Central Bank of Nigeria

Banking Supervision Department
Plot 33, Abubakar Tafawa Balewa Way
Central Business District
P.M.B 0187, Garki, Abuja - Nigeria.
Email: bsd@cbn.gov.ng
Website: www.cbn.gov.ng
Phone: +234 700-225-5226, +234 800-225-5226

BSD/TEN/CON/SRF/03/057 February 19, 2024

LETTER TO ALL DEPOSIT MONEY BANKS AND PAYMENT SERVICE BANKS

EXPOSURE DRAFT OF THE RISK-BASED CYBERSECURITY FRAMEWORK AND GUIDELINES FOR DEPOSIT MONEY BANKS AND PAYMENT SERVICE BANKS

The Nigerian financial system has grown remarkably in recent years with increases in products, services, institutions and stakeholders. Financial Institutions have increasingly leveraged Information Technology to serve their customers and this has led to rapid evolution in the threat landscape. It is necessary that the technology infrastructure and platforms that support financial institutions operations should be managed effectively to promote a sound financial system.

Consequently, the Central Bank of Nigeria has revised the **Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks (DMBs) and Payment Service Banks (PSBs)** to provide guidance in the implementation of cybersecurity programmes and enhance resilience. The revised framework addresses the gaps that have arisen due to the passage of time and outlines the minimum cybersecurity controls to be put in place.

The exposure draft Framework and Guidelines is herewith attached for comments and inputs from stakeholders to enable the CBN finalise the document and issue same subsequently. The exposure draft can be accessed at the CBN website **www.cbn.gov.ng**.

Your comments/inputs can be forwarded to the CBN either in hard or soft copies; hard copies should be sent to the Director, Banking Supervision Department, Central Bank of Nigeria, Abuja, while soft copies should be emailed to bsdcybersecurity@cbn.gov.ng within **three (3) weeks from the date of this letter**.

Thank you.

DR. ADETONA S. ADEDEJI
AG. DIRECTOR OF BANKING SUPERVISION

CENTRAL BANK OF NIGERIA
RISK-BASED CYBERSECURITY FRAMEWORK AND GUIDELINES

FOR

DEPOSIT MONEY BANKS AND PAYMENT SERVICE BANKS

August 2023

Contents

ACRONYMS

ACM	Access Control Matrix
AI	Artificial Intelligence
API	Application Programming Interface
ATM	Automated Teller Machine
BOFIA	Banks and Other Financial Institutions Act
BYOD	Bring-Your-Own-Device
CCISO	Certified Chief Information Security Officer
CISM	Certified Information Security Manager
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
CSAT	Cybersecurity Self-Assessment tool
CSP	Cloud Service Providers
CTI	Cyber-Threat Intelligence
DDoS	Distributed Denial-of-Service
DLT	Distributed Ledger Technology (DLT)
DMB	Deposit Money Banks
ERM	Enterprise-wide Risk Management
FS-ISAC	Financial Services Information Sharing and Analysis Center
IaaS	Infrastructure as a Service
ICAAP	Internal Capital Adequacy Assessment Process
IDS	Intrusion Detection System
IoT	Internet of Things
IPS	Intrusion Prevention System
IR	Incident Response
ISSC	Information Security Steering Committee
KYC	Know Your Customer
MFA	Multifactor Authentication
ML	Machine Learning
NDPA	Nigerian Data Protection Act
NeFF	Nigeria Electronic Fraud Forum
NFC	Near Field Communication
NFIC	Nigeria Financial Industry CERT
NgCERT	Nigeria Computer Emergency Response Team
NigFinCERT	Nigeria Financial Nigeria Computer Emergency Response Team
OSINT	Open-Source Intelligence
PaaS	Platform as a Service
PAM	Privileged Access Management
PoS	Point of Sale
PSB	Payment Service Banks
PT	Penetration Test
QR	Quick Response
RBAC	Role Based Access Control
SaaS	Software as a Service
SDLC	Software Development Life Cycle
SFI	Supervised Financial Institution
SLA	Service Level Agreement
SOC	Security Operation Centre
USSD	Unstructured Supplementary Service Data

INTRODUCTION

The Nigerian financial system has witnessed remarkable growth in recent years, which has led to an increase in products, services, institutions and stakeholders. To increase public confidence in the financial system, it is imperative that banks operate in a safe and secure environment.

Financial Institutions leverage information technology to expedite the flow of funds among entities and for the provision of services to their customers. The technology infrastructure and platforms that support their operations should be managed to safeguard the confidentiality, integrity and availability of information assets, as well as prevent financial loss and mitigate reputational risk.

Cybersecurity threats have continued to evolve and become more complex, with increased frequency of threats such as phishing, ransomware, Distributed Denial-of-Service (DDoS) attacks, amongst others. Consequently, financial institutions are required to proactively secure their critical information assets to ensure that they remain resilient in the face of these persistent threats. The prevalence of the use of emerging technology by financial institutions to deliver services to customers has also increased their attack surface.

It is in this regard that this framework, which outlines the minimum cybersecurity controls to be put in place is being issued. The CBN's Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks (DMBs) and Payment Service Banks (PSBs) is designed to provide guidance in the implementation of cybersecurity programmes towards enhancing their resilience.

The framework provides a risk-based approach to managing cybersecurity risk. The document comprises seven parts: Cybersecurity Governance and Oversight; Cybersecurity Risk Management System; Enhancing Cybersecurity Resilience; Emerging Technologies; Metrics, Monitoring & Reporting; Compliance with Statutory & Regulatory Requirements and Enforcement.

This framework replaces the Risk-based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers issued in October 2018 and addresses the gaps that have arisen due to the passage of time. It equally considers requirements of recent laws and regulations such as the Banks and Other Financial Institutions Act (BOFIA 2020), Nigerian Data Protection Act (NDPA) 2023, etc. The framework should be read in conjunction with all the provisions of all directives, notices, circulars and guidelines that the CBN may issue from time to time.

The CBN Risk-based Cybersecurity Framework and Guidelines for DMBs and PSBs, 2023, shall apply to the following financial institutions under the purview of Banking Supervision Department – Commercial banks, Merchant banks, Non-Interest banks and Payment Service banks, which are hereinafter jointly referred to as Supervised Financial Institutions (SFIs).

1.0 Cybersecurity Governance and Oversight

Cybersecurity governance and oversight sets the agenda and boundaries for cybersecurity management and controls by defining, directing and supporting the security efforts of SFIs. It outlines the responsibilities of the Board of Directors, Senior Management, Chief Information Security Officer (CISO) and other relevant Risk Management Control functions. Governance and oversight entail the development and enforcement of policies, procedures and other forms of guidance that SFIs and their stakeholders are required to comply with.

