CENTRAL BANK OF NIGERIA
Central Business District
Cadastral Zone AO
P.M.B 0187, Garki
Abuja

OTHER FINANCIAL INSTITUTIONS SUPERVISION DEPARTMENT
Tel: 09-46235439
e-mal: ofisd@cbn.gov.ng
Website: www.cbn.gov.ng

OFI/DOA/CON/CIR/003/061

August 13, 2021

LETTER TO ALL OTHER FINANCIAL INSTITUTIONS

EXPOSURE DRAFT OF THE RISK-BASED CYBER-SECURITY FRAMEWORK AND GUIDELINES FOR OTHER FINANCIAL INSTITUTIONS

Due to the recent increase in the number and sophistication of cyber-security threats and attacks against Other Financial Institutions (OFIs), it has become necessary and mandatory for the sub-sector to strengthen its cyber resilience if it is to remain safe and sound.

Consequently, the Central Bank of Nigeria is releasing the attached draft framework and guidelines stipulating minimum requirements for enhancing cyber-security for your comments/inputs.

Kindly send hard copies of your comments/inputs to the Director, Other Financial Institutions Supervision Department, while soft copies should be mailed to OFISDITExaminer@cbn.gov.ng on or before September 17, 2021.

Thank you for your usual cooperation.

NKIRU E. ASIEGBU
Director, Other Financial Institutions Supervision Department

Cc: National Association of Microfinance Banks (NAMB)
Mortgage Banks Association of Nigeria (MBAN)
Finance Housing Association of Nigeria (FHAN)
Association of National Development Finance Institutions (ANDFI)

RISK-BASED CYBERSECURITY FRAMEWORK AND GUIDELINES

FOR

OTHER FINANCIAL INSTITUTIONS (OFIs)

MAY 2021

Table of Contents

1. Introduction

The safety and soundness of Other Financial Institutions (OFIs) require that they operate in a safe and secure environment. Hence, the platform on which information is processed and transmitted should be managed in a way that ensures the confidentiality, integrity and availability of information as well as the avoidance of financial loss and reputational risk, amongst others.

Considering the reliance of financial institutions on information and communications technology (ICT) to operate their business and the rising incidences of cyber threats and attacks targeted at financial institutions, it has become necessary to implement cybersecurity measures to mitigate against those risks.

In recent times, threats such as ransomware, targeted phishing attacks and Advanced Persistent Threats (APT) have become prevalent; demanding that financial institutions including OFIs strengthen their cyber resilience and take proactive steps to secure their critical information assets to ensure their safety and soundness.

Cybersecurity resiliencies considered as an organization's ability to maintain normal operations despite all cyber threats and potential risks in its environment. Resilience provides an assurance of sustainability for the organization using its governance, interconnected networks and culture.

It is against this background that the CBN hereby issues this framework and Guidelines for OFIs. The Guidelines outline the minimum requirements that OFIs are required to observe in the development and implementation of strategies, policies, procedures and related activities aimed at mitigating cyber risk.

The purpose of the Guidelines is to:

a. Create a safer and more secure cyber environment that supports information system security and promote stability of the OFI sub-sector
b. Contribute towards the prevention and combating of cybercrime in the OFI sub-sector;
c. Promote the adoption and implementation of best practices and appropriate cybersecurity standards by OFIs;
d. Promote and maintain public trust and confidence in the OFI sub-sector

e. Promote a cybersecurity culture and awareness through continuous capacity building and skills development.

OFIs should note that for a cybersecurity programme to be successful, it must be fully integrated into their business goals and objectives, and must be an integral part of the overall risk management processes.

The framework provides a risk-based approach to managing cybersecurity risk. The document comprises six parts: Cybersecurity Governance and Oversight, Cybersecurity Risk Management System, Cyber Resilience Assessment, Cybersecurity Operational Resilience, Cyber-Threat Intelligence and Metrics. Monitoring & Reporting.

2. Cybersecurity Governance and Oversight

2.1 Cybersecurity governance sets the agenda and boundaries for cybersecurity management and controls through defining, directing and supporting the security efforts of the OFIs. It spells out the responsibilities of the Board of Directors, Senior Management and Chief Information Security Officer (CISO). This entails the development and implementation of policies, procedures and other forms of guidance that the OFIs and their stakeholders are required to follow.

2.2 The responsibility for the provision of oversight, leadership and resources to ensure that cybersecurity governance becomes an integral part of corporate governance rests with the Board of Directors of the OFI. In this regard, the Board shall ensure that cybersecurity is completely integrated with business functions and, well managed across the OFI.

2.3 Furthermore, the Board shall ensure that cybersecurity governance not only aligns with corporate and Information Technology (IT) governance, but is cyber-threat intelligence driven, proactive, resilient and communicated to all internal and external stakeholders.

2.4 The **responsibilities of the Board of Directors** in relation to cybersecurity include:

2.4.1. The Board of Directors directly or through its appropriate Committee(s) shall have oversight and overall responsibility for the OFI's cybersecurity programme.

2.4.2. Promote a cybersecurity conscious culture within the institution through robust oversight and engagement on cybersecurity.

