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

PAYMENTS SYSTEM MANAGEMENT DEPARTMENT
Tel: 09 462 38300, 09 462 38346
e-mail: psmd@cbn.gov.ng
website: www.cbn.gov.ng

PSM/DIR/PUB/CIR/001/043

March 7, 2023

CIRCULAR TO ALL DEPOSIT MONEY BANKS, MOBILE MONEY OPERATORS AND PAYMENT SERVICE PROVIDERS

ISSUANCE OF THE OPERATIONAL GUIDELINES FOR OPEN BANKING IN NIGERIA

The Central Bank of Nigeria, in furtherance of its mandate for the stability of the financial system and pursuant to its role in deepening the financial system, hereby issues the Operational Guidelines for Open Banking in Nigeria.

The adoption of Open Banking in Nigeria will foster the sharing of customer-permissioned data between banks and third-party firms to enable the building of customer-focused products and services. It is also aimed at enhancing efficiency, competition and access to financial services in Nigeria.

All stakeholders are required to ensure strict compliance with the guidelines and all other regulations, as the CBN continues to monitor developments and issue guidance as may be appropriate.

Musa I. Jimoh
Director, Payments System Management Department

CENTRAL BANK OF NIGERIA

OPERATIONAL GUIDELINES FOR OPEN BANKING IN NIGERIA

APPROVED MARCH 2023

Contents

1.0 PREAMBLE 4
2.0 TERMS AND DEFINITIONS 5
3.0 INTRODUCTION 7
4.0 SCOPE 7
4.1 PARTICIPANTS 7
5.0 OBJECTIVES 8
6.0 OPEN BANKING REGISTRY 8
6.1 ACCREDITATION CRITERIA 9
7.0 CONSENT MANAGEMENT 9
8.0 RESPONSIBILITIES OF API PROVIDER / CONSUMER 9
8.1 ACCESS RULES 9
8.2 AVAILABILITY AND PERFORMANCE 11
8.3 KEY PERFORMANCE INDICATORS (KPIs) 14
8.4 BUSINESS CONTINUITY 15
8.5 PROBLEM MANAGEMENT 15
8.6 INTERFACE REQUIREMENTS 16
8.7 CHANGE MANAGEMENT 17
8.8 REPORTING 18
8.9 ANTI-COMPETITION PRACTICES 19
9.0 DATA AND INFORMATION TREATMENT 19
9.1 DATA ETHICS 19
9.2 DATA PRIVACY 20
9.3 INFORMATION SECURITY 20
9.4 RENDITION OF RETURNS 23
9.5 ANTI-MONEY LAUNDERING (AML) AND COMBATING THE FINANCING OF TERRORISM (CFT) 23
9.6 TESTING 23
9.7 BUSINESS CONTINUITY AND DISASTER RECOVERY 23
10.0 CHANGE AND COMMUNICATION MANAGEMENT 24
10.1 INTRODUCTION OF CHANGE 24
11.0 SHARED INFORMATION FRAMEWORK 26
11.1 INFORMATION SHARING 26
11.2 VERIFICATION OBLIGATION 27

11.3 DIGITAL SIGNATURES 27
11.4 ENABLING DATA FLOWS 28
11.5 RISK ASSESSMENT REPORTING FOR REGISTERED PARTICIPANTS 28
11.6 RISK MANAGEMENT COMMITTEE 28
11.7 CYBERSECURITY BREACH INCIDENT REPORTING 29
11.8 INCIDENT REPORTING PORTAL 29
11.9 DATA BREACH POLICY AND PROCEDURE 29
11.10 DATA INCIDENT MANAGEMENT PROCEDURE 30
11.11 REVALIDATION OF AGREEMENTS 31
11.12 INTELLECTUAL PROPERTY PRESERVATION 31
12.0 DISPUTE RESOLUTION 31
APPENDIX 1 – API STANDARDS 32
APPENDIX II – RISK MANAGEMENT 41
APPENDIX III – SECURITY STANDARDS 47
APPENDIX IV – CUSTOMER EXPERIENCE STANDARDS 58
APPENDIX V – OPERATIONAL READINESS CHECKLIST 62

1.0 PREAMBLE

The Central Bank of Nigeria (CBN), hereafter called the Bank, had issued the Regulatory Framework for Open Banking in Nigeria in its efforts to enhance competition and innovation in the banking system.

The Bank recognise the existence of an ecosystem for Application Programming Interface (API) in the financial and payments system and is aware of various efforts in the industry to develop acceptable standards among stakeholders.

