BSD/DIR/GEN/LAB/11/25

October 10, 2018

LETTER TO ALL BANKS AND PAYMENT SERVICE PROVIDERS

ISSUANCE OF RISK-BASED CYBERSECURITY FRAMEWORK AND GUIDELINES FOR DEPOSIT MONEY BANKS AND PAYMENT SERVICE PROVIDERS

The CBN hereby issues the attached Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks (DMBs) and Payment Service Providers (PSPs), which represents the minimum requirements to be put in place by all DMBs in their respective cybersecurity programmes.

The effective date for full compliance with the provisions of the guidelines is **January 1, 2019** and all DMBs and PSPs are expected to do so, on or before that date.

Please, be guided accordingly.

Yours faithfully,

AHMAD ABDULLAHI

DIRECTOR, BANKING SUPERVISION

RISK-BASED CYBERSECURITY FRAMEWORK AND GUIDELINES

FOR

DEPOSIT MONEY BANKS AND PAYMENT SERVICE PROVIDERS

OCTOBER 2018

Table of Contents

1. Introduction

The safety and soundness of Deposit Money Banks (DMBs) and Payment Service Providers (PSPs) 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 reputation risk, amongst others.

In recent times, cybersecurity threats have increased in number and sophistication as DMBs and PSPs, use information technology to expedite the flow of funds among entities. In this regard, threats such as ransomware, targeted phishing attacks and Advanced Persistent Threats (APT), have become prevalent; demanding that DMBs and PSPs remain resilient and take proactive steps to secure their critical information assets including customer information that are accessible from the cyberspace.

It is in this regard that this framework, which outlines the minimum cybersecurity baseline to be put in place by DMBs and PSPs, is being issued. The framework is designed to provide guidance for DMBs and PSPs in the implementation of their cybersecurity programmes towards enhancing their resilience.

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

DMBs/PSPs 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 five parts: Cybersecurity Governance and Oversight, Cybersecurity Risk Management System, Cybersecurity Operational Resilience, Metrics, Monitoring & Reporting and Compliance with Statutory and Regulatory Requirements.

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 DMBs and PSPs. It spells out the responsibilities of the Board of Directors, Senior Management and Chief Information Security Officer (CISO). This entails the development and enforcement of policies, procedures and other forms of guidance that the DMBs/PSPs 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 DMB/PSP. In this regard, the Board shall ensure that cybersecurity is completely integrated with business functions and well managed across the DMB/PSP.

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** are detailed below:

2.4.1. The Board of Directors through its Committees shall have oversight and overall responsibility for the DMB/PSP's cybersecurity programme. It shall provide leadership and direction for effective conduct of the processes. The Board shall ensure that cybersecurity governance is integrated into the organisational structure and relevant processes.

2.4.2. The Board shall 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 DMB/PSP. Furthermore, the Board shall hold Senior Management responsible for central oversight, assignment of

responsibility, effectiveness of the cybersecurity processes and shall ensure that the audit function is independent, effective and comprehensive.

2.4.3. The Board shall be responsible for all cybersecurity governance documents such as cybersecurity strategy, framework and policies and ensure alignment with the overall business goals and objectives.

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

2.4.5. The Board of every DMB/PSP shall 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 banking groups, such institution may leverage on its group CISO where the bank is part of a group that has a CISO.

2.4.6. The board shall ensure that the cybersecurity budget is approved.

2.5. The **responsibilities of Senior Management** are detailed below:

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

2.5.2. Senior Management shall provide periodic reports (at a minimum quarterly); to the Board on the overall status of the cybersecurity programme of the DMB/PSP.

2.6. The **responsibilities of the Chief Information Security Officer (CISO)** are detailed below:

2.6.1. The CISO shall be responsible for the day-to-day cybersecurity activities and the mitigation of cybersecurity risks in the DMB/PSP.

2.6.2. The CISO shall focus on the DMB/PSP-wide cybersecurity risk rather than IT security risk only, and shall also be responsible for the development and implementation of the cybersecurity programme and strategy as approved by the Board.

2.6.3. A group CISO shall be responsible for establishing and maintaining an enterprise vision, strategy and program in the case of banking group where critical information security expertise and tools are maintained and controlled centrally.

2.7. The **requirements of the Chief Information Security Officer (CISO)** are detailed below:

2.7.1. The CISO shall be of senior management grade and shall possess adequate authority; experience; independence and status within the DMB/PSP to enable him/her function properly.

2.7.2. The CISO shall not report to the Head of Information Technology (IT) operations to avoid conflict of interest while ensuring segregation of duty. He/She shall report to the Managing Director/Chief Executive Officer.

2.7.3. The CISO shall meet educational and experience requirements as provided in the Fit and Proper (Approved Persons) Framework required for Assistant General Managers and above for DMBs and shall be at least senior manager for PSPs. Given the requirements of this job role, experience gained solely in the field of IT shall be deemed to be adequate.

2.7.4. In addition, the CISO shall possess relevant qualifications and in-depth experience in Information Technology with any, or combination of, Information Security Certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Certified Chief Information Security Officer (CCISO).

2.8. The **Information Security Steering Committee (ISSC)**:

2.8.1. Every DMB/PSP shall establish an information security steering committee that shall be responsible for the governance of the cybersecurity programme.

2.8.2. The steering committee shall consist of senior representatives of relevant departments within the DMB/PSP and shall be headed by the CISO.

2.8.3. The roles, responsibilities, scope and activities of the information security steering committee shall be clearly defined.

2.8.4. The **objectives of the Committee** shall include:

2.8.4.1. Ensuring that DMB/PSP's security policies and processes align with the business objectives;

2.8.4.2. Evaluating, approving, and sponsoring institution-wide security investment;

2.8.4.3. Enforcing the implementation of policies for investment prioritization and security risk management; and

2.8.4.4. Providing strategic direction and cybersecurity governance for the DMB/PSP.

2.9. **Risk Management Control Functions**

To ensure the effectiveness of a DMB/PSP's cybersecurity governance, its processes and controls shall be reviewed at least annually. In this regard, the risk management control functions; handled by relevant department of the organization shall have their responsibility as follows:

2.9.1. **Risk Management**

Risk Management shall independently evaluate all the risks relating to cybersecurity in a proactive way. This should include the use of appropriate tools and methodologies for risk

identification, analysis and control. Appropriate reports shall be provided to Senior Management and the Board Risk Management Committee, quarterly.

2.9.2. **Compliance**

The Compliance Department of DMBs and PSPs shall review their cybersecurity programmes and processes to ensure adherence to relevant CBN directives and other extant regulations.

2.9.3. **Internal Audit**

A DMB/PSP's cybersecurity programme shall be audited by the Internal Audit unit to determine the effectiveness of the controls put in place and ascertain if they are adequate for the DMB/PSP's risk exposure. Internal audit shall be independent with the scope of cybersecurity audits clearly defined. Audit programmes shall be risk-based and provide assurance to the Board and Senior Management on the effectiveness of the cybersecurity programme.

2.10. Cybersecurity Strategy and Framework

2.10.1. The Board of Directors shall approve the DMB/PSP's information/cybersecurity strategy, which shall provide direction on how to achieve its cybersecurity goals. The strategy shall address and mitigate cyber-risk while providing compliance with the legal, contractual, statutory and regulatory requirements. The strategy shall align with the DMB/PSP's Information Security Management System (ISMS), information technology and the overall corporate strategy.

