Association of Chief Audit Executives of Banks in Nigeria

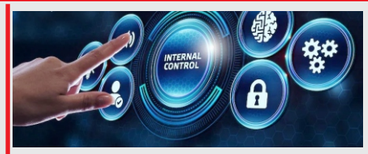
Design+printbyProwess08039221516

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, 2023

International Standard on Quality Management (ISQM)1 Implementation Challenges



Internal Control Over Financial Reporting (ICFR)... Page 21

Page 17

Fraud Prevention in the Digital Age: Emerging Risks and Best Practices to ... Page 6

ACAEBIN EXCO MEMBERS

Prince Akamadu
Chairman

Aina Amah
1st Vice Chairman

Mogbitse Atsagbede
2nd Vice Chairperson

Ugochi Osinigwe
Treasurer

Olusemore Adegbola
Auditor

Olusegun Famoriyo
Chairman, Research & Publication Sub-Comm.

Femi Fatobi
Chairman, Payment & Systems Sub-Comm.

Adeola Awe
Ex-officio I

Olurotimi Omotayo
Ex-officio II

CONTENT

Our Mission Statement

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

Editorial Team

Segun Famoriyo
Aina Amah
Olusemore Adegbola
Femi Fatobi
Ugochi Osinigwe
Adeola Awe

Editorial

Dear Colleagues and Readers,

Let me use this opportunity to wish everyone merry Christmas and Happy New Year in advance.

As we navigate the intricate landscape of internal audit, this quarter's magazine delves into crucial facets that shape our profession and influence organizational resilience. We kick off with an insightful exploration of the challenges inherent in ISQM1 implementation, shedding light on the intricacies of adherence and the road ahead. In the ever-evolving digital age, our second feature underscores the imperative of fraud prevention. "Fraud Prevention in the Digital Age: Emerging Risks and Best Practices" providing a comprehensive guide to staying ahead in this dynamic landscape, with emphasis on the fusion of vigilance and innovation. Chief Audit Executives play a pivotal role in ensuring compliance with regulatory frameworks.

Our third article brings you the latest updates, providing a compass for navigating the ever-changing seas of compliance requirements. Beyond the audit realm, we recognize the significance of personal well-being. "How Simple Lifestyle Measures Add Years to Your Life" offers a holistic perspective, reminding us that a healthy internal auditor is key to robust organizational health.

Also, the article on the Psychology of Corporate Fraudsters: Motivating Factors and Deterrent Strategies takes a cursory look into the psyche behind white-collar deception, motivation motivation and mitigation strategies for effective and secure corporate landscape.

As the financial landscape diversifies, understanding the nuances of Non-Interest Banking becomes imperative. Our article on Non-Interest Banking does justice to that.

Lastly, we dissect the critical role of internal control over reporting by exploring the fundamental role in maintaining the integrity of financial reporting.

As we absorb the insights shared in these articles, let us collectively embrace the opportunities and challenges that lie ahead. This edition has been packaged to address discoveries, learning, and growth in the realm of internal audit for your reading pleasure.

Once again, compliments of the season.

Olusegun Famoriyo
Editor-in-Chief

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

International Standard on Quality Management (ISQM)1 Implementation Challenges

The International Standard on Quality Management 1 (ISQM1) plays a basic role in establishing and maintaining robust monitoring and remediation methods within the complex terrain of auditing. This standard provides the foundation, ensuring high-quality evaluations and the implementation of appropriate corrective measures within auditing systems. Its relevance lies in leading auditing procedures toward retaining precision, integrity, and perfection in evaluations, hence, strengthening the auditing process's trustworthiness and credibility. In this article, we investigate the significance of ISQM1, important advancements in 2023, and predicted trends shaping 2024, giving auditors insights into adjusting to changing standards.

Understanding ISQM1

ISQM1 is a cornerstone of quality management systems for organizations performing audits, financial statement reviews, and other assurance services. Its relevance goes beyond merely being a regulatory guideline, functioning as a guiding beacon that upholds the essence of quality and integrity within the auditing area.

ISQM1 orchestrates the architecture of robust quality management systems at its heart. It presents a framework for organizations to build their operations while adhering to the highest precision, dependability, and ethical conduct standards. This standard is more than just a checklist; it's a thorough road map that leads auditors to be meticulous and exceptional in their assessments.

ISQM1's essence resides in its capacity to synchronize many components of auditing processes. It ensures that businesses build methods that allow for effective monitoring and remediation. By establishing strict rules, it develops a culture in which continuous improvement is not only encouraged but also engrained in the ethos of audit practices. ISQM1 essentially serves as the foundation upon which auditors create trust, reliability, and a reputation for consistent quality in their services.

ISQM1 is a catalyst for upgrading auditing methods to the point where every evaluation, review, or assurance service resonates with dependability and precision. It's the framework that auditing companies use to fine-tune their processes and align them with globally accepted best practices. As a result, this standard enables organizations to provide assessments and assurance services that do more than just meet criteria; they also set quality and integrity benchmarks.

Key Developments in 2023

Refinement of Quality Management Systems: Elevating Standards

The year 2023 encouraged auditing firms to conduct extensive introspection, focused on refining their existing quality management systems to fulfill the stringent ISQM1 criteria. This process of refining was not only about compliance but also about raising the standards of auditing methods. Firms conducted thorough audits of their processes, procedures, and protocols, finding areas for improvement and methodically aligning them with the tight requirements proposed by ISQM1.

Integration of Advanced Technologies

The noticeable shift toward incorporating cutting-edge technologies within auditing methods was a defining aspect of 2023. Recognizing the potential of technology to transform their operations, auditing firms enthusiastically embraced advanced tools and software solutions. From sophisticated data analytics algorithms to AI-powered solutions, these technological interventions aim to boost monitoring skills and enable auditors to manage huge datasets quickly and effectively.

Strengthening Monitoring Capabilities

The strategic incorporation of technology dramatically improved auditing organizations' monitoring capacities. This change provided auditors with real-time monitoring capabilities, allowing them to examine vast amounts of data with remarkable speed and precision. The use of automated monitoring systems aided in the early detection of abnormalities or inconsistencies, allowing for proactive interventions and rapid corrective steps.

Efficiency Enhancement in Irregularity Identification
The combination of improved quality management systems and cutting-edge technology resulted in more efficient detection of abnormalities during audits. Auditors, armed with advanced tools, developed the ability to quickly identify irregularities. This accelerated detection not only accelerated corrective efforts but also permitted auditors to take preventive measures, assuring the early repair of possible faults before they worsened.

Expected Changes in 2024

Refined Regulatory Guidelines

Changes in ISQM1 implementation expected in 2024 signal a phase of revised regulatory rules. Regulatory agencies are likely to implement stricter criteria, emphasizing the critical necessity for exacting quality management processes within auditing businesses. These updated principles attempt to create a more comprehensive framework that requires adherence to higher levels of precision, honesty, and ethical behavior.

Emphasis on Technological Evolution

ISQM1's trajectory in 2024 is expected to be strongly interwoven with technological advancement. Changes on the horizon indicate a considerable shift toward employing modern technologies not just for detection but also for proactive remedial activities. The emphasis shifts to predictive analytics and technology-driven that enable auditors to foresee abnormalities or future difficulties, paving the door for a more proactive approach to risk mitigation and discrepancy resolution.

Robust and Predictive Approach

The adjustments expected in 2024 aim to strengthen auditing methods by encouraging a more rigorous and predictive approach. These modifications are intended to provide auditing firms with tools and techniques that go beyond reactive actions. Instead, auditors are set to take a forward-thinking approach, leveraging technology to anticipate and rectify potential abnormalities before they materialize, thereby improving audit effectiveness and dependability.

Integration of Comprehensive Measures

Changes in ISQM1 implementation expected in 2024 center on incorporating comprehensive measures aimed at assuring proactivity in auditing processes. Auditors are expected to take a comprehensive strategy that blends severe regulatory compliance with cutting-edge technical solutions. This integration is intended to enable auditors to conduct audits with greater precision, alertness, and a proactive attitude toward upholding the highest quality and integrity standards.

Adapting to Evolving Standards

Adapting to the dynamic criteria outlined in ISQM1 necessitates auditors taking a comprehensive approach. It goes beyond simply compliance, urging a proactive embracing of these principles in order to improve audit quality. This adaptation means incorporating technological advances into current quality management systems, cultivating a culture of continuous improvement, and emphasizing preventive actions to address possible concerns proactively. Embracing these developing standards allows auditors to do more than just meet requirements; it allows them to proactively improve the quality and efficacy of their audits.

Conclusion

The significance of ISQM1 in shaping monitoring and remedial methods is critical. Adapting to its changing criteria necessitates a proactive approach that includes the use of technology, ongoing education, and encouraging collaboration between auditors and audited businesses. Start where you are, sign up to our newsletter and get information to help stay ahead of your competition in the ever-changing auditing landscape.

Culled from: auditproo.com

Fraud Prevention in the Digital Age: Emerging Risks and Best Practices to Mitigate the Risks

In the digital age, technology has brought unprecedented convenience and accessibility. However, with every advancement comes new challenges. One of the most significant challenges in today's digital landscape is fraud prevention. As online transactions and digital interactions become increasingly prevalent, the risks associated with fraud have also evolved. This article we will explore the emerging risks faced in fraud prevention and discuss the best practices that can help mitigate these challenges.

With the rapid advancement of technology, the digital age has brought numerous benefits and conveniences to our lives. However, it has also given rise to new challenges, particularly in fraud prevention. As our personal and financial information becomes increasingly interconnected online, it is crucial to understand the emerging risks and adopt best practices to safeguard ourselves and our businesses from fraudulent activities.

Emerging Risks in the Digital Age:

1. **Phishing and Social Engineering**: Phishing attacks have become more sophisticated, with cybercriminals employing deceptive tactics to trick individuals into divulging sensitive information or performing unauthorized actions. These attacks often involve emails, messages, or phone calls that appear to be from reputable sources, luring victims into sharing login credentials, and financial details, or clicking on malicious links.

2. **Identity Theft:** The digital age has created new opportunities for identity thieves. Cybercriminals can obtain personal information through data breaches, social media platforms, or by exploiting weak security practices. Stolen identities can be used for various fraudulent activities, including applying for loans, opening unauthorized accounts, or committing financial fraud.