2.4.3. Ensure that cybersecurity is completely integrated with business functions and well managed across the OFI.

2.4.4. Ensure that cybersecurity governance aligns with corporate and Information Technology (IT) governance. It shall also ensure that cybersecurity governance is cyber-threat intelligence driven, proactive, resilient and communicated to all internal and external stakeholders.

2.4.5. All board members are required to understand the nature of their institution's business and the cyber threats involved.

2.4.6. Establish the institution's vision, risk appetite and overall strategic direction with regards to cybersecurity.

2.4.7. Formulate cybersecurity strategy, policy, procedures, guidelines and set minimum standards for the institution. The Cybersecurity Policy shall be documented and made available for review by the CBN and NDIC Examiners.

2.4.8. Allocate adequate resources for cybersecurity based on the institution's structure

2.4.9. Review management's determination of whether the institution's cybersecurity preparedness is aligned with its cyber risks

2.4.10. Establish or review cybersecurity risk ownership and management accountability and assign ownership and accountability to relevant business lines and not just the IT function

2.4.11. Approve and continuously review the cybersecurity strategy, governance charter, policy and framework which shall provide direction on how to achieve the institution's cybersecurity goals. The strategy shall align with the institution's overall corporate strategy

2.4.12. Ensure that the cybersecurity policy applies to all of the institution's branches, operating entities, including subsidiaries and joint ventures

2.4.13. Review on a regular basis the implementation of the institution's cybersecurity framework and implementation plan, including the adequacy of existing mitigating controls

2.4.14. Incorporate cybersecurity as a standing agenda item at Board meetings.

2.4.15. Review the results of management's ongoing monitoring of the institution's exposure to and preparedness for cyber threats.

2.4.16. Ensure that cybersecurity processes are conducted in line with business requirements, applicable laws and regulations while ensuring security expectations are defined and met across the OFI.

2.4.17. Receive and review on a quarterly basis reports submitted by Senior Management. The report shall detail the overall status of the cybersecurity programme to ensure that the Board approved risk thresholds relating to cybersecurity are being adhered to.

2.4.18. Appoint or designate a qualified individual as the "Chief Information Security Officer" (CISO) who shall be responsible for overseeing and implementing its cybersecurity programme. In the case of a Group structure, such OFI may leverage on its group CISO where the OFI is part of a group that has a CISO.

2.4.19. Ensure that the cybersecurity budget is approved.

2.5 The **responsibilities of Senior Management** shall include:

2.5.1. Senior Management shall be responsible for the implementation of the Board-approved cybersecurity strategy, policies, standards and the delineation of cybersecurity responsibilities.

2.5.2. Provide periodic reports (at a minimum quarterly) to the Board on the overall status of the cybersecurity, cyber risk posture/overall status of the OFI.

2.5.3. Ensure the creation of mitigation and recovery procedures to contain cyber risk incidents, reduce losses and return operations to normal

2.5.4. Implement processes and procedures to protect customer data, transactions and systems.

2.5.5. Ensure the provision of adequate, experienced and skilled staff for the management of cybersecurity.

2.5.6. Incorporate cybersecurity as a standing agenda item at Senior Management meetings.

2.5.7. Document cybersecurity incident response plan indicating the actions the institution will take during and after a security incident. The plan should address inter-alia:

a. The roles and responsibilities of staff;

b. Incident detection, assessment, and reporting;

c. Escalation and strategies deployed.

2.5.8 Collaborate with other institutions and the security agencies to share the latest development on cyber threats/attacks encountered by the institution

2.5.9 Create a post incident analysis framework to determine corrective actions to prevent similar incidents in the future.

2.5.10 Evaluate and manage risks introduced by third party service providers

2.5.11 Develop the cybersecurity framework for Board approval

2.5.12 Submit the Board approved cybersecurity framework to the Director, Other Financial Institutions Supervision Department for information and records.

2.6 Appointment and responsibilities of the Chief Information Security Officer (CISO):

Every OFI shall appoint or designate a Chief Information Security Officer (CISO) whose responsibilities shall include the following:

2.6.1. The day-to-day cybersecurity activities and the mitigation of cybersecurity risks in the OFI.

2.6.2. Develop, oversee and implement the cybersecurity programme and strategy as approved by the Board.

2.6.3. Ensuring that the institution maintains an updated record of its users, devices, applications and their relationships, including but not limited to:

2.6.4. Software and hardware asset inventory; and

2.6.5. Network utilization and performance data.

NIST	National Institute of Standards and Technology
NgCERT	Nigeria Computer Emergency Response Team
OEMs	Original Equipment Manufacturer
OWASP	Open Web Application Security Project
PCI DSS	Payment Card Industry Data Security Standard
POS	Point of Sale
PSP	Payment Service Provider
ROC	Report on Compliance
SAQ	Self-Assessment Questionnaire
SMS	Short Message Service
TV	Television Set
USSD	Unstructured Supplementary Service Data

Glossary

2-Factor Authentication	This is a process in which a user provides two different authentication factors to verify his identity.
Access Control Matrix	Access Control Matrix is a security model in computing that defines the access rights or authorization of each subject with respect to objects in the system.
Acceptable Interruption Window	This is the maximum allowable time of interrupting mission critical systems or applications before restoration.
Advanced Persistent Threat	APT is a targeted network attack in which an unauthorized malicious entity gains access to a network and remains undetected for a long period of time.
Anti-Skimming Device	This is a device that prevents fraudulent capture of personal data from the magnetic stripes cards when they are used on devices such as an ATM.
Automated Teller Machine	This is an intelligent electronic banking channel, which allows banks" customers have access to basic banking services without the aid of any bank representative.