1.1. Responsibilities of the Board of Directors

The Board, through its committees, shall have oversight and responsibility for the SFIs cybersecurity programme. It shall provide leadership, direction and resources for the effective conduct of required processes and shall ensure that cybersecurity governance is integrated into the organisational structure and relevant processes. To this end, the Board shall be responsible for ensuring that:

i. at least two Non- Executive Directors (NEDs), one of whom shall be an Independent NED, shall have requisite knowledge and experience in innovative financial technology, Information Communication Technology (ICT) and/or cybersecurity.

ii. cybersecurity is integrated with business functions and well managed across the SFI.

iii. cybersecurity governance not only aligns with Corporate and Information Technology (IT) governance but is driven by business objectives.

iv. cybersecurity management processes are conducted in line with business requirements, applicable laws and regulations while ensuring security targets are defined and met across the SFI.

v. Senior Management provides central oversight for the cybersecurity programme, assigns responsibilities and ensures the effectiveness of the cybersecurity management processes.

vi. the audit function is independent and staffed with skilled professionals who possess relevant qualifications and experience.

vii. cybersecurity governance documents such as cybersecurity strategy, framework and policies are established and aligned with the SFI's business goals and objectives.

viii. quarterly reports detailing the overall status of the cybersecurity programme are presented by Senior Management. The reports shall, at a minimum, include the following:

a. cyber risk assessment report or updates from the last assessment.

b. status of security initiatives to address cyber risks.

c. incidents recorded, status of losses and recoveries.

d. vulnerability management/ penetration test reports, remediation efforts and challenges encountered therein and compensating controls implemented.

e. status of compliance with Board-approved cyber risk thresholds.

f. status of compliance with Examiners' recommendations in the report of the CBN Cybersecurity Supervisory Review and Evaluation exercise.

ix. a qualified individual is appointed as the CISO on the recommendation of Senior Management. The CISO shall be responsible for overseeing and implementing the bank's cybersecurity programme.

x. in the case of banking Groups, while institutions may collaborate with the group CISO to ensure an effective enterprise-wide cybersecurity programme, a CISO shall be appointed in conformity with the requirements in Section 1.4 of this Framework.

xi. a stand-alone cybersecurity budget which is distinct from other function's budget (e.g., Information Technology or Risk Management) is approved.

xii. cybersecurity risk appetite is defined in the Enterprise-wide Risk Management (ERM) framework.

1.1.1. Cybersecurity Strategy and Framework

The Board is responsible for the SFI's cybersecurity strategy and shall ensure that:

i. the strategy provides direction on how to achieve the cybersecurity goals, mitigate cyber-risk and comply with all legal, contractual, statutory and regulatory requirements.

ii. the approved cybersecurity framework aligns with business objectives and technological approaches to address cyber risks and clearly defines key cybersecurity roles and responsibilities.

iii. the cybersecurity policy clearly conveys its intent and the SFI's approach to achieving the cybersecurity objectives.

iv. the cybersecurity policy is reviewed annually at a minimum, or when there are significant changes to the SFI's cyber-risk exposure.

1.1.2. Cybersecurity Programme

SFIs are required to implement a cybersecurity programme which should, at a minimum, include:

- Risk assessment
- Security policy development
- Incident response planning
- Vulnerability management
- Log monitoring
- Data backup and recovery plan
- Security awareness and training
- List of initiatives to attain target maturity level
- Metrics to assess the effectiveness of the programme

1.2. Responsibilities of Senior Management

Senior Management shall be responsible for the implementation of Board-approved cybersecurity policies, standards and the delineation of cybersecurity responsibilities. They shall be required to:

i. recommend to the Board the appointment of a CISO that meets the regulatory requirements.

ii. obtain CBN approval for the appointment of the CISO.

iii. provide periodic reports (at a minimum quarterly); to the Board on the overall status of the cybersecurity programme as stipulated in Section 1.1 (vii).

iv. ensure that staff of the Information Security function attend relevant training programmes regularly.

v. incorporate cyber-risk management in the ERM framework and governance requirements to ensure consistent management of risk across their institution.

vi. drive cyber risk management processes to ensure adherence to cybersecurity risk appetite.

1.3. Responsibilities of the Chief Information Security Officer

The CISO shall be responsible for the day-to-day cybersecurity activities and the mitigation of cyber risks in the SFI. Consequently, the CISO shall:

i. be responsible for overseeing and implementing the cybersecurity programme and strategy approved by the Board.

ii. develop secure business and communication practices, identify security objectives and metrics, recommend the acquisition of security products/tools to keep information assets safe and resilient, maintain the SFI's data privacy and ensure all employees undertake security awareness training periodically.

1.4. Requirements for appointment as a Chief Information Security Officer

The SFI shall appoint a CISO who meets the under-listed requirements subject to CBN approval:

i. The CISO shall possess adequate authority, experience, independence and shall be of appropriate grade to function effectively. The minimum grade of staff to be appointed CISO shall be as specified below or as may be approved by the CBN from time to time:

   a. Commercial Bank with International Authorisation – Senior Manager
   b. Commercial Bank with National Authorisation – Senior Manager
   c. Non-Interest Bank with National Authorisation – Manager
   d. Commercial Bank with Regional Authorisation – Manager
   e. Merchant Bank – Manager
   f. Non-Interest Bank with Regional Authorisation – Manager
   g. Payment Service Bank – Manager

ii. The CISO shall report directly/functionally to the Managing Director/Chief Executive Officer.

iii. There shall be no direct or indirect report to the Head of Information Technology (IT) operations or Chief Risk Officer to avoid conflict of interest.

iv. The Appointment of a CISO shall be in line with the provisions of the Revised Assessment Criteria for Approved Persons' Regime for Financial Institutions, 2015 or any subsequent regulation.

v. Where the SFI is part of a Group that has a Group CISO charged with establishing and maintaining an enterprise vision, strategy and programme, the SFI's CISO is required to replicate the responsibilities as required in Section 1.4 of this Framework.

vi. The CISO shall possess relevant qualifications with Information Security Certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Certified Chief

Information Security Officer (CCISO) among others and a minimum of ten year's in-depth experience in any of the following roles: Cybersecurity, Information Technology, IT Risk Management or IT Audit.

1.5. The Information Security Steering Committee

Every SFI shall establish an Information Security Steering Committee (ISSC) that shall be responsible for the governance of the cybersecurity programme. The committee shall meet the following requirements:

i. It shall comprise senior representatives of relevant departments within the SFI and shall be chaired by the MD/CEO, while the Executive Director in charge of Technology/Operations may serve as the alternate chairman.

ii. The roles, responsibilities, scope, and activities of the ISSC shall be as defined in the Terms of Reference.

iii. The ISSC shall meet at least once in a quarter.

iv. The agenda for the meeting shall include a presentation on the "State of cybersecurity" and address recent cyber events, vulnerabilities and proposals for controls to reduce cyber risks. The summary of the report shall be included in the reports to the Board referenced in Section 1.1(vii).

1.5.1 Terms of reference of the ISSC

The ISSC shall be responsible for:

i. ensuring that SFI's security policies and processes align with the business objectives.

ii. evaluating, approving, and sponsoring institution-wide security investment.

iii. enforcing implementation of policies for investment prioritization and security risk management.

iv. providing strategic direction and cybersecurity governance for the SFI.