3. **Mobile Payment Fraud**: The widespread adoption of mobile payment apps has opened avenues for fraudsters to exploit vulnerabilities in these platforms. Mobile payment fraud can occur through unauthorized transactions, fake apps, or malware that targets users' devices. Fraudsters can also intercept wireless signals or use malicious software to collect sensitive payment information. Mobile and Online Banking Threats: The widespread adoption of mobile banking applications and online payment systems has opened up new avenues for fraudsters. Malware, fake mobile apps, and fraudulent websites can compromise users' financial information, leading to unauthorized transactions and account takeovers.

4. **Synthetic Identity Fraud:** Synthetic identity fraud involves the creation of fictional identities using a combination of real and fake information. Cybercriminals use these synthetic identities to open fraudulent accounts, apply for loans, or make purchases. This type of fraud is particularly challenging to detect because the identity may not exist in official records.

5. **Ransomware and Data Breaches**: Ransomware attacks have become increasingly prevalent, with cybercriminals encrypting victims' data and demanding a ransom for its release. Data breaches, on the other hand, expose sensitive information to unauthorized parties, leading to potential financial loss and identity theft. Both ransomware attacks and data breaches pose significant risks to individuals and businesses alike.

6. **Sophisticated Cybercriminals:** The digital age has created a new breed of cybercriminals who employ advanced techniques to deceive individuals and organizations. Phishing attacks, identity theft, and social engineering scams have become more sophisticated, making it difficult for traditional security measures to keep up.

7. **Data Breaches**: With the exponential growth of data collection and storage, the risk of data breaches has increased. Cybercriminals target organizations and steal sensitive customer information, such as credit card details, personal identities, and passwords, which they later use to carry out fraudulent activities.

8. **Insider Threats**: While external threats are widely recognized, insider threats pose a significant risk to organizations. Disgruntled employees or those with unauthorized access can abuse their privileges to commit fraud. Detecting and preventing insider fraud can be challenging as these individuals often have legitimate access to systems and data.

shutterstock.com · 381869767

<u>Best Practices for Fraud Prevention:</u>

1. **Educate Yourself and Your Employees**: Stay informed about the latest fraud trends and educate yourself, your employees, and your family about potential risks. Promote a culture of cybersecurity awareness, emphasizing the importance of strong passwords, recognizing phishing attempts, and exercising caution while sharing personal information online.

2. **Implement Strong Security Measures:** Ensure your devices, including computers, smartphones,

and tablets, have up-to-date antivirus software, firewalls, and operating systems. Regularly update software and firmware to patch any security vulnerabilities. Enable multi-factor authentication wherever possible to add an extra layer of protection.

3. **Secure Network Connections:** Use secure and encrypted connections, especially when accessing sensitive information or making financial transactions online. Avoid using public Wi-Fi networks for such activities, as they are more susceptible to interception by hackers. Instead, rely on trusted and secure networks or consider

using a virtual private network (VPN) to encrypt your internet traffic.

4. **Be Cautious with Personal Information:** Limit personal information you share online and on social media platforms. Be cautious when providing sensitive information to websites or services, ensuring they are reputable and secure. Regularly review your privacy settings on social media platforms to control who can access your personal information.

5. **Monitor Financial and Personal Information:** Regularly review your bank and credit card statements for any suspicious activity. Consider signing up for transaction alerts or credit monitoring services that can notify you of any unauthorized activity. Monitor your credit reports for any unfamiliar accounts or inquiries, that could indicate potential identity theft.

6. **Establish Strong Password Hygiene:** Use unique and complex passwords for each online account.

7. **Multi-Factor Authentication (MFA):** Implementing MFA across various digital platforms adds an extra layer of security. The risk of unauthorized access is significantly reduced by requiring users to provide multiple forms of identification, such as passwords, biometrics, or SMS verification codes.

8. **Real-Time Monitoring and Analytics**: Advanced fraud detection systems employing machine learning algorithms can help identify suspicious patterns and behaviours in real-time. These systems can quickly analyze vast amounts of data and provide timely alerts to prevent fraudulent transactions.

9. **Customer Education and Awareness**: Educating customers about the latest fraud trends, common scams, and best practices is crucial in combating fraud. Regularly communicating with customers through email alerts, security notifications, and user awareness campaigns can help them stay vigilant and protect their personal information.

10. **Robust Data Security Measures**: Organizations must prioritize data security by implementing robust encryption protocols, firewalls, and intrusion detection systems. Regular security audits, vulnerability assessments, and timely software updates are essential to protect against data breaches.

11. **Collaboration and Information Sharing**: Building collaborative networks among organizations, industry associations, and law enforcement agencies can enhance fraud prevention efforts. Sharing information on emerging threats and fraud indicators can help identify trends and develop proactive strategies to combat fraud effectively.

12. **Continuous Training and Skill Development:** Investing in regular training and skill development programs for employees involved in fraud prevention is vital. Equipping them with up-to-date knowledge and expertise in emerging technologies and fraud detection techniques can improve their ability to identify and prevent fraudulent activities.

Conclusion

As the digital age continues to evolve, the challenges of fraud prevention also evolve alongside the changes in the digital ecosystem. Sophisticated cybercriminals, data breaches, mobile and online banking threats, and insider fraud pose significant risks to individuals and organizations. However, by adopting best practices such as the measures mentioned above, the fight against fraud can be strengthened. Individuals, businesses, and regulatory authorities must remain vigilant, adapt to emerging risks, and implement effective fraud prevention strategies to protect the digital ecosystem.

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

Compliance Regulatory Updates for CAEs

CBN Code of Corporate Governance

Excerpts from the EY training presentation to the Association of Chief Audit Executives of Banks in Nigeria (ACAEBIN) on the Imperatives for CAEs in the Digital Age held in Kigali, Rwanda between September 04-06,2023.

The Central Bank of Nigeria (CBN) on 13 July 2023, issued a circular on Corporate Governance Guidelines for all Commercial, Merchant, Non-Interest, Payment Service Banks, and Financial Holding Companies in Nigeria effective 1 August 2023.

The recent introduction of the new CBN Corporate Governance Guideline represents a pivotal milestone in enhancing transparency, accountability, and Risk Management within the Banking industry.

We have highlighted the changes in the new CBN Code when benchmarked against the extant code (Code of Corporate Governance for Banks and Discount Houses in Nigeria and Guidelines for Whistle Blowing in the Nigerian Banking Industry – 2014) and highlighted the next steps for you.

Some Key Changes – Governance

New Guideline	Section	Key Changes Include but not limited to:	Some of the potential impact include:
Board Structure and Composition	1.1	◆ The procedure for the appointment to the Board shall be formal, transparent, and documented in the Board Charter. The 2014 version did not specify that it should be in the Board Charter.	◆ The Board should ensure that the procedure of appointing new directors is documented in the Board Charter.
	1.3	◆ The introduction of a new minimum and maximum number of directors on the Board. Minimum in 2014 version is 5 but the new minimum is 7, while maximum in the 2014 version is 20 but the new Code restricts this to 15. This applies for the Boards of Commercial, Merchant, and Non-Interest Banks. ◆ The new code also defines PSBs as minimum of 7 and maximum of 13.	◆ The Board should be conscious of this in managing its size.

Some Key Changes – Governance

New Guideline	Section	Key Changes Include but not limited to:	Some of the potential impact include:
Board Structure and Composition	1.5	◆ The number of INEDs shall be at least 3 for Commercial Banks with international and national authorization, Merchant Banks and Non-Interest Banks (NIBs) with national authorization while 2 for Payment Service Banks (PSBs), Commercial Banks and NIBs with regional authorization	◆ The Board should review the Board composition with respect to the number of INEDs on the Board, in line with the new regulatory guidelines.„
	1.6	◆ In case of public listed banks, the provisions of CAMA 2020 on the number of INEDs shall apply.	◆ The number of INEDs for public listed banks shall be 3 in line with CAMA 2020
	1.7	◆ The introduction of the provision that at least 2 NEDS, one of whom shall be an INED, shall have requisite knowledge and experience in innovative technology, information communication technology, and/or cyber security.	◆ The Board should review its skill set with a view to having at least a NED and INED who is skilled in innovative technology, ICT and cyber security.
	1.8	◆ The inclusion of the provision that no Board shall consist of one gender.	◆ The Board should review its composition to ensure that there is no one gender on the Board and consider a minimum of 40% representation in accordance with Principle 4 of the Nigerian Sustainable Banking Principles.
	1.12	◆ The introduction of the definition of extended family. The provision stated that no more than two members of an extended family shall be on the Board of a Bank. ◆ The CBN defined the extended family of a Director as Directors' spouse, parents, children, siblings, cousins, uncles, aunts, nephews, nieces, in-laws and any other construed relationship as may be determined by the CBN.	◆ The Board should review its composition with a view to ensuring that no more than two (2) members of an extended family sits on the Board.
	1.15	◆ The introduction of the provision that in the case of a Bank that is a subsidiary of a Financial Holding Company (FHC), the aggregate number of directors from the subsidiaries shall not exceed thirty percent of the members of the Board of the Financial Holding Company and the number of directors on the Board of the Financial. Holding Company in the Board of the subsidiary shall not exceed thirty percent.	◆ The Bank should review its composition to ensure that it does not exceed the threshold of 30% for the number of directors in the FHC or the subsidiary.
	1.18 1.19 1.21 1.22	◆ Introduction of procedures around Director resignation: ◆ Resignation of a Director from the board of a	◆ The Board should review its Board Charters, Terms of Reference, Letter of Employment and/or Contract

Some Key Changes – Governance

New Guideline	Section	Key Changes Include but not limited to:	Some of the potential impact include:
Board Structure and Composition		bank shall require a 90 days notice and where a resignation of an INED results in a breach of the minimum number, a replacement should be made within 90 days and if the resignation of the Board results in a breach of NEDs not more than EDs, replacement should be done within 90 days. ◆ Resignation of the Chairman of the Board shall require the Chairman to forward the notice stated above to the Chairman, Board Nomination and Governance Committee who shall circulate to members of the Board and the CBN within seven days of receipt of the notice of resignation.	of Employment of Directors with a view to including these new provisions.
	1.24	◆ Where a merger, acquisition, take over or any form of business combination involves the appointment of a Director from the Board of the legacy institution, the length of service of such director shall include both the periods served pre- and post- combination.	◆ Tenure of directors should be reviewed to ensure adherence with the code after a business combination
Roles and Responsibilities of the Board	2.3	◆ The new Code requires Board and Committee Charters to be reviewed at least once every three years and upon any such review, the Board approved copies shall be submitted to the CBN for its No Objection within thirty (30) days of approval by the Board and prior to its implementation	◆ The Bank should review and ensure that Board and Committee Charters are reviewed at least once every three years and copies submitted to the CBN within 30-days of approval.
	2.4	◆ The Board shall define and approve the bank's strategic goals, its short, medium and long-term strategies and monitor implementation by management.	◆ The Bank should review that the current strategy of the Bank meets all the requirements.
	2.5	◆ The Board shall ensure review of the investment policies and strategies of the Bank at least once every three years, and submit same to the Director Banking Supervision Department, CBN.	◆ The Board should review and ensure its investment policies and strategies are reviewed once every three years and submitted to the CBN.
	2.8	◆ The bank shall ensure there is a Business Continuity Plan (BCP)	◆ The Bank should ensure there is a functional BCP in place.
	2.9	◆ The bank shall implement an Information Technology (IT) Framework that at a minimum covers data confidentiality, network security, third party connections, incidence response and reporting	◆ The Bank should review and ensure compliance to the implementation of an Information Technology Framework.
	2.14	◆ The Board shall approve a succession plan for the MD/CEO, other EDs and senior management staff, which shall be reviewed once every two years.	◆ The Board should review its succession plan and ensure that same is reviewed every review two years.