2.10.2. A DMB/PSP shall also put in place an information/cybersecurity framework in support of its strategy which aligns policies, business and technological approaches to address cyber risks and clearly defines all cybersecurity roles and responsibilities.

2.10.3. In addition, a DMB/PSP shall develop an information/cybersecurity policy either as a separate document or as part of its cybersecurity framework or its Information Security Management System (ISMS). The policy shall clearly convey management intent and the DMB/PSP's approach to achieving its cybersecurity objectives.

2.10.4. The policy document(s) approved by the Board shall be continuously reviewed and updated annually at a minimum or when there are significant changes to the DMB/PSP's cyber-risk exposure and in the light of emerging technologies. The annual review shall ensure its suitability, adequacy and effectiveness to mitigate cyber-risk.

3. Cybersecurity Risk Management System

3.1. Effective Risk Management serves to reduce the incidence of significant adverse impact on an organization by addressing threats, mitigating exposure, and reducing vulnerability. DMBs and PSPs shall incorporate cyber-risk management with their institution-wide risk management framework and governance requirements to ensure consistent management of risk across the institution.

3.2. The Risk Management programme shall be based on an understanding of threats, vulnerabilities, risk profile and level of risk tolerance of the organisation. The process shall also be dynamic in view of the constantly changing risk landscape. The Board and Senior Management shall support and be involved in the cyber-risk management process by ensuring that resources and capabilities are available and roles of staff properly defined in management of risks.

3.3. The Risk Management System shall cover the four basic activities below:

3.3.1. Risk assessment

3.3.2. Risk measurement

3.3.3. Risk mitigation/Risk treatment

3.3.4. Risk monitoring and reporting

3.4. Cyber risk assessments should be updated regularly to address changes or introduction of new technologies, products etc. before deployment to ensure accurate risk measurement.

3.5. Risk treatment options such as risk reduction, risk retention, risk avoidance, risk transfer and how residual risk is addressed should be selected based on the outcome of the risk assessment.

3.6. Information obtained from risk management activities shall be reported to the Senior Management and the Board of Directors to support informed decision making.

3.7. A DMB/PSP shall ensure consistent conduct of risk assessments, vulnerability assessments and threat analysis to detect and evaluate risk to the DMB/PSP's information assets and determine the appropriateness of security controls in managing risk.

3.8. IT risk shall be responsible for assessment, measurement and monitoring/reporting of risks associated with critical IT infrastructure while information/cybersecurity team shall be responsible for risk mitigation/treatment.

3.9. **Cybersecurity Resilience Assessment**

Cybersecurity Resilience Assessment is useful in evaluating an organization's defense posture and readiness to cybersecurity risks. In view of rapid advancement in IT, interconnection between networks (internet) and multiple threats in the cyberspace, a DMB/PSP shall carry out cyber risk resilience assessment to determine its current and target cybersecurity profile.

3.9.1. **Determining the Current Cybersecurity Profile ("present state")**

3.9.1.1. DMBs and PSPs shall determine their "current" cybersecurity position at regular intervals by evaluating all identifiable cybersecurity vulnerabilities; threats and likelihood of successful exploit; potential impact (reputational, financial,

regulatory, etc.); and the associated risks in order to estimate the amount of assets and efforts required to recover from losses/damage attributable to potential cyber incidents.

3.9.1.2. The assessment should include but not limited to adequacy of cybersecurity governance; policies, procedures and standards; inherent risks in business operations; visibility to emerging threats to information assets; capability to swiftly respond and recover from cyber-incidents; vendor risk, and efficacy of existing controls to mitigate the identified risks.

3.9.1.3. In addition to various cybersecurity assessments conducted to identify vulnerabilities, other frameworks/tools available to assist in achieving this objective at no cost are contained in Appendix II. All gaps identified shall be documented and communicated to the Executive Management and Board of Directors.

3.9.2. **Establishing a Target Cybersecurity Profile ("desired state")**

A DMB/PSP shall develop a detailed roadmap to timely address the gaps identified. This document shall state the vulnerability/risk treatment plan with stipulated time frame. The plan may include updating the cybersecurity policy; establishing a security operation center and cyber forensic laboratory; signing-up with external cyber threat intelligence agencies, etc.

3.9.3. **Reporting Cybersecurity Self-Assessment**

A report of the self-assessment which shall depict the procedure/tools/framework used to conduct the cybersecurity self-assessment; identified gaps, threats, and risks; potential value at risk/impact; prioritized action plan to mitigate risks identified; and timeline for remediation; remediation status with possible residual vulnerabilities/risks shall be submitted by DMBs and PSPs to the Director, Banking Supervision Department of the Central Bank of Nigeria annually not later than March 31st . The report shall be signed and submitted by the

Chief Information Security Officer after its endorsement by the Executive Management. See the reporting template in Appendix VII.

4. Cybersecurity Operational Resilience

DMBs and PSPs are required to build, enhance, and maintain their cybersecurity operational resilience which will ultimately contribute to reducing cybercrime in Nigeria and strengthen the banking sector cyber defense.

The following are the minimum controls that a DMB/PSP shall put in place on their critical IT infrastructure to ensure the Confidentiality, Integrity and Availability (CIA) of information assets among others.

4.1. **Know Your Environment**

A DMB/PSP shall endeavor to be acquainted with its business environment and critical assets. It shall devise mechanisms to maintain an up-to-date inventory of authorized software, hardware (workstation, servers, network devices etc.), other network devices, and internal and external network connections. All unauthorized software and hardware device on its network shall also be identified, documented, removed and reported appropriately.

Employees and contractors providing information technology and cybersecurity functions/services shall also be identified. Details on how to improve DMB/PSP's IT infrastructure awareness is contained in Appendix III.

4.2. **Enhancing Cybersecurity Resilience**

A DMB/PSP shall continuously improve on its cybersecurity resilience. This is crucial for the prompt identification of system vulnerabilities; emerging threats and their associated risks; rapid cyber-incident response; increasing cybersecurity maturity level; ensuring the

confidentiality, integrity and availability of information assets whilst promoting a safe and sound banking system in Nigeria.

Leveraging on the DMB/PSPs' resilient cybersecurity governance, risk management and compliance, a DMB/PSP shall adopt the measures in Appendix IV and V as the minimum cybersecurity baselines to enhance its cybersecurity resilience.

4.3. **Cyber-Threat Intelligence**

A DMB/PSP is required to possess an objective knowledge – based on fact – of all emerging threats, cyber-attacks, attack vector, mechanisms and indicators of attack/compromise to its information assets which shall be used to make informed decisions.

To this end, DMBs and PSPs are required to:

4.3.1. Establish a Cyber-Threat Intelligence (CTI) programme which shall proactively identify, detect and mitigate potential cyber-threats and risks.

4.3.2. Establish a CTI policy (as part of the cybersecurity policy) approved by the Board of Directors to aid proactive identification of emerging cyber threat, trends, patterns, risks, and possible impact.

4.3.3. Identify and document various CTI Sources. See Appendix VI for details.

4.3.4. Take informed decisions based on the CTI programme as it provides valuable information on areas susceptible to cyber-attacks, latest threats, attack vector, etc. Decisions may include: reviewing the Bring Your Own Device (BYOD) policy; conducting emergency awareness training, vulnerability assessment, and penetration testing; review of vendor source codes, cyber-incident response plan, BCP/DR plans, vendor SLA; and increased system logging, etc.