The Bank, in collaboration with industry stakeholders, developed Operational Guidelines for Open Banking in line with the provisions of the Regulatory Framework. In view of this, the Bank hereby issues the Operational Guidelines for Open Banking in Nigeria.

2.0 TERMS AND DEFINITIONS

Abbreviations	Definition
2FA	Two Factor Authentication/ Strong Authentication
AC	API Consumer
AP	API Provider
API	Application Programming Interface
CAC	Corporate Affairs Commission
CBN	Central Bank of Nigeria
CM	Configuration Management
DMZ	Demilitarized Zone (pertaining to TCP/IP Networks)
FI	Financial Institution
Fintech	A Financial and Technology Services Company
GUID	Global Unique Identifier
IM	Information Management
ITIL	Information Technology Infrastructure Library
MLS	Message Level Security. In the context of this document, this refers to Message Signing.
MPR	Monetary Policy Rate
NDPR	Nigeria Data Protection Regulation
NITDA	National Information Technology Development Agency
OBR	Open Banking Registry
OLAP	Online Analytic Processing
OLTP	Online Transaction Processing
SLA	Service Level Agreement
Transaction	A request to a financial institution to authorise the disbursement of goods or performance of services on behalf of a customer based on funds the customer has with the financial institution.

UUID	User Unique Identifier
Sponsor	Sponsored Participants - Tier 0 & Tier 1
	Sponsoring Participants - Tier 2 & Tier 3

3.0 INTRODUCTION

The Regulatory Framework for Open Banking in Nigeria established principles for data sharing across the banking and payments system to promote innovations and broaden the range of financial products and services available to bank customers. As a result, open banking recognises the ownership and control of data by customers of financial and non-financial services, and their right to grant authorisations to service providers for the purpose of accessing innovative financial products and services. Open Banking applicability includes Agency Banking, Financial Inclusion, Know your customer (KYC), credit scoring/rating etc. These Guidelines are anticipated to drive competition and improve accessibility to financial and payments services.

Participants in open banking shall adhere strictly to security standards when accessing and storing data, and shall be subject to minimum privacy, operational, customer experience and risk management standards as prescribed by the Bank.

4.0 SCOPE

The Guidelines apply to banking and other related financial services as categorised and determined by the Bank in the Regulatory Framework for Open Banking in Nigeria.

4.1 PARTICIPANTS

Given the open banking regulation, any organisation that has data of customers which may be exchanged with other entities for the purpose of providing innovative financial services within Nigeria, shall be eligible to participate in the Open Banking ecosystem.

Access Level by Data and Service Category shall be as specified in Section 5.1 of the Regulatory Framework for Open Banking in Nigeria.

Entities participating in Open banking shall be categorised based on the following roles. Participants shall assume a role depending on the services:

i. **API Provider (AP):** This refers to a participant that uses API to avail data or service to another participant. An API Provider can be a licensed financial institution/service provider, a Fast-Moving Consumer Goods (FMCG) Company or other retailers, Payroll Service Bureau etc.

ii. **API Consumer (AC):** This refers to a participant that uses API released by the (API) providers to access data or service. An API Consumer can be a licensed financial institution/service provider, an FMCG or other retailers, Payroll Service Bureau etc.

iii. **Customer:** This refers to the data owner that shall be required to provide consent for release of data for the purpose of accessing financial services.

****Requirements and responsibilities of performing each role identified above has been specified in the corresponding sections of this Guidelines.**

5.0 OBJECTIVES

The Open Banking Operational Guidelines:

i. Provide clear responsibilities and expectations for the various participant categories

ii. Ensure consistency and security across the open banking system

iii. Stipulate safeguards for financial system stability under an open banking regime

iv. Promote competition and enhances access to banking and other financial services

v. Outline minimum requirements for participants.

6.0 OPEN BANKING REGISTRY

The Central Bank of Nigeria (CBN) shall provide and maintain an Open Banking Registry (OBR) for the industry. The OBR shall be maintained for the following purposes:

i. To provide regulatory oversight on participants

ii. To enhance transparency in the operations of Open Banking

iii. To ensure that only registered institutions operate within the open banking ecosystem.

The OBR shall be a public repository for details of registered participants. Each participant shall be identified by its CAC business registration number, which shall be the unique key across the OBR system.

The OBR shall maintain an API interface, defined within these guidelines, which shall serve as the primary means by which API providers manage the registration of their API consumers.

OBR shall be a repository of APIs in the Open Banking Ecosystem.

6.1 ACCREDITATION CRITERIA

The technical and non-technical criteria for onboarding into the OBR shall be based on the provisions of section 5.0 in the Regulatory Framework for Open Banking.

