CENTRAL BANK OF NIGERIA

Banking Supervision Department
Central Business District
P.M.B. 0187
Garki, Abuja.

E-mail:bsd@cbn.gov.ng

09-462-36401

BSD/DIR/GEN/LAB/11/016

June 25, 2018

LETTER TO ALL BANKS AND PAYMENT SERVICE PROVIDERS

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

Due to the recent increase in the number and sophistication of cyber-security threats against Deposit Money Banks (DMBs) and Payment Service Providers (PSPs), it has become mandatory for these institutions to strengthen their cyber defenses if they are to remain safe and sound.

The CBN hereby releases the attached draft guidelines stipulating minimum requirements for enhancing cyber-security for your comments/inputs.

Kindly send hard copies of your comments/inputs to the Director, Banking Supervision while soft copies should be emailed to Bsdreturns@cbn.gov.ng on or before July 31, 2018.

Thank you.

K. O. BALOGUN
FOR: DIRECTOR OF BANKING SUPERVISION

RISK-BASED CYBERSECURITY FRAMEWORK AND GUIDELINES

FOR

DEPOSIT MONEY BANKS
AND
PAYMENT SERVICE PROVIDERS

JUNE 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 six parts: Cybersecurity Governance and Oversight, Cybersecurity Risk Management System, Cyber Resilience Assessment, Cybersecurity Operational Resilience, Cyber-Threat Intelligence and Metrics, Monitoring & Reporting.

2. Cybersecurity Governance and Oversight

2.1. Cybersecurity governance sets the agenda and boundaries for cybersecurity management and controls through defining, directing and supporting the security efforts of the DMBs and PSPs. It spells out the responsibilities of the Board of Directors, 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 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.

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 operations security risk, and shall also be responsible for the implementation of the cybersecurity strategy as approved by the Board.

2.6.3. The CISO shall possess adequate authority, experience, independence and status within the DMB/PSP to enable him/her function properly.

2.6.4. The CISO should not report to the Head of Information Technology (IT) operations and to the ensure segregation of duty, the two offices shall be head by separate individuals.

2.6.5. The CISO shall possess educational and experience requirements as provided in the Fit and Proper (Approved Persons) Framework required for Assistant General Managers and above.

2.6.6. In addition, the CISO shall possess any or a combination of Masters in Cyber/Information Security, Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM) certifications with in-depth experience in Information Technology.

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

2.7.1. Every DMB/PSP shall establish an information security steering committee that shall be responsible for the governance of the cybersecurity programme. The steering committee shall consist of senior representatives of relevant departments within the DMB/PSP. The roles, responsibilities, scope and activities of the information security steering committee shall be clearly defined.

The objectives of the Committee shall include:

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

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

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

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

2.8. **Risk Management Control Functions**

To ensure the effectiveness of a DMB/PSP's cybersecurity governance, its processes and controls shall be reviewed at least biannually. In this regard, the risk management control functions shall be responsible for ensuring that cybersecurity risks within the DMB/PSP are properly mitigated.

2.8.1. **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.

2.8.2. Compliance

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

2.8.3. 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.

2.9. Cybersecurity Strategy and Framework

2.9.1. The Board of Directors shall approve the DMB/PSP's 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.

2.9.2. A DMB/PSP shall also put in place a 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.

2.9.3. In addition, a DMB/PSP shall develop a cybersecurity policy either as a separate document or as part of its cybersecurity framework. The policy shall clearly convey management intent and the DMB/PSP's approach to achieving its cybersecurity objectives.

2.9.4. The policy document(s) approved by the Board shall be continuously reviewed and updated once in two (2) years 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 framework and policies shall be reviewed annually to 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.

4. Cyber Resilience Assessment

Cyber 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 resilience assessment to determine its current and target cybersecurity profile.

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

4.1.1. 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.

4.1.2. 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; and efficacy of existing controls to mitigate the identified risks.

4.1.3. 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 I. All gaps identified shall be documented and communicated to the Board of Directors.

4.2. **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 timeframe. 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.

4.3. **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; intended controls to be implemented 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 bi-annually not later than February 28th and August 31st. The report shall be signed and submitted by the Chief Information Security Officer after its endorsement by the Board of Directors. See the reporting template in Appendix VI.

5. **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 to ensure the Confidentiality, Integrity and Availability (CIA) of their information assets among others.

5.1. **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 II.

5.2. **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 III and IV as the minimum cybersecurity baselines to enhance its cybersecurity resilience.