4.3.5. Promptly report all impending and challenging cyber-threats to their information assets to the Director of Banking Supervision of Central Bank of Nigeria using the

Cyber-threat Intelligence Reporting template in Appendix VII after its endorsement by appropriate authorities.

5. Metrics, Monitoring & Reporting

5.1. A DMB/PSP shall put in place metrics and monitoring processes to ensure compliance, provide feedback on the effectiveness of control and provide the basis for appropriate management decisions. The metrics should be properly aligned with strategic objectives and provide the information needed for effective decisions at the strategic, management and operational levels.

5.2. The metrics should assess the effectiveness of the DMB/PSP's overall cybersecurity programme and measure its performance and efficiency. Tools may be employed to achieve this include key risk indicators, key goal indicators, etc.

5.3. The Board and Senior Management of DMB/PSP shall establish an effective and reliable reporting and communication channels throughout the institution to ensure the effectiveness and efficiency of the cybersecurity programme. The cybersecurity programme reporting process shall be consistent, timely, comprehensive, transparent and reliable. The measurement process should help to identify shortcomings and failures of security activities and provide feedback on progress made in resolving issues.

5.4. A reporting process that defines reporting and communication channels shall be established for the dissemination of security-related material such as changes in policies, standards, procedures, new or emerging threats and vulnerabilities.

5.5. The Board of Directors and Senior Management shall be provided with quarterly reports to keep them abreast of the state of the cyber/information security programme and governance issues in the DMB/PSP.

5.6. A DMB/PSP is required to report all cyber-incidents (as defined in Appendix I) whether successful or unsuccessful 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. Where necessary and applicable, additional information should be provided afterwards.

6. Compliance with Statutory and Regulatory Requirements

6.1. The Board and Senior Management of DMBs and PSPs shall ensure compliance with all relevant statutes and regulations such as the Nigerian Cybercrimes (Prohibition, Prevention etc.) Act, 2015 and all CBN directives to avoid breaches of legal, statutory, regulatory obligations related to cybersecurity and of any security requirements.

6.2. The Central Bank of Nigeria shall ensure the establishment of appropriate processes and procedures for the purpose of monitoring compliance with this framework and other extant laws and regulations.

6.3. Non-compliance with the provisions of this framework shall attract appropriate sanctions as may be determined by the Central Bank of Nigeria in accordance with the provisions of the CBN Act and BOFIA.

7. Compliance

The CBN shall monitor and enforce compliance with the provisions of the Guidelines.

8. Effective Date

This Guideline shall take effect from January 1, 2019

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 results in a significant financial loss and negatively impact business operation and service to customers.

A Cyber-Incident is referred to as any incident which may result in a significant financial loss as a result of:

I. Unplanned outage of IT system(s) such as Core Banking Application, Treasury Systems, Trade finance systems, core network devices, Internet banking systems, electronic channels (e.g. ATMs, POS, USSD, Mobile banking, etc.) and connected payment systems e.g. SWIFT, RTGS, NEFT, etc.)

II. Cyber security incident such Distributed Denial of Service (DDOS), Ransomware/cryptoware, data breach, data destruction, web defacement, etc.

III. Unauthorised access, disclosure, tampering or theft of banks and customers' information (personal Identifiable Information and financial data).

A significant financial loss is a loss that exceeds 0.01% of shareholders' funds unimpaired by losses.

Appendix II: Cybersecurity Self-Assessment Tools

Below are few risk assessment tools that can guide DMBs/PSPs in achieving cyber resilience. Other suitable resources may also be adopted.

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.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_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/

Appendix III: Know Your Environment:

1. Asset Management

Hardware: A DMB/PSP shall:

1.1 Maintain an up-to-date inventory of all authorized devices used to process, store or transmit data/information in the institution such as workstations, laptops, switches, routers, firewall, printers, scanner, photocopiers, IP Phones, surveillance cameras, etc. connected to its network. Unauthorized devices shall not be granted access to the network.

1.2 Ensure that all identified devices are categorized not only by the criticality and sensitivity of the data/information they store, process or transmit but also on their mobility.

1.3 Assess and review the profile(s) of personnel(s) and/or third parties who have unrestricted/restricted access to devices identified in "1.1" above.

1.4 Automate the detection of unauthorized devices as they connect to the DMB/PSP's network and ensure that only authorized devices are granted access to the network.

Software: A DMB/PSP shall:

1.5 Devise a mechanism to maintain an up-to-date inventory of all applications/software installed and/or running on all its systems. Unauthorized software/applications identified shall be removed.

1.6 Ensure that the installation of applications/software including patches and hotfixes to authorized workstations/laptops, servers (including those on the demilitarized zone or DMZ), and mobile devices are centrally coordinated and managed.

1.7 Ensure that all legacy but still-in-use software and applications are catalogued. Vulnerabilities associated with them shall be promptly identified and remediated with adequate controls and must be considered for upgrade.

1.8 Establish controls to prevent unauthorized modification or removal of its authorized software/applications while preventing the installation of unauthorized software/applications on its network.

ATM and POSs: A DMB/PSP shall:

1.9 Devise a mechanism to maintain an up-to-date inventory of all ATM and POS machines connected to its network.

1.10 Establish controls to protect all ATM and POS devices against malware, tampering, memory scrapping, and spoofing.

1.11 All POS merchants must be appropriately risk profiled at least annually.

1.12 Ensure that risks associated with these devices are regularly assessed, documented and mitigated promptly.

Network: A DMBs and PSPs shall:

1.13 Maintain an approved up-to-date network topology of their wired and wireless networks irrespective of their location;

1.14 Maintain a catalog of all dedicated/frequently-used network connection(s) to regulatory authorities, switches, vendors/contractors, and wholesale customers with details of the objectives of such connections;

1.15 Implement Authentication, Authorization and Accounting (AAA) policies on network devices;

1.16 Implement secure network management and prompt reporting;

1.17 Devise mechanism to mitigate layer 2 and 3 attacks using Firewall, Access Control Lists (ACLs), etc. and

1.18 Ensure that the Internal Operating System (IOS) software of network devices such as routers are up-to-date.

Protocols: A DMB/PSP shall ensure that

1.19 Protocols used by programmers during application development and those used by endpoint and network devices for data transfer and topology advertisement are secure while meeting functional requirements.

1.20 Vulnerabilities associated with these protocols are regularly assessed and mitigated appropriately. This include but not limited to those used by cellular phones (via mobile network) to communicate with DMB/PSP's IT infrastructure e.g. USSD, SMS, etc.

2. **Staff/Employee:**

The Management of a DMB/PSP shall:

2.1 Identify all employees whose job description is to implement, enforce, and review its physical and technical security controls; this includes but not limited to IT system, IT security administrators, security guards, etc.

2.2 Conduct background check on employees who implement policies, procedures used to protect sensitive information, and plausibly know ways of circumventing those control e.g. IT system administrators and security guards.

2.3 Ensure that risks associated with this category of employee are regularly assessed as part of the enterprise risk assessment framework. Background check shall be periodically conducted to gather reliable information about such employees.