6.2 DATA GOVERNANCE

6.2.1 The Bank shall provide data oversight and governance for open banking information assets for participants in the open banking arrangement to ensure compliance with relevant legal and regulatory provisions.

6.2.2 Notwithstanding the provisions in 6.2.1 above, all participants shall be guided by all extant laws relating to data protection, consumer rights and fair practices.

6.2.3 Participants shall ensure that customer-permissioned data is accurate, up-to-date and complete in data exchanges.

7.0 CONSENT MANAGEMENT

Consent shall be required from customers whose data are required to avail them open banking products and services.

The provisions guiding consent management are as contained in the API Standards Document (Appendix I) and other corresponding sections of Customer Experience (Appendix IV).

8.0 RESPONSIBILITIES OF API PROVIDER / CONSUMER

API Providers/Consumers shall comply with the provisions of this section.

8.1 ACCESS RULES

8.1.1 CONFIGURATION MANAGEMENT

Detailed inventory of open banking system configuration items shall be kept in accordance with current Information Technology Infrastructure Library (ITIL) standards. At the minimum, the inventory shall be electronically searchable for registered participants.

API Providers/Consumers shall be required to have:

i. A Configuration Management (CM) policy approved by its Executive or Board Level Information Technology Steering Committee or equivalent governance body not less than Executive level

ii. Automated CM processes

iii. A log of all changes within the CM system, audited on a quarterly basis, or more frequently, and defined in the approved CM

iv. A configuration database with the following architecture:

   a. Logical listing of system types

   b. Definition of configuration items per system type

   c. Physical listing of systems and specifications of each configuration item per system type

   d. Diagramming tool that reads off the inventory to typify the architecture of the systems showing connections and dependencies

   e. A diagnostic assessment tool for the functional status of the configuration items and points of failure in the system.

8.1.2 SERVICE LEVEL AGREEMENT

A Service Level Agreement (SLA) shall be executed between API providers and API consumers to govern the relationships between the parties. The SLA for open banking shall include:

8.1.2.1 ACCOUNTING AND SETTLEMENT

The following practices shall be adopted:

i. Operations involving movement of funds within the API provider's domain shall be recorded at the account level of the API consumer involved

ii. Metrics used for billing shall be definitively agreed and included in the SLA

iii. Separate principal and fee-collection accounts shall be maintained.

8.1.2.2 FEE STRUCTURE

All participants shall state the fees in the SLA and publicly disclose on their websites and applications.

8.1.2.3 RECONCILIATION OF BILLS

Participants shall implement event-triggered billing systems where the bills are easily traceable to the activity performed per transaction.

8.1.2.4 REGISTRATION AND SPONSORSHIP RESPONSIBILITIES

The details, roles and responsibilities of sponsored participants and direct third parties shall be included in the contract and the sponsoring participant shall be responsible for the execution and performance of the contract.

8.2 AVAILABILITY AND PERFORMANCE

All participants shall make available all systems required for open banking with minimum standards specified in this guideline.

8.2.1 SERVICE MONITORING

API providers/consumers shall:

i. Monitor infrastructural and API levels performance - internally monitor hardware, hypervisor, operating system, application environment metrics at the functional level.

ii. Collect performance metrics for all API transactions - these metrics shall be frequently stored.

iii. Implement monitoring processes that alert (visually or otherwise) first-level support personnel to identify suspicious and critical level occurrences.

8.2.2 INCIDENT MANAGEMENT

8.2.2.1 Classification of Incidents

Open banking incidents are classified as:

i. **Functional:** involving or affecting the good path of a single operation or function. The classification is deemed “systemic” where such a function is critical to a major offering of the system. For instance, a problem with the authentication procedure which effectively bars everyone from accessing the system. Function-level incidents are likely to be spotted via declining metrics such as percentage of successful calls, average total processing time and API availability or while investigating user complaints.

ii. **Performance:** incidents relating to performance may be gradual or acute. In general, they are characterized by degradation of service levels and may be spotted with metrics such as long average processing times, fluctuating

percentage of success rates without any corresponding changes in volume and fluctuating availability.

iii. **Systemic:** cover issues that prevent one or all installations or instances of the Open Banking API infrastructure from offering service, a degradation of service levels across many of the functions, or unavailability of a major system function.