Some Key Changes – Governance

New Guideline	Section	Key Changes Include but not limited to:	Some of the potential impact include:
Officers of the Board	3.1.2	◆ The Chairman shall meet formally with NEDs at least once every year.	◆ The Bank should ensure the Chairman meets the NEDs at least once every year.
	3.1.3	◆ Where a Bank is a member of a Financial Holding Company, the Chairman of the Bank shall not sit on the Board of the FHC in any capacity and vice versa.	◆ The Board should review its composition and ensure that they are in compliant with this provision.
	3.2	◆ The tenure of the MD/CEO of a Bank shall be in accordance with the terms of engagement with the Bank but subject to a maximum period of twelve (12) years. The 2014 version of the CBN CG Code was a maximum of ten (10) years.	◆ The Board show review its Charter and/or Contract of Employment of the MD/CEO and where necessary can extend to 12 years.
	3.3.2	◆ Where an ED becomes a DMD, a cumulative tenure of twelve (12) years applies and shall not be extended.	◆ The Board should review the tenure of its Directors and ensure that the stipulated regulatory tenure is not exceeded.
	3.3.3	◆ Where a DMD/ED becomes an MD/CEO of the same Bank, his/her previous tenure as DMD/ED is not included in computing his/her tenure as MD/CEO. However, this is subject to cumulative tenure limit as stated in Section 8 of this Guidelines (cumulative maximum of 24 years).	◆ The Board should review its Board Charter and/or corporate governance framework to reflect this new provision.
	3.4.1	◆ NEDs shall have unfettered access to corporate information from the MD/CEO, DMD, EDs, Company Secretary, Internal Auditor and Heads of other control functions with direct/indirect reporting lines to the Board, while access to other senior management shall be through the MD/CEO.	◆ The governance documents of the banks should be updated and the Directors and respective heads of control functions should be aware.
	3.4.3	◆ To qualify as a NED in a bank, the proposed NED shall not be an employee of a financial institution except where the bank is promoted by that financial institution and the proposed NED is representing the interest of that financial institution.	◆ The Board governance documents should be appropriately updated and Board Nomination and Governance Committee aware of this.
	3.5.2	◆ The tenure for INEDs shall not exceed two terms of four years each.	◆ The Board should review its Board Charters, letter of employment to ensure that same is in accordance with this provision.
	3.5.3	◆ An INED shall not be a former director, employee, have an immediate family member in a senior management position, borrowed funds from the Bank etc.	◆ The Board should review its INED composition to ensure that same is in compliance with this provision.

Some Key Changes – Governance

New Guideline	Section	Key Changes Include but not limited to:	Some of the potential impact include:
Officers of the Board	3.5.5	◆ The Board shall annually ascertain and confirm the continued independence of each INED	◆ The Board should update its governance documents and also ensure the annual implementation of the provision.
	3.5.7	◆ All INEDs shall hold a formal meeting at least once in a year without the other directors being present.	◆ The Board should update its governance documents and also ensure the annual implementation of the provision.
	3.6 3.6.3	◆ The functions of a company secretary shall not be outsourced by Banks. The role of the Company Secretary in a CMNIB, shall not be combined with that of the Head Legal/Legal Adviser, without the approval of the CBN.	◆ The Board should ensure that an in-house Company Secretary is maintained always and the role not combined with Head Legal/ Legal Adviser for CMNIB.
Board Committees	6.2	◆ The membership of Board Committees shall be reviewed and refreshed at least once every three years.	◆ The composition of Board Committees should be reviewed and provision implemented.
	6.3	◆ All Board Committees shall be chaired by NEDs. However, the Board Audit Committee (BAC), Board Nomination and Governance Committee (BNGC) and the Board Remuneration Committee (BRC) shall be chaired by INEDs.	◆ The Board should review its composition with a view to ensuring that BAC, BNGC and BRC are chaired by INEDs. ◆ Also, all other committees should be chaired by NEDs.
	6.5	◆ In addition to the mandatory Committees listed in Recommended Practice 11.1.6 of NCCG 2018, the Board of any CMNIB shall also establish a Board Credit Committee (BCC) with oversight responsibility on credit matters.	◆ The Board should review its Committee Structure and have a dedicated BCC for oversight of credit matters.
	6.10	◆ The functions of the Board Risk Management Committee (BRMC) and the Board Audit Committee (BAC) shall not be combined for CMNIBs.	◆ The Board should review its Committee Structure and ensure the separation of BRMC and BAC.
	6.13c	◆ At least one member of the Board Audit Committee of a Commercial, Merchant or Non-Interest Bank shall be knowledgeable in innovative technology, ICT, and/or Cybersecurity. In the case of a PSB, the majority of the BAC shall be knowledgeable in innovative technology, ICT, and/or cybersecurity.	◆ The Board shall review the composition of the Board Audit Committee to meet the regulatory requirements with respect to the skills mentioned.
	6.14	◆ In the case of a commercial Bank with an NIB window, at least one NED in the BRMC shall have relevant qualification and experience in Islamic Finance or Islamic Commercial Jurisprudence.	◆ The Board of a Bank with NIB window, going forward, shall appoint a NED with knowledge of Islamic Finance.

Some Key Changes – Governance

New Guideline	Section	Key Changes Include but not limited to:	Some of the potential impact include:
	6.15	◆ The Head of the NIB window of a Commercial Bank shall be a senior management staff with knowledge and experience in the field of Islamic Finance or Islamic Commercial Jurisprudence	◆ The Board shall consider the relevance of Islamic Finance knowledge in appointing a Head of the NIB window.
Cool-Off Period	7.1	◆ An Executive (ED, DMD or MD/CEO) who exits from the Board of a Bank either upon or prior to the expiration of his/her maximum tenure, shall serve out a cooling period of two (2) years before being eligible for appointment as a NED in the same Bank, subject to applicable cumulative tenure limits.	◆ The Board should review its Charter and composition and make the necessary amendments, where applicable.
	7.2	◆ Where an Executive (ED, DMD or MD/CEO) of a Bank is appointed to the Board of its FHC in any role, a cooling-off period of two years shall apply.	◆ The Board should review its Charter and composition and make the necessary amendments, where applicable
	7.4	◆ A NED shall serve out a cooling period of two (2) years before being eligible for appointment in any executive role in the same Bank	◆ The Board should review its Charter and composition and make the necessary amendments, where applicable.
	7.5	◆ No cooling-off period shall apply when any Director in a Bank is appointed to the Board of another Bank or an FHC outside the Bank's group.	◆ The composition of Board committees will be subjected to review.
	7.6	◆ Cooling-off period of two (2) years shall apply, where a Director from a Bank transition to a sister subsidiary and it results in a change of role. However, cooling-off period shall not apply where there is no change of role	◆ The Board should review its Charter and composition and make the necessary amendments, where applicable.
	7.9	◆ Subject to the approval of the CBN, there shall be a cooling-off period of three (3) years between the retirement of a partner from an audit firm currently auditing a bank and the appointment of such partner to the Board of the same bank.	◆ The Board should review its Charter and composition and make the necessary amendments, where applicable.
Continuing Education	9.1	◆ A formal induction programme for new directors shall be conducted within three months of their appointment. The details of such training shall be availed to examiners upon request.	◆ The Board should ensure the update of its governance documents and also ensure new directors are inducted within 3 months of their appointment.
Training	9.2	◆ The Board shall approve an annual budget for the training and continuing education for directors and ensure its proper implementation.	◆ The Board should ensure the update of its governance documents and also ensure ongoing training.

Some Key Changes – Governance

New Guideline	Section	Key Changes Include but not limited to:	Some of the potential impact include:
Board Evaluation	10.5	◆ Banks shall forward to the Director, Financial Policy and Regulation Department (FPRD), CBN, the report of the annual evaluation of the Board and ACE by the independent external consultant latest by May 31st following the end of every financial year or before the Annual General Meeting at which the report for the period/year is to be considered, whichever comes first.	◆ Board/ACE evaluation shall be forwarded to the CBN by May 31 or before the AGM at which the report for the period is to be considered, whichever comes first.
	10.6	◆ The continuous unsatisfactory performance by a director shall be a basis for non-renewal of such a director's tenure.	◆ The Board should update its governance documents and also comply with the provision.
Remuneration	11.10	◆ The Board shall at the end of each financial year, confirm that the implementation and execution of the remuneration policy achieved its objectives.	◆ Board shall review the remuneration policy annually to ensure it meets the company's objectives.
Internal Audit Function	13.1	◆ A Bank shall not outsource its Internal Audit/Compliance functions.	◆ Banks are not to outsource the IA function
	13.4	◆ The Head of Internal Audit, who shall not be below the rank of an Assistant General Manager, shall report directly to the BAC.	◆ All Banks shall ensure that the rank of the Head Of Internal Audit is in line with the code.
	13.5	◆ An independent external assessment of the effectiveness of the Internal Audit function as provided in Recommended Practice 18.6 of NCCG 2018 shall be carried out annually and the report submitted to the Director, Banking Supervision Department, latest May 31st following the end of every accounting year.	◆ Reporting lines shall be reassessed to ensure a direct report structure from the Head of internal Audit to the BAC.
	14.1	◆ NIBs shall have an Internal Shariah Audit function headed by an Internal Shariah Auditor (ISA) not below the rank of an Assistant General Manager. In the case of commercial Banks with NIB window, the head of the internal shariah audit function shall not be below the rank of a Manager.	◆ Banks shall ensure the external assessment of the Internal Audit Function is done annually and submitted to the CBN before 31 May of each year.
	14.3	◆ The ISA in consultation with the ACE, shall determine the scope of the shariah audit and is required to produce internal shariah compliant reports which shall be submitted quarterly to the ACE and the BAC.	◆ Banks shall ensure that The Head Of The Internal Shariah Audit function is of the appropriate rank
	14.5	◆ Appointment and removal of the ISA shall be the responsibility of the Board in consultation with the ACE, subject to CBN's ratification.	◆ The ISA shall ensure the quarterly submission of the compliant reports to the appropriate bodies.