2.4 Ensure that mandatory vacation/leave is adopted to thwart opportunities for fraudulent activities, and key-man risk.

2.5 Ensure that access rights assigned to all users is based on the principles of separation of duties and least privilege.

3. Vendor/Contractors/Third-parties: A DMB/PSP shall:

3.1 Maintain an up-to-date inventory of services rendered by vendor/contractor/third-parties with valid Service Level Agreement (SLA).

3.2 Ensure that each SLA contains at minimum: details of service rendered, Non-Disclosure Agreement (NDA), Roles and Responsibilities of each party, Duration, Vendor Service Level Manager, Service Quality metric/evaluation criteria, and the Right to Audit clause.

3.3 Audit their vendors/contractors/third-parties in order to ensure/enforce compliance with the SLA; and promptly identify risky parties; if possible, visit their office/ IT processing facility

3.4 Assess the qualification, skills and/or experience of vendor staff assigned to them by their vendors/contractors/third-parties.

4. External Connection: A DMB/PSP shall:

4.1 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.

4.2 Assess, document, and mitigate all risks associated with the identified external connections appropriately.

4.3 Where applicable, visit the data center and network infrastructure facilities of third-parties; access their approved cybersecurity policies and ensure it addresses all cybersecurity concerns.

4.4 Ensure that third-party accesses are restricted to only authorized segment of the network; only specific IP addresses from the third-party shall be allowed, and restrict connection(s) to a period of time (where applicable).

4.5 Always log, monitor, and review all third-party connections to their network.

5 **Payment Service Providers:** Where a DMB/PSP (in a nested PSP relationship) engage a Payment Service Providers (entity); third-party for the storage, transmission, processing and security of cardholder data, the DMB/PSP shall:

5.1 Identify, review and document the services provided by the entity.

5.2 Determine and document the scope of the entities involvement in storing, processing, or transmission of cardholder data and the effect on the security of the Cardholder Data Environment.

5.3 Identify and document the technology used by the entity for the services provided.

5.4 Identify and document whether an additional third-party is used by the entity to deliver the services rendered.

5.5 Identify the facilities of the entity where cardholder data/information is located.

5.6 Obtain the following documentation from the entity to validate PCI DSS compliance for the service rendered: Report on Compliance (ROC); Attestation of Compliance (AOC); Self-Assessment Questionnaire (SAQ); and ASV Scan Report Attestation of Scan Compliance (AOSC).

Appendix IV: Enhancing Cybersecurity Resilience

This section provides the minimum controls required for a DMB/PSP to continue to support and provide business services even in the event of cyber –attacks. It provides controls on access right management, secure system configuration, cybersecurity awareness , data loss prevention, system life cycle management, vulnerability management, continuous security monitoring, and enhancing incident response capabilities.

1. **Access Control:**

   A DMB/PSP shall establish an access control policy which ensures that:

   a. There exists mechanism, standards and procedures that govern users, systems and service accounts access provisioning, identification, and authorization to all systems, network, and applications.
   b. All workstations/laptops, end-users, service accounts, network devices (internal and external), and administrators have identities and credentials to access the bank's resources.
   c. Access to its information assets (including customer information), resources and connected services/facilities at any time are limited to only authorize users, services, processes or devices (including wireless network) based on the principle of least privilege and guided by an access control matrix.
   d. Authorizations given to users, service and system accounts are limited to the functions/ services they provide; where necessary implement logon time and days restriction.
   e. Physical access to assets is controlled based on the criticality and sensitivity of the information processed, stored and transmitted by them.
   f. The repositories of all users, administrator, and system identities and credentials are protected.

2. **Secure System Configuration Management:** To enhance resilience through system configuration, a DMB/PSP shall:

    a. Acquire and deploy systems/applications with in-built resilience configuration.

    b. Develop minimum security baseline configuration such as anti-malware; data loss prevention solutions; and systems security settings for workstations/laptops, servers, applications/software including network devices governed by vendor recommendations, informative references in Appendix V and the CBN guidelines.

    c. Devise mechanisms to logically apply and maintain their cybersecurity policies and security baseline configuration on systems, applications and network devices.

    d. Establish a Standard Operating Procedures (SOP) for all IT processes and activities.

    e. Audit the security configurations items on system and network devices to ensure compliance with preconfigured security settings.

    f. Devise a mechanism to monitor, detect, log and report all unauthorized system configuration changes; where possible, the mechanism shall re-apply the security configuration seamlessly.

3. **Cybersecurity Awareness Training:**

Educating employees, contractors and customers on cybersecurity is imperative for a secure cyberspace. To this end, a DMB/PSP shall:

    a. Develop cybersecurity awareness training contents, taking cognizance of the prevailing cyber threats, cyber risk, and various attack-vectors.

    b. Ensure that the content of the cybersecurity awareness training include information contained in the DMBs and PSPs' cyber security policy, roles and responsibilities of

all parties, and emerging cyber –threats.

c. Mandate all Board members and employees to participate the training programme.

d. Ensure that third-party/vendor also undergo the bank's security awareness programme as well.

e. Devise mechanisms to communicate cybersecurity awareness messages to all their customers in the language they understand irrespective of their location. To thwart social engineering attack among others, the messages shall be communicated in English and customers' understandable Nigerian local languages at least monthly or when there is an identified cyber-threat/attack vector via SMS, emails, radio, newspapers, etc.

4. **Data Loss Prevention:**

Protecting and controlling the accessibility and usage of customers Personal Identifiable Information (PII) and bank's sensitive and critical information within and outside the corporate network is a major goal of cybersecurity resilience. Hence,

a. A DMB/PSP shall develop a data loss/leakage prevention strategy to discover, monitor, and protect sensitive and confidential business and customer data/information at endpoints, storage, network, and other digital stores, whether online or offline.

b. The strategy should provide but not limited to a mechanism that:

i. classifies both structured and unstructured data/information;

ii. discovers where sensitive/confidential data/information are stored;

iii. monitors how sensitive/confidential data/information are being used;

iv. continuously protects data whether the endpoint is on/off the corporate network;

v. addresses notable data loss concerns through USB, e-mail, mobile phones and web;

vi. takes prompt actions when a potential data breach is suspected or detected: e.g. blocking an employee's attempt to save a sensitive information to an external storage or network share drive; and

vii. establishes to management a reduction in data loss risk in institution.

c. Critical and sensitive information on assets shall be formally managed throughout removal, transfers, and disposition. All assets identified for disposal shall undergo degaussing, and/or total destruction; in accordance with its approved policy.

d. A DMB/PSP shall validate that similar control exist at vendor managed facilities such as co-location data centers, and cloud service providers.