1.6. Other Risk Management Control Functions

All SFIs shall ensure the effectiveness of their cybersecurity governance by reviewing their processes and controls annually. In this regard, these risk management control functions shall have the following responsibilities:

1.6.1 Risk Management

i. The Risk Management function, internal or outsourced, shall independently evaluate all the risks proactively relating to cybersecurity. This should be executed using appropriate tools and methodologies for risk identification, analysis and control. The assessment report shall be presented to Senior Management monthly and the Board Risk Management Committee quarterly.

ii. Senior Management shall ensure that staff or external risk management professionals engaged to evaluate the institution's cybersecurity posture possess the requisite qualifications and experience.

1.6.2. Audit

i. The Audit function shall be independent and the scope of cybersecurity audits shall be clearly defined.

ii. The SFI’s cybersecurity programme shall be reviewed by the Audit function, internal or external, with a view to determine the effectiveness of the controls put in place and ascertain if they are adequate for the institution’s risk exposure.

iii. Senior Management shall ensure that internal or outsourced audit staff engaged to review the institution's cybersecurity posture possess requisite qualifications and experience.

1.6.3 Compliance

The Compliance function of SFIs shall periodically review the cybersecurity programmes and processes to ensure adherence to relevant CBN directives and extant regulations.

2.0 Cybersecurity Risk Management System

The Risk Management programme shall be based on an understanding of threats, vulnerabilities, risk profile and level of risk tolerance of SFIs. The process shall also be dynamic in view of the constantly changing risk landscape.

2.1. The Risk Management System

The Risk Management System shall cover the five activities below:

2.1.1 Risk Identification

SFIs shall identify associated threats and vulnerabilities to the confidentiality, integrity and availability of their information assets to determine their cyber risk exposure.

2.1.2 Risk assessment

SFIs are required to evaluate risks to their operations, probability of occurrence, impact of risk crystallisation, and security controls that would mitigate identified risks.

This process should be carried out annually and whenever major changes occur within the institution such as an acquisition, merger or when new technology is deployed to handle key business processes. The outcome of this process should be documented in a Cybersecurity Risk Control Self-Assessment.

An independent Audit function should be charged with the responsibility of ensuring that the methodology used in risk assessment is reviewed periodically.

2.1.3 Risk measurement

The Risk Measurement process should quantify the financial impact of Cybersecurity risks to the SFI. The potential impact of such risks should be accounted for as part of Pillar II risks in its Internal Capital Adequacy Assessment Process (ICAAP).

2.1.4 Risk mitigation/Risk treatment

SFIs should implement risk mitigation and control measures that are consistent with the criticality of information assets. Risk treatment options such as risk reduction, risk acceptance, risk avoidance, risk transfer and how residual risk is addressed should be selected based on the outcome of the risk assessment.

Risk acceptance criteria should be clearly defined and approved by the Board. In cases where the SFI chooses to transfer risk, a detailed risk assessment for outsourcing or cyber risk insurance should be documented.

2.1.5 Risk monitoring and reporting

An independent risk management function shall be responsible for assessment, measurement, monitoring and reporting of risks associated with critical IT infrastructure and services while cybersecurity function shall be responsible for risk mitigation/treatment.

A Risk Register should be maintained to facilitate monitoring and reporting. Risk should be closely monitored and reported to the Board and Senior Management in line with defined risk appetite and acceptance criteria.

2.2. Vulnerability Identification

i. The information security function should ensure adequate risk assessment and sign-off before deployment of new technology-based products.

ii. SFIs shall ensure the conduct of yearly vulnerability assessments and threat analysis to detect and evaluate risk to its information assets and determine the appropriateness of security controls to mitigate identified risk.

iii. A third-party shall conduct a penetration test annually, at a minimum.

iv. SFIs shall ensure that internal vulnerability scans are carried out quarterly.

2.3. Third party risk management

SFIs should implement a third-party risk management framework to assess and mitigate the risks associated with such relationships. The third-party risk management framework should include processes for vendor selection, due diligence, contract negotiations, ongoing monitoring and incident response.

Third-party cybersecurity awareness programme should be conducted at least annually to inform stakeholders about their roles and responsibilities around cybersecurity.

Contracts with third parties should be used to implement appropriate measures designed to meet the objectives of the SFI's cybersecurity programme.

Third parties should be routinely assessed using audits, test results, or other forms of evaluations to confirm that contractual obligations are fulfilled.

Service Level Agreements (SLAs) should specify SFIs' right to audit third parties or receive audit reports.

Business continuity response and recovery planning and testing should be conducted with third-party providers.

SFIs should implement some form of Insurance cover for various insurable technology risks to mitigate financial losses.

2.4. Cybersecurity Maturity Assessment

SFIs shall conduct annual evaluation using the CBN Cybersecurity Self-Assessment tool (CSAT) to determine their maturity level.

2.4.1 Determining the Current Cybersecurity Profile (current state)

To determine its current state, an SFI shall carry out the following:

i. Identify its Inherent Cyber risks.

ii. Assess existing Cybersecurity mitigants.

The Cybersecurity Self-Assessment report shall be submitted to the CBN.

2.4.2 Establishing a Target Cybersecurity Profile (desired state)

SFIs shall determine their desired state of cybersecurity maturity. The information security function shall ensure that a roadmap towards achieving the target cybersecurity profile is included in the SFI's corporate strategy.

2.5. Reporting Cybersecurity Self-Assessment

Self-assessment for coverage period (January to December of the previous year) shall be submitted to the Director, Banking Supervision Department of the Central Bank of Nigeria annually, not later than March 31. The report shall be signed and submitted by the CISO after its endorsement by the Executive Management in the format prescribed from time to time.

3.0 Enhancing Cybersecurity Resilience

Cyber resilience is the SFI's ability to prevent, withstand and recover from cyber incidents.

SFIs are required to establish procedures to enhance their cyber resilience. This will ultimately strengthen the financial industry's cybersecurity posture.

The following are the minimum controls that an SFI shall put in place to ensure the confidentiality, integrity and availability of critical information assets among others.

3.1 Know Your Environment

An SFI shall proactively familiarise itself with its business environment and identify its critical assets. To ensure effective security measures, an SFI shall establish mechanisms for maintaining up-to-date inventory of authorised software, hardware as well as internal and external network connections. Additionally, an SFI shall identify and document its data, assets and capabilities. Also, potential threats and vulnerabilities associated with its assets should be monitored.

Employees and contractors providing information technology and cybersecurity services shall also be identified and documented. Details on specific controls are contained in Appendix II.

3.2 Implement Preventive Controls

An SFI shall implement appropriate measures/controls/safeguards for IT systems, processes and people to mitigate cyber risks. These can be administrative, logical or physical controls. Details on specific controls are contained in Appendix III.

3.3 Monitor and Detect

An SFI shall establish capability for ongoing (24/7) monitoring of its IT systems, infrastructure, applications, services, and other relevant components to promptly detect anomalies or cyber incidents. This capability can be outsourced to a third-party

provider or managed internally. Regardless of the chosen approach, SFIs shall ensure the monitoring is adequate to detect cyber threats.

3.4 Respond and Remediate

An SFI shall ensure that the capability for responding to cyber incidents is available in-house or, if outsourced, can be accessed at short notice.

Details on specific controls are contained in Appendix III.