Business Continuity/ Disaster Recovery Plan	These are planned processes that help OFIS prepare for disruptive events and recover within a short period
Bring Your Own Device	BYOD is a privilege given to employees to use their personally owned devices (laptops, smart phones etc.) to access information and resources of their work place.
Cloud Security Alliance	A non-profit organization with a mission to "promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing"
Cyberspace	This is an imaginary environment where communication over computer networks occurs
Demilitarized Zone	A demilitarized zone or DMZ in computing is a physical or logical sub-network that separates the trusted (internal local area network) from other untrusted networks (Internet). It houses external-facing servers, resources and services meant to be accessed from the internet.
False Positive	A false positive is a false alarm generated by a device, process or entity; usually based on preconfigured rules or logic.
False Negative	False negative occurs when a security device omits a vulnerability
Firewall	This is a network security system or software that has the capability to monitor and control incoming and outgoing network traffic based on preconfigured rules.
Financial Services Information Sharing and Analysis Center	This is a global financial industry's information sharing organization that provides timely authoritative information on physical and cyber security threats to help protect the critical systems and assets of its members.
Intrusion Detection System	A device or software/application that monitors a OFIS"s network or systems for policy violations and/or malicious activities.

Internet Protocol Phone	A phone built on Voice over IP technologies (VoIP) for transmitting telephone calls over an IP network, such as the Internet.
Intrusion Prevention System	This is a network threat prevention technology that examines network traffic to identify possible threats while preventing potential exploits of system vulnerabilities.
International Organization for Standardization	ISO is a non-governmental organization with a mission to "promote the development of standardization and related activities in the world with a view to facilitating the international exchange of goods and services, and developing cooperation in the spheres of intellectual, scientific, technological and economic activity."
Local Area Network	A computer networking technology that links devices within a specific range.
Log Management	This is an automatic way of dealing with large volumes of systemgenerated logs. It usually comprises of Log collection, correlation, analysis, search, reporting and retention
Malicious code	Any code or script developed with an intention to cause undesired effects, security breaches or damage to a system.
Mobile code	Any malicious programme, application, or script capable of moving when implanted in an email, document or website.
Nested Payment Service Provider	Any entity that is contracted for its services by another payment service provider for the purposes of providing a service.
Non-Disclosure Agreement	A legal contract or agreement between two or more parties that outlines a degree of confidentiality.
Nigeria Computer Emergency Response Team	A team of experts in the Office of the Nigerian National Security Adviser with a mission to "manage the risks of cyber threats in the Nigeria's cyberspace and effectively

	coordinate incident response and mitigation strategies to proactively prevent cyber-attacks against Nigeria".
Nigeria Cybercrime Act, 2015	This is the first cybercrime bill enacted by the National Assembly of the Federal Republic of Nigeria in 2015
Open-source cyberthreat intelligence	A platform, blog, database that collects, stores and share information on emerging cyber threats, indicators and trends to its subscribers
Open Web Application Security Project	This is a non-profit organization that provides journals, methodologies, documentation, and development of best practices, in the field of web application security at no cost.
Payment Card Industry Data Security Standard	This is an information security standard for OFIs that collect, process, store and transmit cardholder data.
Payment Service Providers	These are third-party service providers who use their infrastructure to store, process, or transmit DMB"s customer information including cardholders" data.
Point of Sale terminal	This is a device that accepts payment cards for electronic funds transfers.
Privileged user	Any user who by virtue of function has super system-rights in any computer, application, database, device, etc.
Patches	These are software designed to improve the features, security, etc. of a system, device, and application/software.
Service Level Agreement	This is a contract between a service provider and a subscriber; who defines the level of service expected from such service provider.
Standard Operating Procedure	This is a step-by-step instruction on carrying out routine operations/tasks. Its purpose it to achieve uniformity of performance, efficiency and quality output at all time.
Threat	Anything that has the potential to cause damage or loss to an information asset.

Unstructured Supplementary Service Data	This is a communication technology used to send message between a mobile phone and an application on a network.
Value Added Service	A term used to describe non-core services of a service provider but offered to its customers.
Vendors	Provider of goods or services to OFI
Vulnerability	This is a weakness or gap in a system, application, process, device, etc.
Cyber Risk	Cyber Risk is any risk to the Confidentiality, Integrity and Availability of an organization's critical information assets arising from a failure of the organization's information technology systems resulting to financial loss, disruption of services, and interference with business as usual or damage to the reputation of the organization.
Cybersecurity	Cybersecurity is therefore an activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.