5. **System Life Cycle Management:**

In managing the life cycle of systems, a DMB/PSP shall:

a. Establish policies and procedures that consistently oversee the lifecycle (identification, acquisition/development, maintenance/update, and disposal) of applications, components, and systems.

b. Ensure that cybersecurity control are considered and incorporated in all stages of the system/application lifecycle. The business requirement for the acquisition/development of systems/applications shall also identify and document the security requirements. This includes but not limited to access control, access right management, authentication, event logging, audit trail, user session management,

separation of duties, and least privilege, etc.

c. Validate that the systems/applications meet all other requirements (functional, performance, reliability, etc.) and any applicable CBN regulations before they are deployed.

d. Ensure that all in-house applications are developed in-line with secure coding practices such as threat modeling, input validation, least privilege, defense in-depth, and fail secure whilst mitigating against OWASP vulnerabilities. These applications shall also be thoroughly tested by a team of qualified software testers and business/application owners.

e. Separate the production/live environment from the development and testing environment(s).

f. Sanitize sensitive data in the development and testing environments by implementing a Data Masking solution to mask/fabricate bank's and customers' sensitive information for the purpose of development, System and User Acceptance Tests.

g. Establish a procedure for the maintenance of on-site and remote organizational assets to prevent unauthorized access.

h. Adopt cryptographic controls such as public key infrastructure, hashing and encryption to guard confidential and sensitive information against unauthorized access.

i. Comply with the extant rules and regulations of your card schemes and associated stakeholder rules.

6. **Vulnerability Management**:

IT vulnerability management is an integral part risk management. To this end, a DMB/PSP shall

promptly identify weaknesses in their IT infrastructure (database, applications, network etc.), account profiles (system administrators and privileged users), vendors, etc.

a. ***Information Assets:***

To promptly identify all system vulnerabilities and cybersecurity risks to operations and IT assets, a DMB/PSP shall:

i. Implement a vulnerability management policy; approved by Executive Management

ii. Establish an automated mechanism to detect all vulnerabilities in its assets. This includes but not limited to workstations, network devices, servers (production, test and development), etc. The vulnerabilities and threats shall be documented; potential business impact and likelihood shall also be identified.

iii. Conduct vulnerability assessment at least quarterly or when there is a significant change (such as installation of new systems, devices, applications, etc.) to the bank's information processing infrastructure or when vulnerabilities are made known.

iv. Further identify vulnerabilities in their assets by engaging professionals in this field to conduct Penetration Tests (PT) annually. However, PT shall be conducted frequently on internet-facing systems/applications.

v. Continuously identify the inherent risks and vulnerabilities associated with IT platform/protocols used for business services e.g. USSD and SMS mobile Banking protocols.

vi. Promptly categorize and resolve issues identified during vulnerability assessment based on their criticality, likelihood and impact. Subsequent validation to assess closure of such vulnerabilities shall also be done. The root cause of the identified vulnerabilities such as a flaw in security policy, system misconfiguration, inconsistent Standard Operating Procedure (SOP), non-

compliance to change management processes, and superficial risk assessment shall also be addressed to thwart future occurrence.

vii. Have a dedicated team that monitors the release of security patches/updates by their vendors / OEMs. Security updates are mandatory, and shall be deployed quickly in accordance with DMBs and PSPs' patch management policy. Patches for well-known or zero day vulnerabilities shall also be applied swiftly in accordance with its emergency patch management process.

viii. Establish an efficient mechanism and processes to identify assets patch compliance status - on operating system and application software on users' laptops and desktop, servers (including those on the DMZ), virtual machines, etc. - and remedy patch deficiencies.

b. ***System Administrators And Privileged Accounts:***

To limit exposure to insider threat, a DMB/PSP shall:

i. Identify all employees and system/service accounts with super-privileges on each system, application, database, and device; and enforce segregation of duties and principle of least privilege for these accounts.

ii. Where applicable, enforce password and account-management policies and practices to these accounts as-well. Use of shared default/anonymous privileged account by multiple users is highly prohibited.

iii. Ensure that no single administrator have unfettered access to its critical systems. Logon credentials to critical systems, applications, and network shall be created and separately documented by at least 2 different employees.

iv. Change the logon credentials of default system accounts on assets before they are connected to the network. This shall apply to test and development servers as well.

v. Establish a strategy, mechanism and an intelligent procedure to log, monitor, and audit actions performed by these accounts. All logs/audit trails shall be

preserved and regularly reviewed in accordance with each institution's account management policy.

c. ***Vendors***:

A DMB/PSP shall ensure that:

i. No vendor has unfettered access to its systems, database, network and applications (especially the core application).

ii. If a vendor needs to access its information asset, management approval shall be sought only for the duration the access is required. Such access shall be administered by an authorized administrator.

iii. No vendor given logged-on to its information assets shall be left unattended to. Their actions shall be logged and closely monitored at all time. If possible, conduct a background check on all vendor staff before they are granted access.

7. **Continuous Security Monitoring:**

There shall be an ongoing awareness of information security vulnerabilities and threats to support s DMB/PSPs risk management decisions. To improve surveillance, it shall:

a. Determine what needs to be monitored by: gathering information about all systems, databases, and network that support business activities; analyze reports about cyber-incidents that have occurred in the past; evaluate the recommendations from both recent internal and third-party audits/ risk assessment of the network; and report of its cybersecurity self-evaluation.

b. Identify the key dependent variables – people, system, database, network and services – that the technical components of the continuous monitoring strategy will depend on.

c. Determine appropriate performance metrics for those variables; this includes but not limited to skills, system availability, event logging capability of systems to be

monitored etc.

d. Establish how the log data collected from various sources will be stored and secured.

e. Define a continuous security monitoring policy/strategy; it shall include but not limited to the identified systems and processes, key dependent variables and their performance metrics, roles and responsibilities, duration to retain log data, events that would trigger these systems to send alerts, monitoring intervals/frequency, and how identified cyber-incidents / breaches will be contained, treated, documented, and reported.

f. Determine a baseline of operations and expected data flows for users, systems, and network of the identified systems. This includes but not limited to logon hours, network traffic threshold, level of processor utilization, etc.

g. Implement across all-delivery channels a risk-based transaction monitoring mechanism which shall securely notify customers of all payment or fund transfer transactions above a specified value defined by customers.

h. Establish a non-intrusive real-time monitoring mechanism to collect, correlate, and detect anomalous user, administrator, system, and process/service activities on critical system, database, and network in a timely manner while verifying the effectiveness of protective measures in place.

i. Ensure that the mechanism provides Value Added Services (VAS) such as separating real events from nonimpact events (false positive), locating and containing events, sending alerts to appropriate staff for investigation, remediation, reporting, keeping historical data for the purpose of forensics, and managing operational risks.

j. Monitor the physical environment of assets – server room, network devices, data center, disaster recovery site, and off-site storage location –to detect potential threats

in a timely manner.

k. Establish an effective and efficient non-intrusive mechanism to detect and perform remediation actions on malicious codes and unauthorized mobile codes on all systems (including those on the DMZ). For signature based solutions, frequency of update shall be at least daily.

l. DMBs and PSPs that intends to or have cloud service providers shall be guided by the continuous security monitoring recommendation of Cloud Security Alliance (CSA).