3.5 Restore Service Operations

An SFI shall aim at recovering its operations timeously to reduce the overall impact of cyber incidents.

Details on specific controls are contained in Appendix III.

3.6 Cyber-Threat Intelligence

An SFI is expected to possess knowledge of emerging threats, cyber-attacks, attack vectors, mechanisms and indicators of attack/compromise that may impact its information assets.

Details on specific controls are contained in Appendix III.

3.7 Sector-specific Cyber Resilience

An SFI shall participate in industry cyber exercises and programmes to evaluate its individual and joint response to potential cyber incidents that may have systemic consequences, as may be advised from time to time.

SFIs shall avoid creating single points of failure in the industry and proactively define plans to mitigate such risks.

4.0 Emerging Technologies

Emerging technologies refer to innovative advancements that are in the early stages of development or adoption and have the potential to significantly influence various industries. SFIs are adopting new technologies and global trends that are transforming various aspects of banking operations and customer experiences.

Some emerging technologies and trends are highlighted below:

1. New Payment Methods
    a. Contactless Payments using Card, Quick Response (QR) codes, Smart Phones and Wearables.
    b. Voice-initiated services
    c. Unstructured Supplementary Service Data (USSD) Codes.
2. Open Banking
3. Distributed Ledger Technology (DLT)
4. Artificial Intelligence (AI) and Machine Learning (ML)
5. Cloud Computing
6. Internet of Things (IoT)
7. Fintech Connections to Banks

4.1 New Payment Methods

4.1.1 Contactless Payments using Card, Quick Response (QR) codes, Smart Phones and Wearables

Contactless payments rely on near field communication (NFC) technology, which allow the transfer of payment information wirelessly between a payment device and a terminal. Cyber-risks associated with the use of contactless payments include data Interception, NFC Spoofing, malicious mobile Apps, Point-of-Sale device tampering.

4.1.2 Voice-initiated services

The adoption of Voice-initiated services by SFIs for customer authentication, information request, transactional commands etc., as a banking channel is expected to be more widespread. Cyber-risks associated with this technology include voice spoofing, unauthorised access, data breach.

4.1.3 Unstructured Supplementary Service Data (USSD) Codes

USSD is a communication system used by mobile network operators to provide quick access to services and information through Short Message System (SMS). SFIs have expanded the functionality of USSD codes to provide financial services.

Cyber-risks associated with the use of USSD include smishing, social engineering, Distributed Denial of Service (DDoS) and SIM Swap.

4.1 Open Banking

Open Banking refers to the practice of sharing financial data, such as account and transaction information, products and services with other financial institutions and third parties through API connections.

The Regulatory Framework for Open Banking in Nigeria establishes principles for data sharing across the banking and payments system to promote innovation and broaden the range of financial products and services available to bank customers.

Cyber-risks associated with open banking include data privacy, fraud, identity theft and API compromise.

SFIs should ensure compliance with the provisions of the Regulatory Framework for Open Banking in Nigeria and Operational Guidelines for Open Banking in Nigeria.

4.2 Distributed Ledger Technology

Distributed Ledger Technology (DLT) is a platform that uses ledgers stored on separate, connected devices in a network to ensure data accuracy and security. Blockchain, is a widely recognised DLT that uses cryptographic techniques to facilitate the process of recording transactions and tracking assets. Applications of DLT include digital identities

for Know Your Customer (KYC), cross-border payments solutions that enable real-time, peer-to-peer transfers, etc.

Cyber-risks involved with DLT include API compromise, data privacy, data loss, Smart Contract vulnerabilities, Money Laundering, Terrorism Financing and Proliferation Financing.

4.3 Artificial Intelligence and Machine Learning

Artificial Intelligence (AI) and Machine Learning (ML) technologies are intelligent machines capable of performing tasks that typically require human intelligence. These include natural language processing, computer vision and robotics. SFIs have adopted AI and ML solutions for the analysis of economic activity, fraud detection, prevention of money laundering, detection of operational issues, improved customer services and online real-time risk management.

These emerging technologies may also be used to improve cybersecurity defences by automating threat detection, anomaly detection and response.

Cyber-risks involved with the use of AI and ML include data breach, data leak, limited data, poor data quality, breach of privacy laws, opaque algorithms, lack of skilled data professionals.

4.4 Cloud Computing

Cloud computing provides access through the web to resources and products, including development tools, business applications, services, data storage, and networking solutions.

SFIs have embraced the use of third-party cloud services in their operations for the benefit of scalability, cost-efficiency, accessibility, security and reliability.

However, such engagements introduce risks including data breach, API compromise, Insider threats, account hijacking, data loss, lack of visibility, Compliance and legal issues.

4.5 Internet of Things

Internet of Things (IoT) refers to the network of physical devices, objects embedded with sensors, software and connectivity. SFIs use IoT to facilitate efficient data collection, processing and automation of key processes.

Cyber-risks involved with the use of IoT include Insecurely configured or poorly protected IoT devices, poor firmware configurations, connectivity and power dependencies, insecure communication and data breach.

4.6 FinTech Connections to Banks

FinTechs may integrate with SFIs systems through API. There has been an increase in the use of APIs for the exchange of customers' data with a view to driving innovation and offering improved financial services.

FinTech connections expose SFIs to cyber risks such as fraud, API compromise, unauthorised access, data privacy, data breach, compliance and legal issues.

SFIs are required to comply with the following regulations in the use of emerging technologies:

1. obtain CBN approval before deploying new emerging technologies or products.
2. desist from engagements with parties and countries on sanction lists.
3. refrain from establishing API connections or granting access to organisations not licensed by the CBN without prior regulatory approvals.
4. maintain professional due diligence and care in the adoption of emerging/evolving technologies.

The minimum-security controls that SFIs shall put in place in the adoption or implementation of new technologies are detailed in Appendix IV.

5.0 Metrics, Monitoring and Reporting

SFIs are required to measure the effectiveness of their cybersecurity programme and provide assurance to relevant authorities by defining and implementing performance metrics.

Defined metrics should be aligned with strategic objectives and provide the information needed for effective decision-making at the strategic, management and operational levels.

i. To assess the effectiveness of the SFIs' cybersecurity programme and measure its performance and efficiency, metrics that may be employed include key performance indicators, key risk indicators, key goal indicators etc. Defined metrics should be reviewed at least annually.

ii. The metrics should help to identify deficiencies, failed security controls as well as highlight the progress made in resolving issues.

iii. SFIs shall establish effective communication channels to disseminate relevant security requirements to employees for effective implementation of the cybersecurity programme.

iv. The Board shall be provided with quarterly reports to inform them of the status of the Cybersecurity programme. The contents of the reports shall be as defined in Section 1.1(vii) of this framework.

v. SFIs are required to report all cyber incidents (as defined in Appendix I) not later than 24 hours after such incident is detected to the Director of Banking Supervision, Central Bank of Nigeria using the report format in Appendix VII or any other format that may be advised from time to time. Where necessary and applicable, additional information should be provided afterwards.

