Process and Procedures.

In a virtual environment, it is ideal to streamline the various work processes. Team members should be involved in assessing the way to get work done as a team. Duplication of efforts are to be identified and the ways to leverage on technology should be discovered. In addition, before new procedures are implemented extensive testing should be done.

5. Ask for employee feedback

In a physical office environment, getting the feedback of employees is somewhat easy. This is usually done by conducting regular performance reviews, keeping the office door open or having a suggestion box in the open. Also, requesting for feedback of employee is just as easy as when leading a virtual team. This can be achieved by hosting virtual meetings, conducting performance review online and distributing online surveys. Getting employees feedback is very important when leading a virtual team.

6. Establish Performance Indicators

When employees work from home, it is mostly a common concern from them when the work they accomplished is not being recognized. It is imperative to have a discussion with employees about their expectations when they work remotely. Having a team member dashboard can assist a team member to track, identify and access lead and lag indicators.

7. Provide ongoing training opportunities, online

Training of employees should not cease after onboarding. This should be an ongoing exercise throughout the lifecycle of the employee. When leading a virtual team, online training opportunities can be taken advantage of for employees to participate in. These online trainings include certifications, workshops, and classes.

Employees may also be encouraged to independently search for training opportunities in their areas of expertise for which they would be reimbursed. A training reimbursement policy should be established so that the virtual members know how to get their programs approved.

8. Out of sight is not out of mind when it comes to praise

In a virtual environment, employees may be forgotten to be praised and thanked for their accomplishment which is always a big mistake as employee recognition is very important in the workplace. Research shows that employees that are not recognized reported being twice as likely to resign in the next year. Always take note of employees who go above and beyond in a virtual environment. Bonuses and extra paid time off may be considered in addition to recognizing top performing employees with praise. In addition, this should be done in the presence of other team members in order to encourage them.

CONCLUSION

Studies have shown that virtual teams can outmatch their physical teams when established and managed the right way. Leading virtual teams entails a little bit more than simply managing them. Irrespective of whether a team is exclusively virtual or semi-virtual, a manager has to be able to motivate and influence the team members from afar. While it can be difficult to establish a strong culture that is required of all great teams, some of the tips discussed above can help in building an effective virtual team.

Bolaji Ajayi
(ProvidusBank Ltd)

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

Bank of Agriculture Limited
Daniel Olatomide
1 Yakubu Gowon Way
Kaduna.
d.olatomidei@boanig.com
08067007183

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

Central Bank of Nigeria (CBN)
Lydia I. Alfa
Plot 33, Abubakar Tafawa Balewa
Way Central Business District,
Cadastral Zone, Abuja,
Federal Capital Territory, Nigeria
lialfa@cbn.gov.ng
08033177216

Citibank Nigeria Ltd
Bolaji Ajao
27 Kofo Abayomi St
Victoria Island, Lagos
bolaji.ajao@citi.com
Tel: (234)1 2798400, 4638400 Ext. 8446
DL: (234)1 2798446, 4638446.
Mobile - 07057878877

Coronation Merchant Bank Ltd
Dele Dopemu
10, Amodu Ojikutu Street
Victoria Island,
Lagos.
ddopemu@coronnationmb.com
01-4614892, 07034109732.

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

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

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

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

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

First Bank of Nigeria Ltd
Uduak Nelson Udoh
9/11, McCarthy Street, Lagos
Uduak.udoh@firstbannigeria.com
01-9054583, 08022902268

First City Monument Bank Ltd
Amarachukwu Okogbue
10/12 McCarthy St,
Lagos.
amarachukwu.okogbue@fcmb.com
08033062602

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

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

Guaranty Trust Bank Plc
Segun Fadahunsi
178, Awolowo Road, Ikoyi, Lagos
segun.fadahunsi@gtbank.com
08023285640

Heritage Bank Ltd
Prince Akamadu
130, Ahmadu Bello Way,
Victoria Island, Lago
Prince.akamadu@hbng.com
08037649757

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

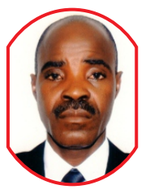
JAIZ BANK PLC
Abdullahi Usman
No. 73 Ralph Shodeinde Street,
Central Business District,
P.M.B. 31 Garki Abuja,
Nigeria.
ABDULLAHI.USMAN@jaizbankplc.com
09-4605138, 08032089010,
08086103555

Keystone Bank Limited
Clifford Odiase
707 Adeola Hopewell Street,
Victoria Island, Lagos
CliffordOdiase@keystonebankng.com
09087500658, 07035385884

NEXIM BANK
Mr Ichide Friday
NEXIM House
Plot 975 Cadastral Zone AO,
Central Business District,
P.M.B. 276, Garki,
Abuja, Nigeria.
ichidejnr@gmail.com
07085122928.

Nigeria Mortgage Refinance Company
Samuel Ekanem
No 18 Mississippi Street,
Off Alvan Ikoku Way
Maitama,
Abuja, Nigeria
sekanem@nmrc.com.ng
08023394068

Nova Merchant Bank
Ifeatu Onwuasoanya
23, Kofo Abayomi Street
Victoria Island, Lagos.
Ifeatu.onwuasoanya@novambl.com
08024114481



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

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

Rand Merchant Bank
Femi Fatobi
3RD Floor, Wings East Tower,
17A, Ozumba Mbadiwe Street
Victoria Island, Lagos
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.
Emeka Owoh
142, Ahmadu Bello Way
Victoria Island, Lagos
emeka.owoh@sc.com
08037027452

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

SunTrust Bank Nig. Ltd.
Adedokun Aremu
1, Oladele Olashore Street,
Off Sanusi Fafunwa Street,
Victoria Island, Lagos
adedokun.aremu@suntrustng.com
09038989319, 08020663423

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

Union Bank of Nigeria Plc
Kabir Garba
36 Marina,
Lagos.
unionbank,com
08033028899

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

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

Wema Bank Plc.
Adekunle Onitiri
Wema Towers
54 Marina, Lagos
adekunle.onitiri@wemabank.com
+234 1 4622364, 08022245818

Zenith Bank Plc.
Mogbitse Atsagbede
Plot 84 Ajose Adeogun St
Victoria Island, Lagos
mogbitse.atsagbede@zenithbank.com
08023270998