8. **Incident Response:**

This is an organized approach to addressing and managing the aftermath of a security breach or attack (also known as an 'incident') with an objective of reducing damage, recovery time and incident costs. For an effective and efficient Incident Response (IR), a DMB/PSP shall:

a. Review its Disaster Recovery and Business Continuity plan documents (DR/BCP) with the business (stakeholders) to ensure they are adequate and effective to support cybersecurity resilience.

b. Create a DR/BCP test calendar to ascertain the effectiveness and efficiency of the Disaster Recovery and Business Continuity plans.

c. Test the DR/BCP. Lessons learned shall be incorporated into the DR/BCP documents as an improvement.

d. Develop an IR policy with stakeholders. The IR policy shall stipulate:

i. the creation of a cyber-incident response plan; approved by the Board of Directors;

ii. Senior management and business process owners definition of an Acceptable Interruption Window (AIW) for all categories of cyber-incidents and

performance metric at each stage of the IR process;

iii. the establishment of a dedicated team whose focus shall be on detecting and responding to cyber-incident;

iv. adequate and continuous training of the IR team on how to respond, report cyber-incidents, and conduct trend analysis to thwart future occurrence;

v. conducting cybersecurity drills based on the approved cyber-incident response plan and test schedule to ascertain its viability, effectiveness and efficiency;

vi. the adoption of automated detection tool such as network and system (endpoint) scanners; and alerts from Log Management solutions, Firewall, Intrusion Detection/Intrusion Prevention systems (ID/IPS), etc. for effective early detection of cyber-incidents;

vii. appropriate chain of custody when collecting, analyzing and reporting cyber-incident in a manner that is legally admissible; and

viii. how crisis information shall be communicated and shared with stakeholders including the CBN and the public.

9. **Payment Service Provider Security Assurance Programme:**

To ensure that systems and data entrusted by a DMB/PSP (in a nested PSP relationship) to PSPs (entity) are maintained in a secure and compliant manner, the institution shall establish an assurance programme which shall include but not limited to:

i. Launching a due diligence programme on proposed or existing PSP companies thorough vetting prior to establishing a relationship and after engagement to ensure that the entity holds skills and experience appropriate for the service provided.

ii. Establishing written agreements and policies between it and the entity for consistency

and mutual understanding of service provided on their respective responsibilities and obligations.

iii. Continuous monitoring of the PSP's PCI DSS compliance status to provide an assurance of the PSP's compliance with the applicable requirements for the services provided.

iv. Obtaining and reviewing the appropriateness of the entity's incident response, business continuity plan, and cyber-insurance coverage.

v. Reviewing PSP compliance with your third-party security policies

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 Center	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: Cyber-Threat Intelligent Sources

Internal Threat Intelligence (TI) sources

Internal intelligent data sources are those security events generated by the IT infrastructures of DMBs/PSPs. This includes systems and security logs, database activity logs, malware detection report, analysis of network traffic, etc.

1. A DMB/PSP shall have an approved Security Operations Center ("SOC") strategy as sub-set of the Cybersecurity framework (with clear mission, vision and objective) to support its overall business objectives, minimize cybersecurity risk, while meeting regulatory requirements.

2. The strategy shall explicitly state the model of SOC to be adopted (On-premise, In-house, Outsourced or Hybrid).

3. A DMB/PSP's approved organizational chart shall also depict the SOC structure and its team.

4. There shall be a dedicated and secure physical space for the SOC to engender teamwork, brain-storming, knowledge-sharing among members and quick response time.

5. Its ambience shall also be protected with both technical and physical controls and equipped with a TV to keep the SOC staff abreast of imminent cyber events which may affect the DMB/PSP information assets.

6. The SOC shall not just house sophisticated tools but equipped with a Security Information and Event Management (SIEM) solution that aggregates data from various security feeds to provide real-time analysis of security alert. Where applicable, the SOC shall be able to perform prompt remediation service.

7. For intuitive correlations and prompt visibility of the bank' security posture, feeds to the SIEM shall also include logs from network devices, vulnerability assessment systems; application and database scanners; penetration testing tools; IDS/IPS; and enterprise antivirus system.

8. It shall be up and manned continuously (24x7), managed and administered by skilled IT professionals with technical knowledge, experiences and suitable credentials in areas such as operating systems, networking, cryptography, database administrator, digital forensic, etc. For effective monitoring, shifts work schedule shall be adopted. At least two (2) members of the team shall manage the SOC at all time; responsibilities should be clearly defined.

9. The SOC team shall have adequate knowledge of the business, its environment and infrastructure in order to prioritize the most appropriate response when cyber-incidents occur.

10. The SOC shall have well documented processes to:

    - triage various types of cyber-incidents with appropriate response approved by the business process owners for operational consistency;
    - identify, analyze and report emerging threats; and
    - gather and preserve evidence for Forensic Investigation.

11. There shall be a capacity planning tool/process that communicates SOC infrastructure (SIEM) storage to enable the SOC team balance task workload with available resources.

12. At a minimum, the team shall comprise of a SOC Manager, Analysts and Intelligence Architects.

13. Risk and vulnerability assessment shall be conducted on the SOC infrastructure. The SOC infrastructure and processes shall be continually audited either as standalone or part of the cybersecurity process.

14. The SOC shall be able to provide input to the institution's Cybersecurity Awareness Training program based on the identified security incidents.

15. The SOC shall periodically provide cyber-incident reports to Board and Senior Management.

16. Although internal Threat Intelligence (TI) sources provide information that is peculiar to a DMB/PSP's environment, each institution is advised to subscribe to external TI sources for threats notification and possible mitigants.

External TI sources:

These are sources external to a DMB/PSP environment. They combine various sources of TI into a single source which is easy to understand.

1. A DMB/PSP shall subscribe to external TI providers such as data feeds from IT vendors; intelligence sharing group such as the NgCERT, FS-ISAC, ICS-CERT; other DMBs/PSPs; and relevant agencies to keep them informed of emerging cyber-threats and vulnerabilities.

2. Caution shall 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 Providers (PSPs)

Introduction

In accordance with Section 3 of the Central Bank of Nigerian Risk-based Cybersecurity Security Framework, Deposit Money Banks (DMBs) and Payment Service Providers (PSPs) 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 bank'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 PSPs shall conduct and report their Risk-based Cybersecurity Self-Assessment using this template annually but not later than March 31st by the Chief Information Security Officer after its endorsement by the Executive Management. The report shall be submitted to the Director, Banking Supervision Department, Central Bank of Nigeria.

Purpose

The objective is to determine the Cybersecurity resiliency of Nigerian DMBs and PSPs; the ability of DMBs and PSPs to maintain normal operations in spite of all threats and potential risks in the cyberspace.

Definition of Terms:

Likelihood of occurrence: This is the probability that an event will take place. Adopt the legend below to specify the likelihood of occurrence.

Likelihood of occurrence	Impact Definition
High	The identified threat is active and prevalent; the DMB/PSP has little/ineffective/no controls in place to prevent the vulnerability from being exploited by the threat.
Moderate	The identified threat is active and prevalent; but the DMB/PSP has some controls in place which may be capable to prevent the vulnerability from being exploited by the threat.
Low	Identified threat does not apply to the DMB/PSP or the DMB/PSP has sophisticated and efficient controls in place which provides assurance that the risk may not crystallized.

Impact: This is the potential damage caused by a cyber-attack (threat agent). Adopt the legend below to specify the magnitude of potential impact.

Magnitude of Impact	Impact Definition
High	Reputational damage; System down time > 6 hours for mission critical systems, loss of major tangible assets or resources; high monetary loss, violation of the CBN regulations on cybersecurity.
Moderate	Reputational damage; System down time > 1 hour but < 6 hours for mission critical systems, loss of minor tangible assets or resources; moderate

	monetary loss, loss of tangible assets or resources.
Low	System down time < 1 hour for mission critical systems, insignificant monetary loss, loss of tangible assets or resources.