6.0 Compliance with Statutory and Regulatory Requirements

i. The Board and Senior Management of SFIs shall ensure compliance with all relevant statutes and regulations such as the Nigerian Cybercrimes Prohibition, Prevention Act, 2015, NDPA, 2023, National Cybersecurity Policy and Strategy, 2021, etc., and all CBN directives to avoid breaches of legal, statutory, regulatory obligations on Cybersecurity.

ii. SFIs shall participate in Industry cyber exercises and programmes to evaluate their individual and joint response to potential cyber incidents that may have systemic consequences, as may be advised from time to time. Such exercises may be conducted by the Nigeria Financial Nigeria Computer Emergency Response Team (NigFinCERT) or any other body as may be advised periodically.

iii. Non-compliance with the provisions of this framework shall attract appropriate sanctions as defined in Section 68 of BOFIA, 2020 or subsequent regulations.

7.0 Enforcement

i. The CBN shall monitor and enforce compliance with the provisions of this framework.

ii. This shall be done through the annual Cybersecurity Supervisory Review and Evaluation exercise, Risk Based Examination, Annual Industry Standard Compliance audit and periodic spot check exercises.

APPENDICES

APPENDIX I: Critical Systems and Cyber-Incidents

For the purpose of this framework, ‘critical system’ shall mean any IT infrastructure (servers, applications, databases, network, ATM, POS, etc.) whose unavailability (such as failure, unplanned downtime, etc.), corruption, unauthorized access and/or interception of the information it stores, processes or transmit will result in a significant financial loss and negatively impact business operation and service to customers.

Cyber-Incident is referred to as any incident which may result in:

i. financial loss that exceeds 0.01% of shareholders’ funds unimpaired by losses.
ii. data breach and data destruction.
iii. unplanned outage in Core Banking Application.
iv. website defacement.
v. any glitch that results in financial losses.
vi. others that may be determined from time to time.

APPENDIX II: Know Your Environment

A sound knowledge of the institution's business and IT environment is crucial to managing its cybersecurity posture to ensure resilience.

1.1. Know Your IT Assets

SFIs shall:

a. Maintain an up-to-date inventory of all authorized IT assets on-premises and in third-party cloud infrastructure used to process, store or transmit data/information such as workstations, laptops, ATMs, POS, network switches, routers, firewall, printers, scanners, photocopiers, IP Phones, Mobile devices, surveillance cameras, Applications, Databases, Services, Protocols etc.

b. Establish asset ownership and assign responsibility for managing each asset to a specific individual or team.

c. Ensure that all identified devices are categorized by the criticality and sensitivity of the data/information they store, process or transmit.

d. Identify and document account profiles (systems administrators and privileged users), third-party vendors accounts, etc.

e. Regularly review the account profile of staff (systems administrators and privileged users) and third parties who have access to devices identified in "1.1" above.

f. Maintain an inventory of all data assets, including locations, owners and access controls.

g. Implement a data classification framework that categorises data based on its sensitivity and criticality.

h. Document data handling procedures, retention policies and secure data disposal processes.

i. Maintain an approved up-to-date network topology diagram of wired and wireless networks irrespective of location.

j. Maintain a catalog of all network connections to regulatory authorities, switches, third parties and wholesale customers with details of the objectives of such connections.

k. Regularly review the catalog and remove any connection that is no longer required.

1.2. Know Your Vulnerabilities

SFIs shall:

a. implement a vulnerability management policy approved by the Board.

b. conduct a vulnerability assessment of all IT assets and present the report of the assessment to ISSC and Senior Management at least once every quarter.

c. conduct vulnerability assessment when there is a significant change to the institution's information processing infrastructure (such as installation of new systems, devices, applications, etc.) or when there is knowledge of new vulnerabilities.

d. where possible, implement automated vulnerability scanning tools for continuous identification of vulnerabilities.

e. conduct external Penetration Test (PT) on IT Assets at least annually. Penetration Tests may be conducted more-frequently on internet-facing financial systems/applications.

f. conduct regular audits of IT assets and associated services, on premises and in cloud infrastructure to identify any potential weaknesses. This may include third-party audits, security reviews or compliance assessments.

g. continually identify inherent risks and vulnerabilities associated with IT platform/protocols used for business services e.g., USSD, Mobile Banking among others.

h. establish efficient mechanisms and processes to identify patch compliance status of IT assets.

1.3. Know Your Threats

SFIs shall:

a. establish a Cyber-Threat Intelligence (CTI) programme approved by the Board which should include policies to aid proactive identification of emerging cyber threats, trends, patterns, risks, and possible impacts.

b. identify and document various internal and external Cyber Threat Intelligence Sources. Internal sources are the IT infrastructures that generate logs. External sources are reputable commercial threat intelligence sources. These feeds should be integrated with security controls to enhance threat detection and response capabilities.

c. leverage "Open-Source Intelligence (OSINT) by monitoring publicly available sources, such as search engines, online forums, social media platforms, and security blogs.

d. where possible, monitor the dark web for mentions of the institution, critical assets, or sensitive information such as customers' data or staff's access credentials.

e. take informed decisions based on the CTI programme as it provides valuable information on areas susceptible to cyber-attacks, latest threats, attack vectors, etc. Decisions may include reviewing the Bring-Your-Own-Device (BYOD) policy, conducting emergency staff or customers awareness/training, vulnerability assessment, penetration testing, review of vendor source codes, cyber-incident response plan, BCP/DR plans, vendor SLA, among others.

f. engage in information sharing and collaboration with trusted industry peers, sector-specific information sharing establishments e.g., Nigeria Computer Emergency Response Team (NigFinCERT), Nigeria Financial Industry CERT (NFIC), Financial Services Information Sharing and Analysis Centre (FS-ISAC), Nigeria Computer Emergency Response Team (ngCERT), Nigeria Electronic Fraud Forum (NeFF), Law Enforcement Agencies (LEAs), and other Cybersecurity information sharing communities. Sharing threat intelligence will enable the financial industry to stay ahead of emerging threats.

g. promptly report all cyber-threats to their information assets to the Director of Banking Supervision of the Central Bank of Nigeria using the Cyber-threat Intelligence Reporting template in Appendix VII. The report should be rendered on or before the 5th day of the following month.

1.4. Know Your Third-Party Service Providers and Connections

SFIs shall:

a. maintain a record of all third-party service providers (including Cloud Service Providers-CSP).

b. periodically review their records to ensure discontinued third parties' access credentials have been revoked and network connections terminated.

c. identify and document all connections to third parties - wholesale customers, vendors and switches that provide Value-Added-Service (VAS). The objective of each connection shall be documented and reviewed regularly.

d. evaluate the security controls and processes of the CSP before adopting a cloud service. Where applicable the data centre and network infrastructure facilities of third parties should be visited, their cybersecurity policies should be reviewed to ensure that all cybersecurity concerns are addressed.

1.5. Know Your Privileged Users:

SFIs shall:

a. identify and document all employees and system/service accounts with privileged access on systems, applications and databases in an Access Control Matrix (ACM).

b. regularly review the ACM to ensure privileges are withdrawn once staff role changes.

c. ensure that risks associated with this category of persons are regularly assessed as part of the enterprise risk assessment framework.