8.2.2.2 Incident Management Procedures

In the event of an incident, API providers/consumers shall:

i. Determine the scope and impact of the incident and notify API providers/consumers relying on services via the recommended communication channel;

ii. Assess the functionality and reliability of the failover system;

iii. Consider workarounds to restore service in a timely manner;

iv. Evaluate the cost efficiency of the failover compared with the loss experienced from the incident; and

v. Investigate root cause and commence resolution following documented procedures.

vi. Also, adhere to the following:

   a. Create and regularly test an incident response plan

   b. Provide skilled personnel to monitor and support Open Banking API infrastructure on 24x7 basis

   c. Provide contacts of the relevant personnel to API providers/consumers within SLA documentation

   d. Design and review on a quarterly basis an incident management and response manual indicating failover and failback steps to be undertaken for a critical incident

   e. Maintain an incident manual with lessons learnt from previous critical incidents.

8.2.3 PERFORMANCE MONITORING

APs shall:

i. Provide performance monitoring dashboards which registered ACs can access at any time to generate reports or locate patterns

ii. Collaborate with ACs to provide built-in performance metric gathering into their APIs to monitor API performance

iii. Publish performance metrics in the Meta Directory under the Get Performance API call

iv. Record individual API performance metrics with at most 5-minute intervals between data points. Any interval missed is assumed to be downtime except within a period coinciding with a scheduled change or maintenance activity

v. Make the performance metrics available as part of the API standard

vi. Publish the KPIs on the open banking portal which shall be available to the public without requiring any token, cookies, etc.

vii. APs shall send a summarized monthly report to the Bank using the Open Banking registry API interface.

These metrics shall be kept on a transactional level for investigative purposes.

The following types of performance information, at the minimum, are required from all APIs published by API providers:

#	**Metric**	**Description**
1	msg_validation_time	Average time it takes to validate the message e.g. sender authentication, time stamp checking, message signature verification, Authentication token verification, message fields validation etc.
2	network_proc_time	Network processing time i.e. time between the timestamp in the request message and the timestamp on the API server at the time of receipt.
3	avg_db_time	Average time it takes to perform database operations
4	avg_ext_call_time	Average time it takes to perform subroutine API calls from within the API
5	avg_log_time	Average time it takes to log API calls.
6	avg_total_proc_time	Average total processing time i.e. time between receiving a request and dispatching a response.

#	Metric	Description
7	avg_req_proc_time	Average request processing time i.e. time between when a request is received and dispatched to internal micro-services for processing
8	avg_rsp_proc_time	Average response processing time i.e. time between when a response is received internally, formatted and sent to the client system.
9	total_api_calls	Total number of API calls processed
10	%_success	Relates to messages successfully received, unpacked and responded to
11	%_approved	Relates to messages that achieved the function for which the call was made.
12	calls_per_sec	Average calls per second.

APs shall provide API availability metrics which include metrics collected:

i. From outside the APs' networks;

ii. Over the internet;

iii. Through at least two major Internet Service Provider routes;

iv. Per API endpoint.

8.2.4 Event Logging

i. Requests and responses shall be logged for at least 180 days by APs and ACs

ii. Participants shall assess the requirements and provide sufficient infrastructure given the volumes they expect and peak period loads.

8.3 KEY PERFORMANCE INDICATORS (KPIs)

The following generic performance levels form the minimum standard for Open Banking systems:

S/N	Metric	Operational	Suspect	Critical
1	Availability	>98%	>=95%	<95%

2	Avg. API Total. Processing Time	<3 secs	<=7 secs	>7 secs
3	Success Rate	>95%	>=90%	<90%

S/N	Incident-type	Response SLA	Resolution	Fail-over
1	Functional	2 hours	4 hours	+30 minutes
2	Performance	30 minutes	2 hours	+30 minutes
3	Systemic	15 minutes	30 minutes	+30 minutes

8.3 BUSINESS CONTINUITY

8.4.1 APs/ACs are required to maintain a Business Continuity Plan (BCP) that includes quarterly failover exercises and review of processes. Plans shall indicate the architecture of the Online Transaction Processing (OLTP) and Online Analytical Processing (OLAP infrastructure, physical and logical redundancies, replication intervals, processes for failover and fail-back, responsible individuals and/or roles and trigger events.

8.4.2 The threshold for failover and fail-back procedures is 30 minutes of downtime.

8.4.3 APs/ACs shall provide sufficient redundancies and fail-safe/recovery procedures to match their SLAs. The gaps and level of risk in providing redundancy may be estimated by considering:

i. Possibility of in-flight data loss and if such losses occur, the viability of recovery procedures to maintain integrity

ii. If replication is employed to maintain redundant processing infrastructure,

a. the replication time-lag between OLTP systems and on the average, the nature and quantity of data processed in that timeframe; and

b. the replication time-lag from OLTP to OLAP systems.