How 8 simple lifestyle measures add years to your life.

Adults who monitor eight simple health measurements may live longer lives, according to studies. Following the American Heart Association's Life's Essential 8 can shave up to six years off your biological age, according to researchers.

The checklist includes measures such as eating properly, exercising frequently, not smoking, and getting enough sleep.

The other four criteria are about staying skinny, keeping cholesterol low, and maintaining optimal blood pressure and blood sugar levels.

According to experts, the eight steps support optimal heart health, which may reduce the rate of biological aging.

The checklist includes eating well, exercising regularly, quitting smoking, getting adequate sleep, and maintaining a healthy weight. The eight steps may help reduce biological aging.

A study by Columbia University's Professor Nour Makarem found that higher cardiovascular health is associated with decelerated biological ageing, as measured by phenotypic age. The study also found a dose-dependent association, with as heart health increases, biological ageing decreases.

The research suggests that adherence to Life's Essential 8 metrics and improving cardiovascular health can slow down the body's ageing process and have numerous benefits in the long run. Reduced biologic ageing is associated with lower risk of chronic diseases, longer life, and lower risk of death.

Dr. Donald Lloyd-Jones, chair of the writing group for Life's Essential 8 and former volunteer president of the American Heart Association, said that these findings help understand the link between chronological age and biological age and how following healthy lifestyle habits can help us live longer. The preliminary study will be presented at the American Heart Association's Scientific Sessions 2023 in Philadelphia.

A separate study published in Sweden found that people with a higher biological age than their actual chronological age have an increased risk of stroke and dementia. The study also found that the risk of developing ALS, also known as motor neurone disease (MND), increases with higher biological age.

Life's Essential eight factors

- Eat better: Include whole foods, lots of fruits and vegetables, lean protein, nuts, seeds, and cooking in non-tropical oils such as olive and canola
- Be more active: Adults should get 2 ½ hours of moderate or 75 minutes of vigorous physical activity per week
- Quit tobacco: Use of inhaled nicotine delivery products, which includes traditional cigarettes, e-cigarettes and vaping, is now a leading cause of preventable death
- Get healthy sleep: Most adults need 7-9 hours of sleep each night. Adequate sleep promotes healing, improves brain function and reduces the risk for chronic disease.
- Manage weight: Achieving and maintaining a healthy weight has many benefits.
- Control cholesterol: High levels of non-HDL, or 'bad,' cholesterol can lead to heart disease
- Manage blood sugar: Over time, high levels of blood sugar can damage your heart, kidneys, eyes and nerves
- Manage blood pressure: Keeping your blood pressure within acceptable ranges can keep you healthier longer

allure.vanguardngr.com

Training on Report Writing and Effective Communication Skill for Internal Auditors held on October 18th and 19th, 2023 in conjunction with Platinum Edge Consulting



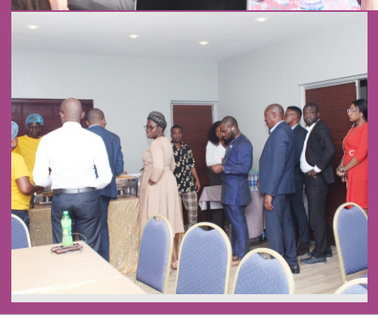













Training on Report Writing and Effective Communication Skill for Internal Auditors held on October 18th and 19th, 2023 in conjunction with Platinum Edge Consulting













Happy Birthday Distinguished CAEs

CORONATION MERCHANT BANK

Oct. 05

Adeola Awe

BOA BANK of AGRICULTURE

Oct. 13

Daniel Olatomide

parallex

Oct. 14

Seyi Ogundipe

Fidelity

Oct. 26

Ugochi Osinigwe

SunTrust Bank

Nov. 03

Youseuph Edu

Sterling

Dec. 06

Edward Onwubuya

PROVIDUSBANK

Dec. 10

Aina Amah

NEXIM

NIGERIAN EXPORT-IMPORT BANK

Dec. 25

Ayaghena Ozemede

PremiumTrust Bank

Dec. 31

Dumebi Okwor

Internal Control Over Financial Reporting (ICFR)

Internal Control Over Financial Reporting (ICFR) appears to be an emerging concept to many assurance providers in Nigeria at the moment, but this should not be so, because, the concept has been introduced in Nigeria since year 2007 through the Investment and Securities Act (ISA) 2007 sections 60 to 63. This happened just five years after its first introduction in the United State of America in 2002 through the SOX Act Section 404 (SOX 404). Therefore, counting from year 2007 to the year 2023 of this writing, ICFR has been in Nigeria for seventeen (17) years.

The purpose of this writing is to look at the various regulatory requirements driving ICFR implementation in Nigeria and the key elements the assurance providers can consider in supporting their organization comply with the ICFR requirements.

What is Internal Control Over Financial Reporting?

Understanding Internal Control Over Financial Reporting requires a broad understanding of the following:

- Internal Control System,
- corporate goals and objectives - why businesses are established,
- business operating models and
- factors that can mar or enhance a company's abilities to achieving the goals and objectives.

Internal Control has been broadly defined differently by many sources. The Wikipedia defines Internal Control as "everything that controls risks to an organization". (myaccountingcourse.com) defines Internal Control as "a procedure or policy put in place by management to safeguard assets, promote accountability, increase efficiency, and stop fraudulent behavior". (investopedia.com) defines internal control as "accounting and auditing processes used in a company's finance department that ensure the integrity of financial reporting and regulatory compliance, and prevent fraud, improve operational efficiency, ensure that budgets are adhered to, policies are followed, capital shortages are identified, and accurate reports are generated for leadership".

COSO defines Internal Control as "a process, effected by an entity's board of directors, management and other personnel designed to provide reasonable assurance to the stakeholders of the achievement of the organizational goals and objectives. They help to safeguard stakeholders' investments and corporate assets, and achieve operational efficiencies through improved business performance, increased productivity, cost savings, credible financial and non-financial reporting and compliance to laws and regulations.

For me, an Internal Control system is defined as "a system comprising of policies, procedures, and practices adopted by the business management and approved by the company board to ensure that the negative risks that will impact the day to day business operations and mar the achievement of the corporate goals and objectives are prevented, timely detected and root causes properly addressed while ensuring that the positive risks and success opportunities are maximized for the best interest of the organization".

What are Some of the primary reasons why businesses are established?

Businesses are established to achieve specific goals and objectives. There are numerous goals and objectives a business can achieve, but the Committee of Sponsoring Organizations of the Treadway Commission (COSO) has classified the business goals and Objectives into four, namely: Strategic goals and objectives, Operational goals and objectives, Reporting goals and objectives, and Compliance goals and objectives. COSO also, classified the risk events that can prevent or enhance the achievement of the business goals and objectives as Strategic risks, Operational risks, Reporting risks and Compliance risks. Negative risks mar the achievement of the corporate goals and objectives while positive risks enhance the opportunities for the achievement of the corporate goals and objectives.

A brief description of the COSO perspectives of the corporate goals and objectives and the factors that can impact their achievement have been presented in figure 1 below.

Figure 1 - A brief Description of the COSO Perspectives of Corporate Goals and Objectives and the factors that can impact the achievement.

COSO Categorizations Corporate Purposes.	Factors impacting corporate goals and objective achievements.
Strategic Goals and Objectives are the measurable. actionable- and specific items that an organization may want to achieve in the long-term, usually within the periods of the three to twenty-five years' timeline or more. Examples of strategic gaols and objectives may focus on revenue target, profitability, cost saving, product and service and asset size.	**Strategic Risks** ❁ Wrong business strategic decision leading to failed strategy. ❁ Reactive response to critical & emerging changes and delayed or missed great opportunities. ❁ Competition, new business, and capital availability risk.
Reporting Goals and Objective Are the promises to produce and communicate financial and non-financial statements to stakeholders within and outside the organization.	**Reporting Risk / Misstatements** ❁ Material errors, ❁ Material mistakes, negligence, and fraud.
Legal and Regulatory Compliance Goals and Objectives are commitments to abide by the applicable regulations and the internal corporate policies, processes without compromise to ethical values and good business conducts.	**Legal and Regulatory Compliance Risk** ❁ Taxation risks ❁ Corporate Governance Codes – National & Sectoral, ❁ ABC, AML/CFT, Human Rights risk and Accounting Standards.
Operational Goals and Objectives Are goals and objectives an organization may want to achieve in the short-term often within the periods of one to two years and driven by the strategic goals and objectives. Operational goals and objectives are encapsulated in tactical planning which occur in the daily plan, weekly plan, quarterly and in the annual budget.	**Operational Risks** ❁ People, third party risks, credit risks, Liquidity and Underwriting risks ❁ Product Quality, HSEQ and Technology risks. ❁ Litigation or reputational and brand image risk ❁ Market Risk – interest rate, forex, or commodity pricing.