APPENDIX III: Cybersecurity Controls

Implementing cybersecurity controls is a strategic and proactive approach to protecting critical assets, ensuring uninterrupted operations and safeguarding reputation. SFIs are expected to implement measures and procedures to protect their systems, networks and data from unauthorized access, use, disclosure, disruption, modification or destruction. Minimum expectations are provided below:

1. Implement Preventive Controls

1.1. Access Controls

SFIs shall:

Establish an access control policy to ensure that:

a. mechanisms, standards and procedures that govern users', systems' and service accounts' access provisioning, authentication and authorisation exist on all IT systems, network and applications.

b. a review of user access is conducted periodically to confirm that only least privilege rights are granted to authorised systems/applications.

c. access modification or revocation is carried out immediately when there is a change or discontinuation of role.

d. multifactor authentication, Role Based Access Control (RBAC) and layered controls are implemented to secure employees, customers and third-party access to the institution's network, systems and applications.

e. authentication mechanisms used for systems and applications are based on their criticality and sensitivity. Critical systems must use multi-factor authentication.

f. access is continuously validated using mechanisms such as Zero-Trust to prevent the use of compromised credentials.

g. channels to report access credential breaches exist and are communicated to relevant stakeholders.

h. mechanisms for automated recovery/blocking of compromised accounts are implemented.

1.2. Privileged Access Management (PAM)

SFIs shall:

a. at a minimum, biennially conduct background checks on employees such as System administrators, Database Administrators, Application Administrators, Information Security professionals etc., who implement policies and procedures to protect sensitive information. These checks should include CRMS checks, address verification, social media checks, lifestyle analysis, amongst others.

b. establish controls such as just-in-time access, session monitoring, password vaulting, least privilege principles and segregation of duties for privileged accounts.

c. ensure logon credentials to critical systems, applications, and network are created and separately documented by at least two employees.

d. ensure that all logs and audit trails of privileged users' activities are preserved and regularly reviewed in accordance with the institution's security policy.

e. prohibit the use of shared default or anonymous privileged account by multiple users.

f. ensure that logon credentials of default system accounts including test and development servers are changed before they are commissioned for use.

1.3. Third Party Service Providers or Vendors Access Control:

SFIs shall:

a. ensure that vendors do not have unfettered access to systems, databases, network and applications.

b. ensure that access requests by a vendor to information assets are approved by management. Access shall be limited to the part of the system required for a defined duration and should be monitored and revoked on completion of the task.

c. ensure that vendors are not left unattended when accessing information assets.

1.4. Physical Access Controls

SFIs shall:

a. establish physical security measures including, but not be limited, to physical access controls such as video surveillance, biometrics, etc.

b. ensure that vendors are accompanied when physically accessing critical information systems such as a Data Centre.

c. maintain and review logs of physical entry into sensitive areas.

1.5. Secure System Configuration Management

SFIs shall:

a. develop minimum security baseline configuration such as anti-malware, data loss prevention and systems security settings for IT assets, which should be governed by vendor recommendations, best practice and security standards. Additional informative references that can be adopted to develop security baseline configuration are contained in Appendix V.

b. ensure that policies for security solutions are managed centrally and cannot be turned off locally by users.

c. ensure hardening of new computer systems, Applications, or Databases prior to release into production.

d. ensure that configuration information of hardware and software are reviewed and verified regularly.

e. Ensure that wireless network use strong encryption and the frequency of encryption key change has been defined.

1.6. Application and Data Security

SFIs shall:

a. ensure cybersecurity controls are considered and incorporated in all stages of the system/application lifecycle. The business requirement for the acquisition/development of systems/applications shall identify and document the security requirements.

b. ensure secure coding practices and conduct regular security testing throughout the Software Development Life Cycle (SDLC) to identify and address vulnerabilities in applications and systems.

c. ensure that Open-Source codes or libraries are properly tested before use.

d. implement Data Discovery and Classification, appropriate Data Access Controls, Encryption, and Data handling procedures based on the sensitivity of the Data.

e. provide regular training and awareness programmes to employees to educate them on data handling best practices, security measures and their responsibilities in protecting data assets.

f. deploy data loss prevention technologies and policies to prevent unauthorized data disclosure or leakage.

g. ensure regular data backup, implement secure backup storage and regularly test the restoration process as well as the security of stored data.

h. implement secure data disposal procedures, such as secure deletion or destruction methods (e.g., degaussing/demagnetizing), when data is no longer needed.

i. ensure compliance with relevant data protection and privacy regulations such as Nigeria Data Protection Act (NDPA) 2023 and any subsequent legislation, among others.

1.7. Remote Work Security

SFIs shall:

a. ensure that remote access to the network is through secure VPN connections or other encrypted remote access solutions. The use of unencrypted Remote Desktop Protocol for connection to corporate systems over the internet shall not be allowed.

b. require employees to use Multifactor Authentications (MFA) for authentication to the corporate network when accessing the bank's resources remotely.

c. ensure the use of secure collaboration and communication tools that offer end-to-end encryption, secure file sharing, and protected video conferencing capabilities.

d. provide security awareness for staff working remotely to ensure they observe security best practices.

1.8. Cloud Information Asset Management

SFIs shall:

a. understand the model of cloud service procured and the security requirements/responsibilities of the organization versus those of the CSP for each cloud service model and ensure that the security responsibilities of both parties are met. These should apply to Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a Service (IaaS) and any other cloud service utilised.

b. ensure uniform security policies are adopted in infrastructure in the cloud and on-premise.

1.9. Vulnerability Remediation and Patch Management

SFIs shall:

a. ensure that responsibilities and timelines for remediation of identified vulnerabilities are specified for different categories.

b. ensure that vulnerability remediation and patch application processes are regularly audited and reports presented to Senior Management.

c. scan patches for malware prior to application.

d. deploy security updates promptly after thorough testing and in accordance with its Patch Management Policy.

2. Monitor and Detect

2.1. Continuous Security Monitoring

SFIs shall:

a. establish a non-intrusive continuous (24x7) monitoring mechanism to collect, correlate, and detect anomalous user, administrator, system, and process/service activities on critical systems, databases, and networks in a timely manner.

b. implement monitoring and auditing mechanisms to detect and investigate suspicious activities that could indicate unauthorized access or data breach.

c. specify and document log retention period based on the criticality of data. The retention period should be approved by the Board.

d. monitor the physical environment of assets – server room, network devices, data centre, disaster recovery site, and off-site storage location.

e. ensure that security monitoring is done through a Security Operation Centre (SOC). The SOC can be in-house or outsourced and shall be resourced with skilled People, adequate processes and appropriate tools such as Security Information and Event Management (SIEM) solution for cyber monitoring.

f. periodically provide cyber-incident reports through the SOC to Board and Senior Management.

g. enable logging capabilities on all systems and applications on-premises and in third-party locations including cloud platforms to monitor and analyse activities within the systems to detect unusual activities or indicators of compromise.

h. deploy automated detection tools such as network and system (endpoint) scanners, Firewalls, Intrusion Detection/Intrusion Prevention systems (ID/IPS), etc. for effective early detection of cyber-incidents.

i. set up alerts and notifications for suspicious or unauthorized access attempts.

j. ensure logging and monitoring of remote access activities.