Risk level: To determine the risk level, DMBs/PSPs should consider the likelihood of a threat exploiting a vulnerability; the impact of a successful attack and the existence of security controls to mitigate the risk. Adopt the legend below to state the residual risk level.

Risk Level	Risk Level Definition
High	Corrective action(s) must be put in place immediately.
Moderate	Corrective action(s) must be put in place within a stipulated time
Low	The board shall accept the risk / determine if corrective actions are needed.

Name of Institution

Month, Year

CYBERSECURITY SELF-ASSESSMENT REPORT

Approved By: _____ Approval Date: _____

Approved By: _____ Approval Date: _____

CYBERSECURITY SELF-ASSESSMENT OF NAME OF YOUR INSTITUTION

Scope *State/ Describe the coverage of this Cybersecurity Self-Assessment*

Cybersecurity Assessment Methodology *State the tools/documents/guidelines/framework used to conduct this self-assessment*

Identified Threats					
Threat No 1	***Description of threat***	***Likelihood***	***Impact***	***Mitigating Control(s)***	***Residual Risk***
		Likelihood of occurrence.	Level of impact		Risk level.
Comments to Control(s):					
Threats No 2	***Description of threat***	***Likelihood***	***Impact***	***Mitigating Control(s)***	***Residual Risk***
		Likelihood of occurrence.	Level of impact		Risk level.
Comments to Control(s):					
Threats No 3	***Description of threat***	***Likelihood***	***Impact***	***Mitigating Control(s)***	***Residual Risk***
		Likelihood of occurrence.	Level of impact		Risk level.
Comments to Control(s):					
Threats No 4	***Description of threat***	***Likelihood***	***Impact***	***Mitigating Control(s)***	***Residual Risk***

		Likelihood of occurrence.	Level of impact		Risk level.
Comments on Control(s):					
Threat No 5	***Description of threat***	***Likelihood***	***Impact***	***Mitigating Control(s)***	***Residual Risk***
		Likelihood of occurrence.	Level of impact		Risk level.
Comments on Control(s):					
Threat No 6	***Description of threat***	***Likelihood***	***Impact***	***Mitigating Control(s)***	***Residual Risk***
		Likelihood of occurrence.	Level of impact		Risk level.
Comments on Control(s):					
Threat No 7	***Description of threat***	***Likelihood***	***Impact***	***Mitigating Control(s)***	***Residual Risk***
		Likelihood of occurrence.	Level of impact		Risk level.
Comments on Control(s):					
Threat No 8	***Description of threat***	***Likelihood***	***Impact***	***Mitigating Control(s)***	***Residual Risk***
		Likelihood of occurrence.	Level of impact		Risk level.
Comments on Control(s):					
Threat No 9	***Description of threat***	***Likelihood***	***Impact***	***Mitigating Control(s)***	***Residual Risk***
		Likelihood of occurrence.	Level of impact		Risk level.

Comments on Control(s):					
Threat No 10	***Description of threat***	***Likelihood***	***Impact***	***Mitigating Control(s)***	***Residual Risk***
		Likelihood of occurrence.	Level of impact		Risk level.
Comments on Control(s):					

Vulnerability Assessment

Asset No 1	***Description of Vulnerability***	***Threat***	***Likelihood***	***Impact***	***Mitigating Control(s)***	***Residual Risk***
			Likelihood of occurrence.	Level of impact		Risk level.
Comments on Control(s):					***Time Frame***	Time Frame to Close Vulnerability
Asset No 2	***Description of Vulnerability***	***Threat***	***Likelihood***	***Impact***	***Mitigating Control(s)***	***Residual Risk***
			Likelihood of occurrence.	Level of impact		Risk level.
Comments on Control(s):					***Time Frame***	Time Frame to Close Vulnerability
Asset No 3	***Description of Vulnerability***	***Threat***	***Likelihood***	***Impact***	***Mitigating Control(s)***	***Residual Risk***
			Likelihood of occurrence.	Level of impact		Risk level.
Comments on Control(s):					***Time Frame***	Time Frame to Close Vulnerability

Asset No 4	***Description of Vulnerability***	***Threat***	***Likelihood***	***Impact***	***Mitigating Control(s)***	***Residual Risk***
			Likelihood of occurrence.	Level of impact		Risk level.
Comments on Control(s):					***Time Frame***	Time Frame to Close Vulnerability
Asset No 5	***Description of Vulnerability***	***Threat***	***Likelihood***	***Impact***	***Mitigating Control(s)***	***Residual Risk***
			Likelihood of occurrence.	Level of impact		Risk level.
Comments on Control(s):					***Time Frame***	Time Frame to Close Vulnerability
Asset No 6	***Description of Vulnerability***	***Threat***	***Likelihood***	***Impact***	***Mitigating Control(s)***	***Residual Risk***
			Likelihood of occurrence.	Level of impact		Risk level.
Comments on Control(s):					***Duration***	Time Frame to Close Vulnerability
Asset No 7	***Description of Vulnerability***	***Threat***	***Likelihood***	***Impact***	***Mitigating Control(s)***	***Residual Risk***
			Likelihood of occurrence.	Level of impact		Risk level.
Comments on Control(s):					***Duration***	Time Frame to Close Vulnerability
Asset No 8	***Description of Vulnerability***	***Threat***	***Likelihood***	***Impact***	***Mitigating Control(s)***	***Residual Risk***
			Likelihood of occurrence.	Level of impact		Risk level.
Comments on Control(s):					***Duration***	Time Frame to Close Vulnerability

Asset No 9	*Description of Vulnerability*	*Threat*	*Likelihood*	*Impact*	*Mitigating Control(s)*	*Residual Risk*
			Likelihood of occurrence.	Level of impact		Risk level.
Comments on Control(s):					*Duration*	Time Frame to Close Vulnerability
Asset No 10	*Description of Vulnerability*	*Threat*	*Likelihood*	*Impact*	*Mitigating Control(s)*	*Residual Risk*
			Likelihood of occurrence.	Level of impact		Risk level.
Comments on Control(s):					*Duration*	Time Frame to Close Vulnerability

Justification

Based on the Threat Sources, Events and System Vulnerabilities Assessment completed above, the system's overall risk is Pick a Risk Level.

Reason	

_____

Conducted by Name & Signature *Title* *Date*

Central Bank of Nigeria

Cyber-Threat Intelligence Report Template

For

Deposit Money Banks (DMBs) and Payment Service Providers (PSPs)

Purpose

The purpose of the cyber-threat intelligence reporting is to provide a risk-based approach to promptly identify emerging cyber threat, trends, patterns, risks, and their potential impact. It is not the aftermath of an incident but a proactive measure to mitigate against emerging cyber-risk.

Definition of Terms:

Likelihood of occurrence: This is the probability that an event will take place. Adopt the legend below to specify the likelihood of occurrence.

Likelihood of occurrence	Impact Definition
High	The identified threat is active and prevalent; the DMB/PSP has little/ineffective/no controls in place to prevent the vulnerability from being exploited by the threat.
Moderate	The identified threat is active and prevalent; but the DMB/PSP has some controls in place which may be capable of preventing the vulnerability from being exploited by the threat.
Low	Identified threat does not apply to the DMB/PSP or it has sophisticated and efficient controls in place which provides assurance that the risk may not crystalize.