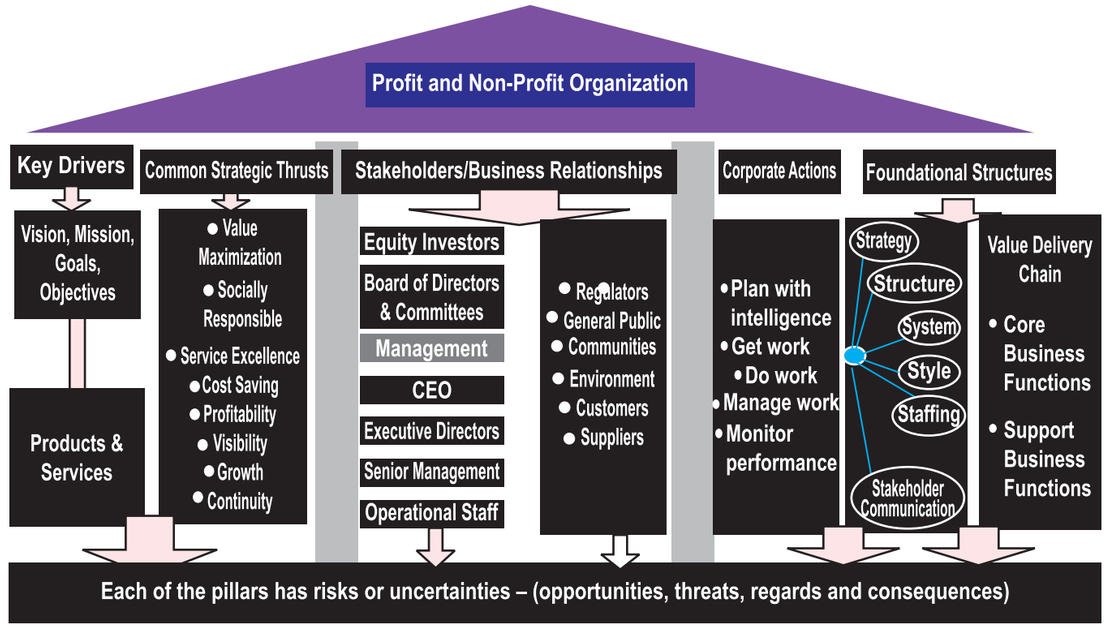
It is important to note that there are other different risk management standards that have their own unique risk categorization that may be different from that of COSO framework perspectives. Examples: The BASEL Framework classified the risks for banks to be Market Risks, Credit Risks, Capital Risks and Operational Risks. The Solvency Framework for the insurance business has classified the insurance risk to include Market Risks, Credit Risks, Liquidity Risks, Operational Risks and Underwriting risks.

What are the critical building blocks required of the organizations to achieve corporate goals and objectives?

The Business Operating Model shown in figure 2 below depicts the critical building blocks that every organization should be intentional and prioritize to reinforce the organization's ability to sustain the achievement of the corporate goals and objectives. These building blocks are anchored on commitment to business excellence demonstrated by understanding what the company stands for and doing the proper things to

making the company stand tall and test of time.

Figure 2
An overview of a Business Operation Model Highlighting the Critical Building Blocks for Achieving Corporate Goals and Objectives



Stakeholders and Stakeholders' Communication are part of the critical business building blocks required by the organizations to pay serious attention in the achievement of their corporate goals and objectives. The Financial Reports which include the Financial Statements are the critical tools for communicating financial performance of the organizations to the stakeholders who need the information for insight to make risk-informed decisions, develop business plan and execute actions. For the stakeholders to rely on the financial reports to make right decisions and take proper actions, the credibility of the financial reports must be assured across all levels. The three lines of defense assurance providers which include management reviews, internal control, internal audit, enterprise risk management, HSEQ provide the assurance.

Who Is Responsible for the Certification of The Financial Statements Credibility?

Generally, everyone in the organization that has input to the production of the financial and non-financial reports emanating from any organization right from the transactions origination, approvals, processing and reporting has the responsibility for the certification of the credibility of the reports. In most jurisdictions across the globe, companies are required to make available a copy of their audited annual financial statements prepared by qualified independent accountants to the members of the organizations and the same should be filed with the regulators. The credibility of the audited financial statements should be certified by the company and attested by the statutory auditor before he filing and communication to the members of the company.

In Nigeria, this is a mandatory compliance requirement as stipulated by the Companies and Allied Matters Act (CAMA) 2020 (cac.gov.ng), Investment and Securities Act (ISA) 2007 (The Securities and Exchange Commission, Nigeria), and the Financial Reporting Council Act (FRC Act) 2011 (FRC-Rules-Updated-Original-Rule-4-Inclusive.pdf (frcnigeria.gov.ng). CAMA 2020 section 386 requires that the audited financial statements (balance sheet and the profit and loss account annexed to it) shall be approved by the board of directors and signed on their behalf by two directors authorized to do so. The Investment and Securities Act section 60 requires that the Chief Executive Officer and Chief Financial Officer or officers or persons performing similar functions in a public company filing periodic or annual reports shall certify as follows on the reports filed:

Figure 3 – The Investment and Securities Act (ISA) 2007, Section 60 to 65 stating the requirement for Certification of the credibility of the audited Financial Statements

Section 60:

(1)A public company whose securities are required to be registered under this Act shall file with the Commission on a periodic basis, its audited financial statements and such other returns as may be prescribed by the Commission from time to time.

(2)The Chief Executive Officer and the Chief Financial Officer or Officers or persons performing similar functions in a public company filing periodic or annual reports under subsection (1) of this section, shall certify in each annual or periodic report filed, that

(a) The signing Officer has reviewed the report;

(b)Based on the knowledge of the officer, the report does not contain
(I)Any untrue statement of a material fact, or
(ii)Omit to state a material fact, which would make the statement, misleading in the light of the circumstances under which such statement was made:

(c)Based on the knowledge of such officer, the Financial Statement and other financial information included in the report fairly present in all material respects the financial condition and results of operations of the company as of and for the periods presented in the report.

(d)The signing officers
(i)Are responsible for establishing and maintaining internal controls.
(ii)Have designed such internal controls to ensure that material information relating to the company and its consolidated subsidiaries is made known to such officers by others within those entities particularly during the period in which the periodic reports are being prepared.
(iii)Have evaluated the effectiveness of the company's internal controls as of date within 90 days prior to the report.
(iv)Have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date.

(e)The signing officers have disclosed to the Auditors of the company and Audit Committee
(i)All significant deficiencies in the design or operation of the Internal Controls which would adversely affect the company's ability to record, process, summarise and report financial data and have identified for the company's Auditors any material weakness in the Internal controls and
(ii)Any fraud, whether or not material, that involves management or other employees who have significant role in the company's internal controls.

(f)The signing officers have identified in the report whether or not there were significant changes in internal controls or other factors that could significantly affect internal controls subsequent to the date of their evaluation, including any corrective actions with regard to significant deficiencies and material weaknesses.

Section 61:

(1) A public company shall establish a system of internal controls over its financial reporting and security of its assets, and it shall be the responsibility of the Board of Directors to ensure the integrity of the company's financial controls and reporting.

(2) The Board of Directors of a public company shall report on the effectiveness of the Company's internal control system in its annual report.

Section 63:

An Auditor of a public company shall, in his audit report to the company, issue a statement as to the existence, adequacy and effectiveness or otherwise of the internal control system of the public company.

Section 65:

(1) A public company who contravenes the provisions of Sections 60, 61, 62, 63 and 64 is liable to a penalty of not less than N1,000,000 and a further penalty of N25,000 per day for the period of violation continues.
(2) An Auditor who contravenes the provisions of sections 60, 61, 62, 63 and 64 is liable to a penalty of N100,000 and a further penalty of N5,000 per day for the period the violation continues.

Similar to the above ISA 2007 requirements, CAMA 2020 requires that the Chief Executive Officer and Chief Finance Officer of all companies with shares registered with the Corporate Affairs Commission (CAC) to make the same certifications on the audited annual financial statements for filing with the Commission and reporting in the company's annual general meeting. The small companies registered with CAC are exempted from this CAMA 2020 requirements. CAMA 2020 states that where a managing director, chief financial officer or person performing similar functions fails to discharge the duty imposed on him under the section, he commits an offence and is liable on conviction to a penalty as the Commission shall specify in its regulations. In addition, the Financial Reporting Council Act (FRC Act) 2011 section 7(2g) requires the Chief Executive Officer and Chief Finance Office of the Public Interest Entities (PIE) to make the same certifications on their audited financial statements for filing with the Council. ISA 2007 states that the relevant entities who fail to comply with the relevant sections shall be liable to civil, administrative and criminal sanctions within the latitude of the Financial Reporting Council of Nigeria Act 2011.

Achieving the above certification requirements could be herculean tasks for the certification the regulated companies. The implication is that the approving officers, signing officers and certification officers of the audited financial statements should trust the competencies and capabilities within their business functions and three lines of defense assurance providers. The trust will strengthen their confidence to believe that the financial accounting treatments, record keeping practices and reporting processes fully conform the applicable

accounting standards which in this case is IFRS In Nigeria. and the Financial Statements Assertions principles of Existence, Completeness, Accuracy, Classification, Rights, Obligations, Valuation and Allocation.

Given that the compliance requirements for internal control over financial reporting is focused on the financial controls around the financial transactions processing and reporting processes, it is very important to note that adopting a big picture approach in the ICFR implementation by embedding a robust Agile Risk Based Enterprise Risk Management (ERM) Framework For assessing risk exposures, developing risk responses and adopting strong Combined Assurance Strategy for testing control activities enterprise wide provide a great advantage to the organizations in making the certification requirements on the credibility of their financial statements.

How Do We Implement Internal Control Over Financial Reporting?

The key questions to the Internal Auditor and other assurance providers within the three lines of defense:

(1) Is your organization a public listed company in the Nigerian Stock Exchange (now NGX Group) or a Public Interest Entity or considered as a big company with shares and registered with CAC?

(2) How well is your organization complying with the provisions on internal control over financial reporting?

(3) Does your organization have the capacity and capabilities to undertake the ICFR implementation using its own internal/in-house resources?

(4) Achieving successful ICFR implementation requires having a string entity level controls which nclude a positive tone at the top and also strong control activities around the key financial accounts and supporting processes:(a) Do you know the criteria for assessing the entity level controls.
(b) How about the basis for selecting the key financial accounts and testing the associated control activities including the ICT systems?
(c) What ICFR reporting templates should be considered for stakeholders reporting of the control effectiveness test results.
(d) When is an Internal control over Financial Reporting considered adequate and effective or otherwise?

(5) Do you need expertise support from eternal consultants? If yes, what type of support do you need – co-sourcing or out-sourcing?