3. Respond and Remediate

SFI shall:

a. develop an incident response plan and playbooks to establish clear procedures for detecting, analysing and responding to security incidents on-premise or in cloud environments.

b. conduct tests such as Cyber Drills, Red-Team vs Blue-Team and Table-Top exercises regularly to ensure the effectiveness of the incident response plan. Outcome of tests should be used to update the plan/playbooks communicated to Senior Management.

c. ensure that Senior Management participate in tests to enhance their awareness and preparedness for making crucial decisions in the event of a cyber-attack.

d. establish a dedicated Incident Response (IR) team whose focus shall be on detection, analysis and response to cyber incidents.

e. ensure adequate and continuous training of the IR team on response to cyber-incidents.

f. ensure that generally accepted and appropriate forensic procedures, including chain of custody, are used to gather, analyse and report evidence in a manner that is legally admissible.

g. define how information should be communicated and shared with relevant stakeholders.

h. establish a Memorandum of Understanding or contractual agreement with incident response providers to assist rapidly with mitigation efforts.

i. implement robust backup and recovery mechanisms for critical data and perform backup restoration tests periodically.

4. Restore Service Operations

SFIs shall:

a. ensure implementation of recovery plan, processes and procedures to restore systems and assets affected by cybersecurity incidents.

b. ensure that incident response plan have clear specifications for moving to the recovery stage including verifying that all threats have been effectively addressed prior to restoring affected systems, data or access.

c. implement improvements based on lessons learned and review of existing strategies.

APPENDIX IV: Emerging Technologies

The minimum controls required in adopting emerging technologies shall include the identification of risks and opportunities, establishment of security controls, monitoring and reporting.

1. Risks and Opportunities Identification

Emerging technologies may have unknown vulnerabilities that can be exploited by malicious actors. It is crucial to identify and mitigate potential risks through robust security measures such as:

a. development of a strategy and policy on the adoption and use of emerging technologies.

b. development of a business case for the proposed adoption.

c. assessment of potential risks and controls considering their operating environment.

2. Security Controls Implementation

SFIs shall at a minimum establish the following controls:

a. conduct regular assessments (vulnerability assessments, penetration tests, etc) to identify and remediate any security flaws in the adopted emerging technology.

b. review and continually update security controls based on identified risks.

c. establish robust access controls including strong authentication systems (MFA, biometrics, etc.) and privileged account management.

d. encrypt sensitive data both in-transit and at rest and implement cryptographic controls using the appropriate industry-standard protocols.

e. establish data minimization practices to reduce the amount of sensitive data stored on edge devices.

f. establish data protection measures and comply with data privacy laws and regulations.

g. adhere to regulatory requirements and adopt industry best practices and cloud provider recommendations for secure configuration of cloud resources.

h. implement timely update and patches.

i. ensure adopted technology does not increase risk exposure of existing technology.

j. implement secure coding practices when developing and using APIs. Employ strong authentication and authorisation methods for API access, enforce usage limits, and regularly audit and monitor API activities.

k. establish appropriate security architecture design to ensure secure integration and prevent misconfigurations and weak points. Implement a layered security approach to create a more secure environment.

l. implement a comprehensive data backup strategy including regular backups and encryption of critical data stored in the cloud, ensuring backups are stored in a separate location from the primary cloud environment and testing of data restoration processes.

m. conduct due diligence when selecting third-party service providers.

n. evaluate the security practices, certifications, and records of accomplishment of third-party in maintaining the security of their services.

o. establish adequate SLAs with providers (cloud, Edge, API. etc.) that defines the service level expectations, resolution of identified issues and penalties for breach of agreement.

p. develop employees' capacity and awareness on the adopted emerging technologies.

q. develop a business continuity plan that integrates disruptions from emerging technology and third-party dependencies.

r. conduct regular security audits to ensure control measures are effective and up to date.

3. Monitor and Report

SFIs shall:

a. continually monitor and periodically report the impact of the adoption of emerging technologies on the cybersecurity posture to Management.

b. develop an incident response plan/mechanism that integrates emerging technologies and outlines steps to be taken in the event of a security incident or breach.

c. periodically review vendor security assessment to ensure that identified risks are promptly remediated.

d. establish a process for continuous monitoring and audit of new adoptions to detect and address security vulnerabilities and misconfigurations.

e. monitor and secure AI-enabled systems to prevent misuse or manipulation.

f. periodically monitor and report on regulatory and statutory compliance requirements on use of emerging technology.

g. ensure that the cloud service providers comply with relevant regulations and have appropriate security controls.

APPENDIX V: Informative References

ISO	Information Security Management Systems	https://www.iso.org/isoiec-27001-information-security.html
	Cybersecurity guideline	https://www.iso.org/standard/44375.html
NIST	Special Publications	https://www.nist.gov/publications/
	Resource Centre	https://beta.csrc.nist.gov/
PCI Security Standard Council	Document Library	https://www.pcisecuritystandards.org/document_library
COBIT 5	COBIT 5 for Information Security	https://isaca.org

APPENDIX VI: Cybersecurity Self-Assessment Tools

Below are a few risk assessment tools that can guide SFIs in achieving cyber resilience.

1. The FFIEC Cybersecurity Assessment Tool
   https://www.ffiec.gov/cyberassessmenttool.htm

2. US-CERT Cyber Resilience Review (CRR)
   https://www.us-cert.gov/ccubedvp/assessments

3. ICS-CERT‟s Cybersecurity Evaluation Tool (CSET)
   https://ics-cert.uscert.gov/sites/default/files/FactSheets/ICSCERT_FactSheet_CSET_S508C.pdf

4. Payment Card Industry (PCI) Data Security Standard Self-Assessment Questionnaire
   https://www.pcisecuritystandards.org/

5. ISO 27001 - https://www.iso.org

6. The CBN circulars relating to cybersecurity
   https://www.cbn.gov.ng/documents/

7. Nigerian Cybercrimes (Prohibition, Prevention etc.) Act, 2015

8. NgCERT website https://www.cert.gov.ng

Other suitable resources may also be adopted but caution should be exercised on open-source cyber-threat intelligence feeds due to high rate of false positive and/or false negative alerts.

APPENDIX VII: Reporting Templates

Central Bank of Nigeria

Risk-based Cybersecurity Self-Assessment Reporting
For
Deposit Money Banks (DMBs) and Payment Service Banks (PSBs)

Introduction

In accordance with Section 2.5 of the Central Bank of Nigerian Risk-based Cybersecurity Security Framework, Deposit Money Banks (DMBs) and Payment Service Banks (PSBs) are expected to conduct a cybersecurity self-assessment. This assessment shall identify all cybersecurity vulnerabilities, threats, likelihood of successful exploit, potential impact (reputational, financial, and regulatory) to information assets; and the associated risks. The self-assessment shall include but not limited to identifying the adequacy of cybersecurity governance, policies, procedures and standards; inherent risks in the institution's business operations; visibility to all emerging threats to information assets; capability to swiftly respond and recover from cyber-incidents; and determining the potency of existing controls to mitigate the identified risks.