Impact: This is the potential damage caused by a cyber-attack (threat agent). Adopt the legend below to specify the magnitude of potential impact.

Magnitude of Impact	**Impact Definition**
High	Reputational damage; System down time > 6 hours for mission critical systems, loss of major tangible assets or resources; high monetary loss or violation of the CBN regulations on cybersecurity.
Moderate	Reputational damage; System down time > 1 hour but < 6 hours for mission critical systems, moderate monetary loss, loss of tangible assets or resources.
Low	System down time < 1 hour for mission critical systems, insignificant monetary loss, loss of tangible assets or resources.

Risk level: To determine the risk level, DMB/PSP should consider the likelihood of a threat exploiting a vulnerability; the impact of a successful attack and the existence of security controls to mitigate the risk. Adopt the legend below to state the residual risk level.

Risk Level	**Risk Level Definition**
High	Corrective action(s) must be put in place immediately.
Moderate	Corrective action(s) must be put in place within a stipulated time
Low	The board shall accept the risk / determine if corrective actions are needed.

Name of Institution

Month, Year

CYBER-THREAT INTELLIGENCE REPORT

Approved By: _____ Approval Date: _____

Approved By: _____ Approval Date: _____

Identified Cyber-Threats								
S/No	***Threat(s) Name and Description***	***Date detected***	***How was the threat identified (Internal/External Source)***	***Potential Victim(s)/ Targeted Asset***	***Likelihood***	***Impact***	***Security Controls In Place***	***Level of Residual Risk***
		Select Date			Likelihood of successful attack.	Level of impact if successful		Risk level with the controls in place.
Comments								
S/No	***Threat(s) Name and Description***	***Date detected***	***How was the threat identified (Internal/External Source)***	***Potential Victim(s)/ Targeted Asset***	***Likelihood***	***Impact***	***Security Controls In Place***	***Risk level***
		Select Date			Likelihood of successful attack.	Level of impact if successful		Risk level with the controls in place.
Comments								
S/No	***Threat(s) Name and Description***	***Date detected***	***How was the threat identified (Internal/External Source)***	***Potential Victim(s)/ Targeted Asset***	***Likelihood***	***Impact***	***Security Controls In Place***	***Level of Residual Risk***
		Select Date			Likelihood of successful attack.	Level of impact if successful		Risk level with the controls in place.
Comments								

S/No	Threat(s) Name and Description	Date detected	How was the threat identified (Internal/External Source)	Potential Victim(s)/ Targeted Asset	Likelihood	Impact	Security Controls In Place	Level of Residual Risk
		Select Date			Likelihood of successful attack.	Level of impact if successful		Risk level with the controls in place.
Comments								
S/No	**Threat(s) Name and Description**	**Date detected**	**How was the threat identified (Internal/External Source)**	**Potential Victim(s)/ Targeted Asset**	**Likelihood**	**Impact**	**Security Controls In Place**	**Level of Residual Risk**
		Select Date			Likelihood of successful attack.	Level of impact if successful		Risk level with the controls in place.
Comments								
S/No	**Threat(s) Name and Description**	**Date detected**	**How was the threat identified (Internal/External Source)**	**Potential Victim(s)/ Targeted Asset**	**Likelihood**	**Impact**	**Security Controls In Place**	**Level of Residual Risk**
		Select Date			Likelihood of successful attack.	Level of impact if successful		Risk level with the controls in place.
Comments								
S/No	**Threat(s) Name and Description**	**Date detected**	**How was the threat identified (Internal/External Source)**	**Potential Victim(s)/**	**Likelihood**	**Impact**	**Security Controls In Place**	**Level of Residual Risk**

				Targeted Asset				
		Select Date			Likelihood of successful attack.	Level of impact if successful		Risk level with the controls in place.
Comments								

_____ _____ _____

Prepared by Name & Signature *Title* *Date*

Central Bank of Nigeria

Security Incident Reporting Template

For

Deposit Money Banks (DMBs) and Payment Service Providers (PSPs)

Security incidents must be reported by DMBs to the Director, Banking Supervision, Central Bank of Nigeria within the first six 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 necessary, additional document should be provided and appended to this form.

CONTACT INFORMATION	
DMB's/PSP's Name:	
Staff Name:	
Designation:	**Department:**
Phone No:	**Email:**
Additional Contact Details: _____ _____ _____	
INCIDENT DETAILS	
Date & Time Incident was Discovered:	
New Incident ☐	**Update to Incident** ☐

	Please provide reference to previous incident:

Date & time Incident was detected:

Type of Incident Detected:

☐ Unauthorised Access	☐ Advanced Persistent Threat	☐ Phishing
☐ Denial of Service	☐ Inappropriate/Misuse of system	☐ Unplanned Downtime
☐ Unauthorised Use	☐ Website Defacement	☐ Malicious Code
☐ Access or Credential Abuse	☐ Sustained Probe/Scan	☐ Others

If other, please state:

Description of Incident:

_____

_____

_____

_____

Incident Impact :

☐ Outage of Critical IT System	☐ Theft or Loss of Customer Information
☐ Loss of sensitive Information	☐ Outage of Infrastructure
☐ Financial Loss	☐ Cybersecurity Incident (DOS, Ransomware etc.)
☐ Regulatory & Legal	☐ Others.

If other, please state:

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's/PSP's network, critical system(s) or a combination at risk is impacted. May lead to system downtime.
Low	Non-critical system(s) was impacted.

Please select impact:

☐ High
☐ Moderate
☐ Low

Description of Impact:

_____

_____

_____

_____

_____

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

Description of Impact Category:

_____

_____

_____

_____

_____

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

Incident Notification

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

If other, please state:

INCIDENT ACTIONS

Incident Detection: (Date, Time and Details):

_____

_____

_____

_____

_____

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

Please provide details on location, purpose of this system/ network, affected applications (including hardware, manufacturer, software developer, make/ model, operating system, database version etc.) running on the systems/networks, etc., If known, any TCP or UDP ports involved in the incident; If known, provide the affected system's IP address If known, provide the attacker's IP address:

_____

_____

_____

_____

Containment Measures:

_____

_____

_____

Evidence Collected (Systems Logs, etc.):

_____

_____

_____

Eradication Measures:

_____

_____

_____

Recovery Measures:

_____

_____

_____

Other Mitigation Actions:

_____

_____

_____

Acronyms

AIW	Acceptable Interruption Window
APT	Advanced Persistent Threat
ATM	Automated Teller Machine
AOC	Attestation of Compliance
AOSC	ASV Scan Report Attestation of Scan Compliance
BCP/DR	Business Continuity/ Disaster Recovery Plan
BYOD	Bring Your Own Device
CSA	Cloud Security Alliance
COBIT	Control Objectives for Information and related Technology
DMB	Deposit Money Bank
DMZ	Demilitarized Zone
FFIEC	Federal Financial Institutions Examination Council
FS-ISAC	Financial Services Information Sharing and Analysis Center
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IDS	Intrusion Detection System
IP Phones	Internet Protocol Phones
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
LAN	Local Area Network
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 DMB/PSP 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 DMB/PSP'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.
Internet	An internet is an interconnected computer networks linked by the internet protocol suite.
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 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.
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 cyber-threat 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 DMB/PSPs 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 DMB/PSP
Vulnerability	This is a weakness or gap in a system, application, process, device, etc.