Implementing Internal Control Over Financial Reporting in any organization could be time-consuming and burdensome, particularly as the internal or in-house resources will be preoccupied with their core mandates to deliver on their primary job functions. In addition, knowledge gaps on ICFR and implementation standards and project management methodology could cause serious performance challenges for the in-house resources. Leveraging the expertise of credible external consultant may make a great difference in terms of quality of deliverables, time and cost savings. Whether an organization is using in-house resources or external expertise for the ICFR implementation, the process owners, risk and control owners and the three lines of defense play significant roles in helping the ICFR implementation succeed. The Securities and Exchange Commission and The Financial Reporting Council of Nigeria through (SEC-Guideline-on-Sec-60-63-of-ISA-2007 (8).pdf and FRC-Guidance-on-Management-Report-on-Internal-Control-over-Financial-Reporting-ICFR-1-1.pdf (frcnigeria.gov.ng) recommended the adoption of COSO Internal Control Framework or any other suitable standard such as Canadian CoCo or UK Turnbull Report for the implementation of the ICFR in Nigeria. CoCo was built on COSO Frameworks and mostly used in Canada, but COSO is the most globally adopted ICFR implementation framework and was used for the compliance of SOX404 ICFR requirements in the United States of America. Adopting COSO Internal Control Framework to implement Internal Control Over Financial Reporting requires reference to a number of COSO Internal Control–Integrated Framework 2013, a number of other COSO publications such as: COSO Internal Control-Integrated Framework: Executive Summary, COSO Internal Control-Integrated Framework: Framework and Appendices, COSO illustrative Tools: Assessing Effectiveness of a System of Internal Control and COSO Internal Control over External Financial Reporting: A Compendium of Approaches and Examples. Also required for referencing are and the subject guidelines provided by Financial Reporting

Council of Nigeria, Securities and Exchange Commission and Institute of Internal Auditors (IIA). The detailed information about COSO Frameworks and the key elements to consider in the ICFR implementation, the control effectiveness testing and reporting templates will be discussed in an upcoming ICFR Part 2 of the ICFR writing.

What are the Specific ICFR Implementation Phases an Organization can Adopt?

SEC ISA 2007, CAC CAMA 2020, FRC Act 2011 and COSO did not prescribe any specific implementation activity phases for the Implementation of ICFR in the organizations. SEC, FRC and COSO through the published guidelines provided only good practice guidelines about the key components of the internal control system, the specific principles and other factors that may be considered to demonstrate commitment to embedding adequate Internal Control in the organizations as well as testing the effectiveness. This means that the organizations adopting COSO or any other suitable framework may adopt different project different Implementation Activities lifecycle. Many leading practices organizations have prescribed different ICFR implementation activities lifecycle as guidelines. Based on my research on the many project management activities lifecycles prescribed by some of the leading practices organizations and my personal experiences working with the families of COSO frameworks and client projects on SOX404 ICFR Compliance and ISA 2007 ICFR projects, the ICFR Implementation Activities Phases presented in figure 4 below can be considered as a guide for a single location small/medium scale business.`

Figure 4 – A example of an ICFR implementation phase, key deliverables and timelines for s single location small/medium scale company

ICFR Implementation Phase	Key Activities To Be Considered	Key Deliverable To Be Considered	Estimated Timelines
Phase 1 – Project preparatory training	Conduct project Purpose Awareness training targeted at the key Principal stakeholders including senior and Executive Management, Boards and Board committees and Assurance Functions.	• Project Awareness training and Presentation Materials.	2 working days.
Phase 2 Project Planning	Obtain relevant background information about the organization which form input to the project planning processes. Project Planning, resources mobilization and validation of project Scope, deliverables, and Communication protocols	• Communications Protocols • Validate project deliverables, Documentation templates & Style, and Distribution Lists. • Tim table for interviews and focus groups discussions. • List of documents for desktop reviews and responsibility.	2 working days.
Phase 3 Conduct ICFR Readiness and Resilience Assessment	Conduct Entity level Gap Analysis to determine the overall tone at the top and commitment to excellence to reinforce vale driven risk culture. The activities involve: ✸ Understanding the business needs, stakeholders' expectations, regulatory requirements of ICFR and implications to the organization. ✸ Identifying current gaps in the organization's Risk Management and Internal Control systems specific to the ICFR project objective. ✸ Report on the gaps and recommendations top addressing the gaps. ✸ Agree with Management and Board the next steps to drive the project to fruition. ✸ Based on the agreed next steps, develop the initial route/roadmap for the transition from the current state to the targeted or envisioned state. Adopting COSO framework for the readiness assessment requires the five COSO components and 17 principles to the company's Enterprise Risk Management and internal Control Operating Models and Practices in order to assess whether the five COSO Internal control components and 17 principles are present and operating well in the organization.	Gap Analysis reports of finding showing the gaps and strengths to the business- needs, stakeholders' expectations, industry maturity model and the best practices benchmarks and recommendations to address the gaps.	3 woking ays.
Phase 3 Conduct Risk Control Mapping	Risk Assessment, control mapping and control rationalization. The objectives are to validate whether the components of	Financial statement accounts	15 working

Figure 4 – A example of an ICFR implementation phase, key deliverables and timelines for s single location small/medium scale company

ICFR Implementation Phase	Key Activities To Be Considered	Key Deliverable To Be Considered	Estimated Timelines
on key Financial Accounts	internal control and principles are designed and functional well at the financial statement reporting business process level. The activities involved include: **Risk Assessment** Assessment of the Control Activities Identification and quantification of the risks around the financial statement account to determine the significant accounts and mapping or linking the accounts to the business processes. **Control Mapping** Linking Controls to the specific risks identities and related financial statement accounts processes.	mapped to the risks and business processes	days
	Rationalization Analysis of the controls around the key financial statement accounts to determine strengths and gaps (weak controls and non-existent controls), finding redundant or duplicated controls and irrelevant controls and eliminating them from the financial statement reporting risk and control registers. **Optimization** remediate internal control gaps by redesigning or refining the existing poorly designed controls and introducing new controls where no controls exist, given consideration to the business needs, stakeholders expectations, statutory compliance requirements.	Financial statement, Reporting Risk and controls Registers highlighting the controls categories well designed controls, weak or poorly designed controls and controls that do not exist at all. Refined or transformed financial statement reporting risk and control registers with well-designed key controls mapped to the key financial statements accounts and related processes.	·5 working days
Phase 4 – Develop Financial Reporting Contyrol Blueprint & Implementation Roadmap.	Develop statements of guidelines and implementation of route map for embedding the ICFR into the corporate culture. Typical content include reference to the Financial Reporting Risk and Control register, processes, policies and procedures. Reporting templates for each category of stakeholders, distribution lists, reporting frequency responsibilities and implementation route map.	Financial Statement Reporting Blueprint	7 working days
Phase 5 Embed Financial Reporting Control Blueprint into Corporate culture.	**Key activities involved:** ✸ Assessing the training needs for each stakeholder categories (Board, Board Committee Members, Management Teams, Operational Staff and the Assurance Team for knowledge transfer. ✸ Use the training materials and facilitate training for each of the stakeholder's category. ✸ Incident tracking, root cause analysis and follow-up resolution. ✸ Continuous monitoring of the results of the financial statement risks and controls, collating and interpreting the reports, communication to the relevant stakeholders and quality validation.	• Training Material and attendance list, participants performance reports and certificates. • Stakeholder's Report. • Statistics of incidents, root cause and resolution status.	
Phase 6 – Control Self-assessment testing of financial reporting Control effectiveness.	Periodic testing of the adequacy and effectiveness of the ICFR (ICT controls, process Controls and data quality management controls) by the Assurance teams including Internal Audit function to enable the Management, Board, and other internal stakeholders develop insight on the quality of the ICFR in preparedness of the management certification as required by the laws and regulation.	• Populated Risk and Control Testing Sel-Assessment templates, working papers documentation, test evidences. • Management certification of the adequacy and effectiveness of the company's internal control over financial reporting and basis for the certification statement.	7 working days ·

Figure 4 – A example of an ICFR implementation phase, key deliverables and timelines for s single location small/medium scale company

ICFR Implementation Phase	Key Activities To Be Considered	Key Deliverable To Be Considered	Estimated Timelines
Phase 7 – Develop Stakeholders Reporting.	Consolidation of the audit observations and finding and developing stakeholder reports based on the Board approved frequency and regulatory requirements. Validate draft reports with the internal stakeholders' categories for accuracy, completeness, validity, etc.	Draft and final reports of observations or findings, conclusions and recommendation for improvement.	3 working days
Phase 8 – Continuous Quality Management programmes	Involves reviewing the ICFR Blueprint documents and content and operational practice for continued relevance in line with the business needs, stakeholders' expectations and regulatory compliance.	Quality management review reports improvement recommendations responsibilities and implementation timelines.	Driven by incidents, planned review cycle frequency, industry changes and events peculiar to the company.
Phase 9 Third Party Independent Attestation.	Attestation involves an independent review by an external statutory auditor of a company's financial statement data and effectiveness of the associated or link internal controls by applying the applicable methodologies and procedures as required by the regulation	External independent opinion on the adequacy and effectiveness of the company's internal controls over financial reporting and basis for the opinion.	Preferably, External Auditor responsibility.

It is important to note that some of the phases above can be collapsed or merged into one, for example, Phase 1 –Project Preparatory Training and Phase 2- Project Planning may be grouped under one. Similarly, Phase 3 – Conduct Risk Control Mapping on Key Financial Accounts and Phase 4 – Develop Financial Reporting Control Blueprint & Implementation road map. May be merged as one phase

The question on when an Internal Control System should be considered Adequate and Effective, how to test the entity level and control activities and what reporting templates to consider will be discussed in detail in my upcoming ICFR part 2 blog. However, a brief over view response to the question has been provided below.