6.1. **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:

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

6.1.2. 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.

6.1.3. Identify and document various CTI Sources. See Appendix V for details.

6.1.4. 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.

6.1.5. 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 VI after its endorsement by appropriate authorities.

7. Metrics, Monitoring & Reporting

7.1. 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.

7.2. 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.

7.3. 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.

7.4. 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.

7.5. 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.

7.6. A DMB/PSP is required to report all cyber-incidents whether successful or not immediately after such incident was identified to the Director of Banking Supervision, Central Bank of Nigeria using the report format in Appendix VI. Where necessary and applicable, additional information should be provided afterwards.

8. **Compliance with Statutory and Regulatory Requirements**

   8.1. 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.

   8.2. 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.

   8.3. 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.

9. **Compliance**

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

10. **Effective Date**

    This Guideline shall take effect from August 1, 2018

Appendix I: Cybersecurity Self-Assessment Tools

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

Appendix II: Know Your Environment:

1. **Asset Management**

Hardware: A DMB/PSP shall:

1.1 Maintain an up-to-date inventory of all authorized devices such as workstations, laptops, switches, routers, firewall, printers, scanner, photocopiers, etc. used to process, store or transmit data/information in the institution.

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.

1.5 Ensure that all legacy systems but still-in-use (both critical and non-critical) shall be catalogued. Vulnerabilities associated with them shall be promptly identified and compensating controls applied and must be considered for upgrade.

Software: A DMB/PSP shall:

1.6 Devise a mechanism to maintain an up-to-date inventory of all applications/software (authorized and unauthorized) installed and/or running on all its systems. Unauthorized software/applications identified shall be considered for removal.

1.7 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.

1.8 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.

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

Other Network devices: A DMBs and PSPs shall:

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

1.11 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;

1.12 Devise a mechanism to maintain an up-to-date inventory of all other authorized network devices - ATMs, IP Phones and surveillance camera etc. - connected to its network. Unauthorized other devices shall not be granted access to the network; and

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

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 rotation of job duties and responsibilities; and mandatory vacation/leave are employed to thwart opportunities for collusion, 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 III: 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 an unprecedented 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 IV 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. Communicate cybersecurity awareness to their customers in the language they understand; possibly in local dialect at least monthly or when there is an identified cyber-threat or attack vector. SMS

f. Devise mechanisms to communicate cybersecurity awareness messages to all their customers in the language they understand irrespective of their location. To thwart phishing attack among others, the messages shall be communicated in English and local dialects 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 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:

educate employees through a warning pop-up message, encryption, or prevent the action; 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, fault deny, defense in-depth, and fail secure whilst mitigating against OWASP vulnerabilities. These applications shall also be thoroughly tested by a team of independent software testers

and business/application owners.

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

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

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

6. **Vulnerability Management**:

A DMB/PSP shall promptly identify latent weaknesses in their IT infrastructure (assets), account profiles (system administrators and privileged users), and vendors.

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 strategy; approved by the Board of Directors.

  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). The 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 sources 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 incessantly 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 and 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. Categorize the identified systems and processes needed to be monitored according to their criticality and sensitivity to its operations.

f. Define a continuous security monitoring policy/strategy which shall be approved by the Board of Director; 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.

g. 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.

h. 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.

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

j. 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.

k. 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.

l. 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.

m. 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 (IR):**

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, 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:

- 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.

- Establishing written agreements and policies between it and the entity for consistency and mutual understanding of service provided on their respective responsibilities and obligations.

- 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.

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

- Reviewing PSP compliance with your third-party security policies

Appendix IV: 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 V: Cyber-Threat Intelligent Sources

<u>Internal Threat Intelligence (TI) sources</u>

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 document approved by the Board of Directors (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). The SOC shall have its own budget approved; by the Board.

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

- 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, Intelligence Architects and Forensic Analysts.

13. Risk and vulnerability assessment vulnerability assessment shall be conducted on the SOC infrastructure. The SOC infrastructure and processes shall be continually audited.

14. It shall have a forensic laboratory equipped with specialized forensic tools to support incident response investigation efforts.

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

16. The SOC shall periodically provide cyber-incident reports to Board and Senior management.

17. Although internal 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 VI: Reporting Templates

1. Cybersecurity Self-Assessment Available at: https://www.cbn.gov.ng/documents/
2. Cyber-Threat Reporting Available at: https://www.cbn.gov.ng/documents/
3. Cyber-Incidents Reporting Available at: https://www.cbn.gov.ng/documents/

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.