In-view of this extant regulation, DMBs and PSBs shall conduct and report their Risk-based Cybersecurity Self-Assessment using the CBN Cybersecurity Self-assessment tool (CSAT), or any other tool as may be advised from time to time, annually but not later than March 31st. The CSAT shall be prepared by the Chief Information Security Officer, with inputs from other relevant functions, and shall also be endorsed by the CISO and Executive Management. The report shall be submitted to the Director, Banking Supervision Department, Central Bank of Nigeria.

Central Bank of Nigeria

Security Incident Reporting Template

For

Nigeria Deposit Money Banks and Payment Service Banks (PSBs)

Security incidents must be reported by DMBs and PSBs to the Director, Banking Supervision, Central Bank of Nigeria within 24 hours of the incident happening. Additional updates must be provided if the earlier reporting was incomplete, (i.e., new information due to investigation). Also, where required, additional documents should be provided and appended to this form.

New Incident ☐	**Update to Incident** ☐ *Incident reference no:*
CONTACT INFORMATION OF BUSINESS PROCESS OWNER	
DMB/PSB Name:	
Staff Name:	
Designation:	**Department:**
Phone No:	**Email:**
Additional Contact: _____	
INCIDENT DETAILS	
Date and Time Incident was Discovered/Detected:	
Date:	

Incident Type:

☐ Unauthorized Access ☐ Advanced Persistent Threat ☐ Phishing
☐ Denial of Service ☐ Unplanned Downtime ☐ System Failure
Ransomware ☐ Website Defacement ☐ Malicious Code
☐ Access or Credential Abuse ☐ Sustained Probe/Scan ☐ Others…Not a Cyber incidence
(Tick all that apply)

Incident Category

☐ State Sponsored ☐ Non-State ☐N/A

☐ Hackers ☐ Cyber criminals ☐ Insider / Collusion ☐Activist ☐ Others. Fire Incident

Incident Impact Description
(Please include details of how the incident was detected.)

Incident Impact Type *(Tick all that apply)*

☐ Outage of Critical IT System ☐ Theft or Loss of Customer Information
☐ Loss of sensitive Information ☐ Outage of Infrastructure
☐ D-DOS, ☐ Regulatory and Legal
☐ Others.

If other, please state:

Financial Loss

Financial Loss:

Recoveries:

Estimated Cost of Repair:

Incident Impact (Severity):

Impact	Impact Definition
High	Critical system(s), customer facing applications/systems, internal network or a combination is impacted. System downtime is experienced.
Moderate	Systems or network that can put the DMB/PSB's network, critical system(s) or a combination at risk is impacted. May lead to system downtime.
Low	Non-critical system(s) was impacted.

☐ High
☐ Moderate
☐ Low

Incident Impact (By Risk):

Impact Category	Low	Medium	High
Financial			
Reputation			
Functional/Operational			
Legal and Regulatory			

Does the affected critical system(s)/ network(s) have potential impact on another critical system/critical asset(s) of the DMB/PSB?
If "Yes", please provide more details:

Incident Notification

☐ Internal Management
☐ CBN
☐ Others: Fire Service
☐ Affected Customer
☐ Law enforcement (Police, EFCC, etc.)

INCIDENT ACTIONS

Incident Detection: (Date, Time and Details):

Affected System or Network: (Date, Time and Details):

PROVIDE THE ATTACKER'S IP ADDRESS: (If Applicable)

Containment Measures:

Evidence Collected (Systems Logs, etc.):

Eradication Measures:

Recovery Measures:

Other Mitigation Actions:

Lessons Learned:

Key Point of Vulnerability:

Glossary

2-Factor Authentication	This is a process in which a user provides two different authentication factors to verify his identity.
Acceptable Interruption Window	This is the maximum allowable time of interrupting mission critical systems or applications before restoration.
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.
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.
Application Programming Interface (API)	Set of rules and protocols that allows different software applications to communicate and interact with each other.
Automated Teller Machine	This is an intelligent electronic banking channel, which allows bank customers have access to basic banking services without the aid of any bank representative.
Bring Your Own Device (BYOD)	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.
Business Continuity/ Disaster Recovery Plan	These are planned processes that help institutions prepare for disruptive events and recover within a short period.
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"
Cloud Service Providers	Third parties that offer cloud computing services, providing institutions with access to computing resources, storage, databases, and applications over the internet.
Cyber Drill	This is a simulated cyberattack exercise conducted by institutions to test and assess their cybersecurity incident response capabilities.
Cyber risk insurance	A specialized insurance policy that provides financial protection to institutions against losses resulting from cyber incidents.
Cyberspace	This is an imaginary environment where communication over computer networks occurs
Degaussing	A process of permanently erasing data stored on magnetic media, such as hard drives and magnetic tapes, by exposing them to a strong magnetic field.
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 Negative	False negative occurs when a security device omits a vulnerability
False Positive	A false positive is a false alarm generated by a device, process or entity; usually based on preconfigured rules or logic.
Financial Services Information Sharing and Analysis Centre	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.

Financial Services Information Sharing and Analysis Centre (FS-ISAC)	This is a global nonprofit organization dedicated to enhancing cybersecurity and resiliency in the financial sector.
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.
Internal Capital Adequacy Assessment Process (ICAAP).	This is a comprehensive risk assessment framework used to evaluate capital adequacy based on internal risk profiles and potential losses.
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."
Internet	An internet is an interconnected computer networks linked by the internet protocol suite.
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 Detection System	A device or software/application that monitors an institution's network or systems for policy violations and/or malicious activities.
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 system-generated 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.
Multifactor authentication	A security measure that requires more than one distinct authentication factor to confirm the identity of a user, process, or device in order to gain access to a system.
Nested Payment Service Provider	Any entity that is contracted for its services by another payment service provider for the purposes of providing a service.
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 Electronic Fraud Forum (NeFF)	This is a collaborative platform within the Nigerian financial industry focused on combating electronic fraud and cybercrime.
Non-Disclosure Agreement	A legal contract or agreement between two or more parties that outlines a degree of confidentiality.
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.
Open-source cyber-threat intelligence	A platform, blog, database that collects, stores and share information on emerging cyber threats, indicators and trends to its subscribers.
Open-Source Intelligence (OSINT)	Open-Source Intelligence (OSINT) refers to information collected from publicly available sources, such as websites, social media platforms, and public records.

Payment Card Industry Data Security Standard	This is an information security standard for DMB/PSPs that collect, process, store and transmit cardholder data.
Point of Sale terminal	This is a device that accepts payment cards for electronic funds transfers.
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.
Secure Coding	A principle of writing software code that adheres to code security best practices. It involves using coding techniques and best practices to minimize vulnerabilities and prevent potential cyber-attacks.
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.
Shareholders' Fund	Shareholders' Funds represent the equity held by shareholders in a company, including common and preferred stock
Single points of failure	These are components or elements within a system or network that, if they fail, can cause the entire system to fail.
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 DMB/PSP
Vulnerability	This is a weakness or gap in a system, application, process, device, etc.
Zero-Trust	Security model that requires all users and devices to be continuously authenticated, authorized, and verified before accessing resources or data.