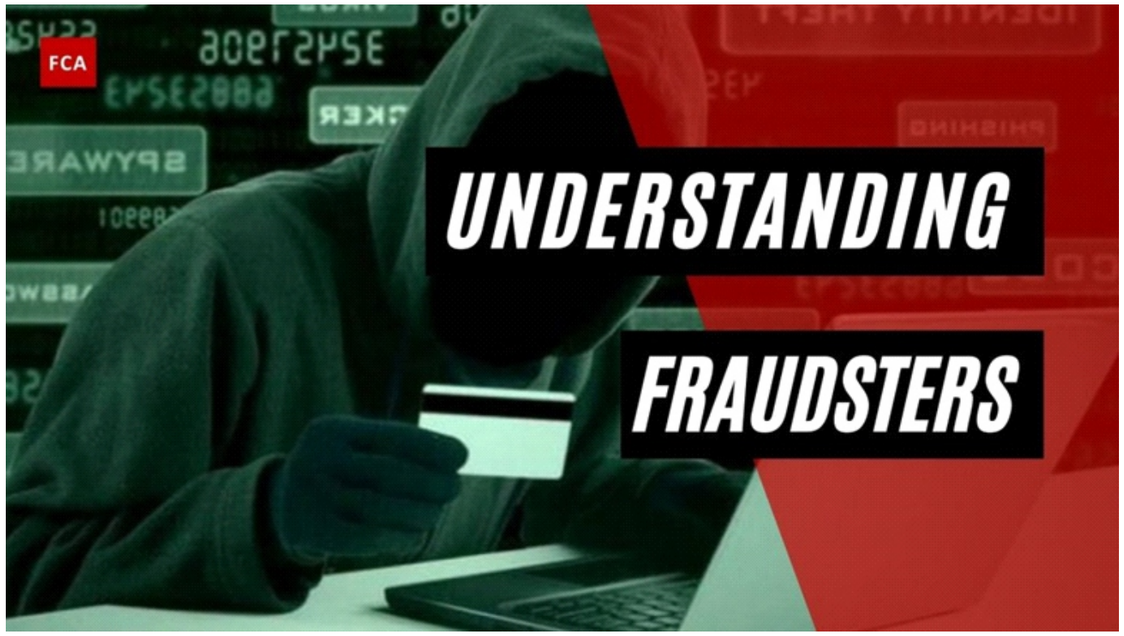
In Nigeria, the criteria for evaluating the adequacy and effectiveness of the internal controls, and the deficiencies in an organization depends on the Guidelines provided by the Financial Reporting Council of Nigeria (FRC) and Securities and Exchange Commission (SEC). The SEC and FRC guidelines on implementing Internal Control Over Financial reporting states that an internal control system is considered inadequate and ineffective if one or more material deficiencies that will lead to material misstatement of the financial statement reporting and disclosures have been identified. These deficiencies need to be remediated before the commencement of the statutory audit of the financial statements.

Based on COSO Internal Control perspectives, an effective internal control, each of the five components of COSO Internal Control and the 17 principles must be present and functioning well in the organization for the internal control system to be adequate and effective. COSO considers an internal control system to be deficient, inadequate and ineffective when at least one COSO Internal Control component does not exist in the organization and functioning well.

References:

1. Internal control - Wikipedia
2. What are Internal Controls? - Definition | Meaning Example (myaccountingcourse.com)
3. Internal Controls: Definition, Types, and Importance (investopedia.com)
4. Internal Control | COSO
5. www.cac.gov.ngResources (CAMA 2020)| Corporate Affairs Commission (cac.gov.ng)
6. The Securities and Exchange Commission, Nigeria
7. (FRC-Rules-Updated-Original-Rule-4-Inclusive.pdf (frcnigeria.gov.ng).
8. (SEC-Guideline-on-Sec-60-63-of-ISA-2007 (8).pdf
9. FRC-Guidance-on-Management-Report-on-Internal-Control-over-Financial-Reporting-ICFR-1-1.pdf (frcnigeria.gov.ng)
10. COSO Internal Control-Integrated Framework: Executive Summary,

Sally Ogwo Okey-Umahi
(MIoD, Auditor, Speaker) Executive Director,
Platinum Edge Consulting



The Psychology of Fraudsters in the Corporate Sector: Motivating Factors and Deterrence Strategies

Fraud remains a much less researched typology than other crime categories, probably due to the fact that these offences are generally non-violent, usually undramatic, and are often perceived, however mistakenly, to involve neither immediate nor direct personal loss, and consequently, no victim is easily or quickly identified Shawyer and Walsh (2007). Nobody is a born fraudster; rather, a person is motivated to become one by their circumstances and environment. Fundamentally, frauds are motivated by a person's or a group's existing circumstances and surroundings and is greatly influenced by how a person or group acts and thinks in a given circumstance, as well as by how honest they are. (Shivam and Chandana 2019).

The only thing that is constant in fraud is change as it is a dynamic process which is multi-layered and penetrates corporate procedures while the fraudsters always find new methods to commit fraud and cover their traces. As a result, dealing with fraud is a long, complicated procedure that requires a deep understanding of both the reasons behind its occurrence and the ways by which it can be mitigated. Fraud is a widely conceivable concept, but its characteristics are frequently unrecognizable and not until it is too late. According to the Institute of Internal Auditors, fraud is "any illegal act characterized by deceit, concealment, or violation of trust". These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage (Vousinas, 2017).

Corporate fraud is a growing phenomenon that impacts organizations, and a crucial point is that the fraud is carried out by the typical white-collar criminal, who is educated, has status and has a lot to lose if discovered. The popularly used Fraud Triangle proposes that three elements are normally evident when fraud happens; the pressure or motive, the rationalization and the opportunity ' (Fahad & Rubasundram, 2020). Whilst this has mainly been used to assess the thoughts of a potential fraudster, all forms of fraud including occupational fraud is done covertly since it violates the employee's fiduciary duty to the company, and the fraud is committed to gain direct or indirect financial benefit to the fraudster at the cost of the organization's assets, reserves, and revenues.

International Standard of Auditing 240 (2009) defines fraud as a purposeful conduct by one or more people, including management and those in positions of authority, employees, and third parties, that

involves the use of deception to acquire an unfair or illegal benefit. The perpetrator must have knowledge of the conduct and the purpose to deceive for it to be declared fraud, and the victim must have experienced loss or damage as a result of the act (Fisher, 2015). Therefore, in the corporate sector, fraud refers to any action taken or knowledge of an action taken to obtain an unfair or illegal benefit. Ramamoorti and Olsen (2007) defined fraud as a human activity that involves deception, deliberate intent, intensity of desire, risk of being caught, breach of trust, rationalization, etc. Therefore, it is crucial to comprehend the psychological aspects that may have an impact on the actions of fraudsters. The notion that one must "think like a crook to capture a crook" provides the justification for using behavioral science ideas (Ramamoorti, Morrison, & Koletar 2009). Many business professionals, particularly in the financial sector, have a propensity to undervalue behavioral explanations. But as the prevalence of fraud rises,

putting a focus on behavioral aspects could be a crucial strategy for both detecting fraud and deterring it.

Many organisations both private and public sectors are struggling to deal with fraud. Importantly, fraud by collusion of two or more people, according to the latest study of the Association of Certified Fraud Examiners (ACFE), is the most difficult crime to be detected and results in high financial loss for organisation. Surprisingly, this kind of fraud remains "clouded and shallow", and it cannot be solved by the preventive framework which is focused on the solo psychology of fraud perpetrators (Nuswantara & Maulidi, 2020).

Fraud prevention is profitable and can help to ensure stability and going concern of any organisation. Once fraud has occurred, it is not easy to recover such losses, as such it is advisable to prevent such losses from occurring. There is a saying "prevention is better than cure". It is important to be proactive rather than reactive. The possibility of being caught mostly persuades the potential fraudsters not to commit fraud.

Concept of Psychology

The word 'psychology' is derived from two Greek roots: 'psyche', meaning mind or soul, and 'logos', meaning 'study of'. Psychology, therefore, literally means 'study of the mind'. A definition by Atkinson, Atkinson, Smith, Bern, & Hilgard, (1990) suggests that psychology is 'the scientific study of behaviour and mental processes. Psychology is the study of the nature, functions, and phenomena of behavior and mental experience; simply put, it is the science of human behavior (Malimage, 2019). In general, psychology seeks to understand, explain, predict, and control individual and group behavior. Specifically, personality psychology studies individuals; social psychology looks at group behavior; cross-cultural psychology (anthropology) analyzes the impact of culture and context on behavior; and abnormal/personality/forensic psychology, sociology, and psychiatry focus on deviant behavior (including for instance, industrial psychopaths). Criminological psychology studies psychological problems associated with criminal behavior, criminal investigation, and the treatment of criminals (Colman

2003).

Concept of Fraud

Ernst and Young (2009) defines fraud as an act of deliberate action made by an entity, knowing that such action can result in a possession of unlawful benefits. Adeniji (2004) and Institute of Chartered Accountants of Nigeria (ICAN) (2006), states that fraud is an intentional act of individuals among management, employees or third parties who produce errors in financial reporting in favour of their personal desires. Fraud can also be considered as any deliberate misrepresentation, concealing and negligence of a truth to manipulating the financial statement at the expenses of the firm.

Merriam Webster's Dictionary of Law (1996) as quoted in Manurung and Hadian (2013) defined fraud as "Any act, expression, omission, or concealment calculated to deceive another to his or her disadvantage, specifically, a misrepresentation or concealment with reference to some facts material to a transaction that is made with knowledge of its falsity and or in reckless disregard of its truth or falsity and with the intent to deceive another and that is reasonably relied on by the other who is injured thereby".

Fraud is any intentional act or omission designed to deceive others, resulting in the victim suffering a loss and the perpetrator achieving a personal gain. Fraud is any attempt on the part of an agent, officer, employee, or representative of a business or other entity to induce another person or entity to give specific information about the goods or services offered or the interest rates or fees that may be paid. Fraud is an attempt by a person to obtain access to something or profit by misleading other people. Fraud commonly includes theft, corruption, conspiracy, embezzlement, money laundering, bribery, and extortion. The legal definition varies from country to country, but fraud generally involves using deception to dishonestly make a personal gain for oneself or create a loss for another.

Concept of the Fraudster

The term "fraudster" comes from a Latin word that means deception. To commit fraud is to use misleading or fabricated information to accomplishan illegitimate intention and unlawful acts. Fraudsters can be classified into three categories: pre-planned fraudsters, intermediate fraudsters, and slippery-slope fraudsters.

Pre-Planned Fraudsters

These consist of fraudsters who have pre-conceived intention to commit fraud. For instance, a pre-planned fraudster can create multiple accounts to steal credit cards from shoppers and companies and use stolen credit to buy luxury goods online. Pre-planned fraudsters can be either short-term or long-term players. Short-term pre-planned fraudsters are engaged in fraudulent acts for immediate gain without the intention to continue the action in future. Long-term pre-planned fraudsters are professional fraudsters who have constantly engaged in fraudulent activities to dispose others of their money and other valuables. Examples of long-term pre-planned fraudsters include bankruptcy fraudsters and those who execute complex money laundering schemes.

Intermediate Fraudsters

Intermediate fraudsters are honest individuals who become fraudsters during hard times or when an urgent need arises to meet personal and family obligations. Hence, intermediate fraudsters become fraudsters because of the need to survive and pay for family members' care.

Slippery-Slope Fraudsters

Slippery-slope frauds are the newest and most innovative methods of fraud. They consist of fraudsters who purchase items with other people's money. The slipper-slope fraudsters lure victims into revealing sensitive personal information by offering instant gratification or cheap goods and services. Slippery-slope fraud may also entail infecting the victim's computer with a piece of software called a 'backdoor'. Slippery-slope fraudsters can also remotely access the victim's computer to extract valuable information (such as passwords and other personal data) from the computer.

Profiles of Fraudsters

There are two broad profiles of fraudsters: opportunity fraudsters and professional fraudsters.

Opportunity Fraudsters

An opportunity fraudster is usually a law-abiding person who sees an opportunity to commit fraud. For example, this type of fraudster might imagine insurers have unlimited funds and might find it acceptable to make up claims to recover premiums paid in previous years when there was no claim. Opportunity fraudsters perpetrate most internal frauds. For instance, an opportunity fraudster might falsify expenses or inflate the price of purchased inventory for his benefit or personal gain.

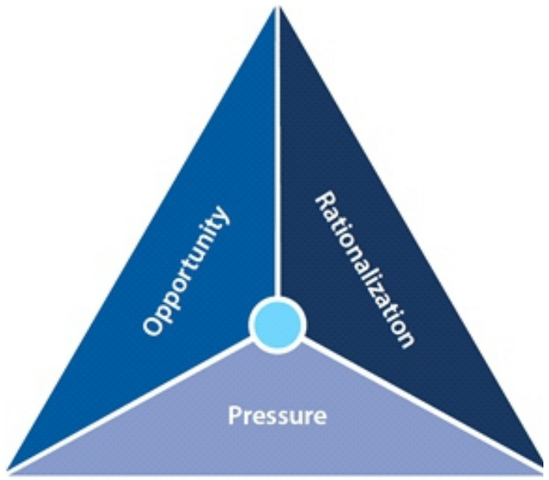
Professional Fraudsters

Professional fraudsters are criminals who specialize in getting other people to part with their money and valuables. Professional fraudsters often target vulnerable people. A professional fraudster earns and complements their income by committing fraud. Although they may be operating under the guise of a legitimate business; but they intend to steal and defraud their victims for their gain. Professional fraudsters may use a business name and email address, but their identity is often difficult to trace. An extension of the professional fraudster profile is an organized crime involving persons capable of committing complex and extensive fraud. They may be students, seniors, or business owners. These professionals rely on a network of accomplices to carry out their fraud and succeed in business.

Psychology of a Fraudster

Criminality is not confined to the lower classes and to social misfits but extends, especially where financial fraud is concerned, to upper-class and socially well-balanced. Two factors should be considered in analyzing the psychology and personality of the fraudster: The biological qualities of an individual, which vary widely and influence behavior, including social behavior, the social qualities that are derived from and in turn shape how the individual deals with other people. Three general types of financial fraudster have been observed: Calculating criminals who want to compete and to assert themselves and situation-dependent criminals who are desperate to save themselves, their families or their companies from a catastrophe. Third type of criminal that has emerged out of catastrophic business failures and embarrassments is called power broker.

According to AKGVG & Associates (2022), corporate frauds are deceptions performed by people against the companies that employ them, and frequently, these deceptions are carried out in a dishonest or unethical way. Corporate fraud can be extremely difficult to identify and harder to stop. The organization can somewhat reduce the risk of fraud by implementing policies, conventions, and checklists. Though corporate frauds can be committed in a variety of ways, the most typical mode of operation involves gaining access to and using sensitive information from the company—such as reports, facts, and information about clients, vendors, and employees—for one's own benefit. The term "Fraud Triangle" is used in various accounting and auditing studies that explain three basic reasons behind corporate fraud. The three points involved are pressure, opportunity, and rationalization. All three elements must be present for fraud to occur.



Fraud Triangle (Cressey 1953)

Pressure is a mindset of an individual or employee towards committing fraud and occur when employee is under financial duress. Not meeting the financial targets for example pressurizes employees to commit fraud. There are different types of pressure viz: 1. financial pressure – motivated by greed, living beyond one's means, high bill or personal debt, personal financial loss, unexpected financial needs, debt burdens, medical issue, falling sales. 2. Work related pressure – getting little recognition for job performance, having or feeling of job dissatisfaction, fearing losing one's job, being overlooked for promotion, feeling under paid. 3. Vice pressure – gambling, drug, alcohol, expensive extra marital relationship. 4. Other pressure – spouse who insist on improved lifestyle, challenge to beat the system, legitimate financial needs, speculative investment, feeling over worked and under paid, greed and tendency for ask for more.

Opportunity means ability to execute plan without being caught (Cressey 1953). It is probably the only major area where a company can exercise control over. Employee in this case is in the position to commit crime. The following could give rise to such factors: weak internal control, poor management oversight, poor accounting and financial statement recording, weak corporate governance, failure to discipline fraud perpetuators, lack of audit trail, lack of access to information, lack of supervision, lack of segregation of duties.

Rationalization mentally justifying the crime or developing a defense mechanism to justify his/her action as follows: the organization owe it to me, I am only borrowing the money and will pay back, nobody will get hurt, I deserve more, it is for a good purpose,

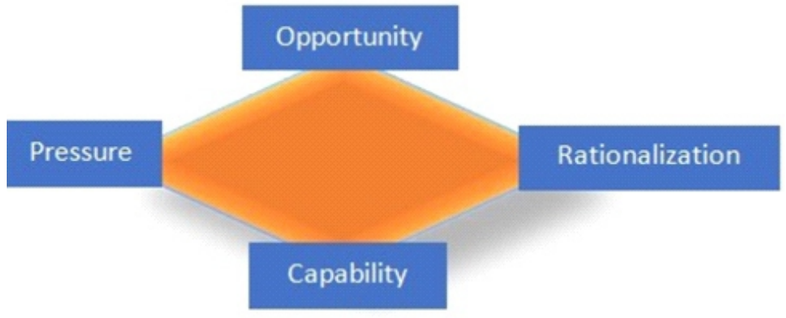
something has to be sacrificed, we will fix the book as soon as we get over this financial difficulty.

Capacity According to Wolfe & Hermanson (2004), even if a fraudster has a strong motive (pressure), opportunity, and justification (rationalization), there will be chances that fraudster might not commit fraud if there is no 'capability'. Capability here means traits, ability or position of authority to pull off the crime, capacity to understand and exploit accounting system and internal control weaknesses to the greatest advantage, confident that fraud behaviour will not be detected or believes that he could easily talk himself out of trouble if caught, capacity to deal with stress in order to manage the fraud.

Fraud Diamond Theory Wolfe & Hermanson (2004)

Factors and Motivations for Fraud in a Firm: Empirical Review

The study by Boyle, DeZoort, and Hermanson (2015) examined the fraud triangle, the fraud diamond, and CEO risk level among a sample of eighty-nine auditors



in public accounting in an experiment. Their results indicate that auditors who evaluated fraud risk factors based on the fraud diamond demonstrated higher fraud risk assessments than auditors who evaluated based on the fraud triangle. Dellaportas (2013) examined the factors that influence accountants to commit fraud using the fraud triangle. The data were collected through face-to-face interviews of ten accountants serving sentences in prison for committing fraud and other offenses. While the findings differed from inmate to inmate, the overall findings suggest that the offenders used their position as accountants to deceive others when they faced a crisis. The findings also suggest that pressures varied from financial to non-financial and internal control deficiencies were taken advantage of by the perpetrators. The perpetrators also demonstrated various rationalizations for their fraudulent acts.

Shivam and Chandana (2019) examined the 'perceived pressure' element of the fraud triangle. The study found Need, Greed and Vices as the prime factors of motivation for an individual. These three factors are linked together in a cycle and often progressive from one activity to another. Bonny, Goode, and Lacey (2015) in their extensive study found that living beyond means, gambling, sudden external financial pressure, naturally dishonest person, external pressure from others to steal, drug dependency, alcohol problem and internal pressure from workmates to steal are the most common pressures and motivation to commit frauds for an individual.

Manurung and Hardika (2015) studied the used financial stability, external pressure, and financial targets as the variable for 'Pressure', ineffective monitoring, and nature of the industry as the variables for 'Opportunity', switching the auditors as a variable for 'Rationalization' and change in directors as a variable for 'Capability'. The study found that only change in directors, the variable for capability, had significant correlation with financial statement fraud. Cohen, Ding, Lesage, and Stolowy (2010), examined the role of manager's behavior in the committing fraud. The study holds the question whether the actual reasons behind fraud are in line with the categories of fraud triangle theory and Theory of planned behavior. The study identified five conditions each under Incentive/Pressure and Opportunities which would lead to fraudulent activities by the managers. Condition such as (1) expectations of investment analyst, institutional investors, significant creditors etc; (2) the existence of significant financial interests in the entity; (3) a significant portion of the compensation being contingent upon achieving aggressive targets for stock price, operating results, financial position or cash flow; (4) a high degree of competition or market saturation and (5) the need to obtain debt or equity financing to stay competitive pressurizes the managers to commit fraud.

Baker, Cohanier, and Leo (2016) studied whether there may have been additional factors beyond those of the traditional "fraud triangle" which contributed to the breakdowns in internal control system.

To be continue in the next Edition

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

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

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
07040092783

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

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

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

Ecobank Nigeria Ltd
Tunde Dawodu
Ecobank Pan African Centre (EPAC)
270, Ozumba Mbadiwe Street,
Victoria Island, Lagos, Nigeria.
tdawodu@ecobank.com
08023070443

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

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

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

First Bank of Nigeria Ltd
Mufutau Abiola
9/11, McCarthy Street, Lagos
Mufutau.Abiola@firstbanknigeria.com
081291456605

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

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

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

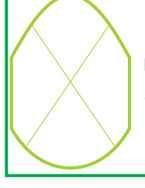
Globus Bank Limited
Monday Edwards
6 Adeyemo Alakija Street,
Victoria Island, Lagos
mondayedward@globusbank.com
08023192506

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

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

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

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



Lotusbank
2, Bourdillon Road
Ikoyi Lagos.

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

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

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

Nova Merchant Bank
Isiaka Arowolo
23, Kofo Abayomi Street
Victoria Island, Lagos.
Isiaka.arowolo@novambl.com
08033088681

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

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

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

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

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

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

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

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

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

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

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

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

Union Bank of Nigeria Plc
36 Marina,
Lagos.

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

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

Wema Bank Plc.
Oluwole Esomojumi
Wema Towers
54 Marina, Lagos
Oluwole.esomojumi@wemabank.com
08094214819

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