8.4 PROBLEM MANAGEMENT

This refers to management of incidents known to be recurring or which are not resolved within the window of the SLAs.

8.5.1 Problem Register

8.5.1.1. Problem Register Content

APs/ACs shall maintain a problem register which at a minimum is required to indicate:

i. The date/time a problem was discovered;

ii. Characteristics of the problem such as system symptoms and impact;

iii. Any interim measures that have been applied to manage the problem while keeping the system operational;

iv. Documented plans for a resolution or description of the intended solution;

v. Deployment date – date of implementation of changes to the system; and

vi. Review and problem resolution date.

8.5.1.2 PROBLEM REGISTER REQUIREMENTS

8.5.1.2.1 The problem register shall be:

i. Made available to Regulators, Auditors, Risk and Control teams within the organization; and

ii. Provided in reports to ACs according to schedule stipulated in (section 8.8 Reporting) of this Guidelines.

8.5.1.2.2 The Problem Management system shall be:

i. Electronic, or cloud-based and on no account should it be paper-based; and

ii. Auditable and trackable with unique references.

8.5 INTERFACE REQUIREMENTS

Interface requirements between APs and ACs shall be as follows:

i. The integration and communication interfaces between an AP and AC shall be 100% electronic using a system of API taxonomy as defined by the API guidelines within the CBN open banking framework

ii. The software architectural style shall be Representational state transfer (REST) while the data interchange format shall be JavaScript Object Notation (JSON)

iii. In order to be compatible with evolving global financial standard, the data standard for financial transactions shall be model based on ISO 20022 or any other applicable minimum standards.

8.6 CHANGE MANAGEMENT

APs/ACs shall collate change requirements and plan the changes for the next month except in cases where the change is expected to resolve a critical incident or problem.

All changes, either pre-empted or responsive, shall be:

i. Reported with sufficient details;

ii. Accompanied with notifications to stakeholders that could be affected by the change;

a. 24 hours before the intended change;

b. 1 hour before the intended change;

c. Immediately the change has been completed and services have been confirmed restored;

d. 30 minutes after the change should have been completed but has been prolonged or the change failed;

e. At the point of commencing a change rollback; and

f. When services have been restored.

8.6.1 COMMUNICATION MANAGEMENT

APs/ACs shall provide or prescribe secure real-time communication platforms for first level incident responders within their organizations and respective ACs/APs for incident notification, investigation, and resolution.

The platform shall be required to accommodate text, voice, and video conferencing modes of communication to support various scenarios.

In addition, formal channels (such as help and support systems or ticketing solutions) shall be used for incident reporting and management.

For the avoidance of doubt, emails are not a sufficient method of incident management for the Open Banking system.

8.7 REPORTING

8.8.1 API CONSUMER REPORTS

APs and ACs shall provide monthly reports to respective ACs/APs indicating:

i. API Performance levels for the month and previous Fiscal Year months or previous quarter;

ii. Metrics grouped into the following three API categories: Registration, Meta-Data and Transact APIs;

iii. Statistics of incidents/problems, SLA compliance and aggregate impact in downtime or loss of service;

iv. Number and category of Fraud and Disputes with accompanying SLA performance;

v. Excerpts of the problem register indicating new, existing and resolved problems;

vi. Changes made, reason (in sufficient detail), timing and estimated impact; and

vii. Changes scheduled for the next month and potential impact.

8.8.2 CUSTOMER REPORTS

Information on the use of customer-permission data shall be accessible to respective APs/ACs. APs/ACs are required to provide the following to customers that have subscribed to one or more ACs:

i. Notification of an AC accessing the customer's account(s)/wallet(s) in real-time or near-time via email, SMS or in-app prompts;

ii. A transcript of AC's activities on the use of customer-permissioned data shall be provided to the customers at the minimum every month or for a period less than a month as may be requested by a customer;

iii. A transcript of each AC's activities against the customer's account/wallet for at least the last 30 days. Transcript shall show the;

   a. transaction carried out,

   b. interface or channel signature

   c. time and status of each transaction showing request and response pairs; and

   d. any associated financial movements

iv. Appropriate distinctions in account statement records of AC-related activity versus normal account activities outside of Open Banking arrangements.

8.8 ANTI-COMPETITION PRACTICES

i. No AP/AC shall be allowed to engage in unethical and unprofessional practice such as de-marketing. Participants shall therefore be mandated to adhere to Section 2.0 of the provisions of the Code of Conduct in the Nigerian Banking Industry

ii. Where a participant needs to terminate a relationship, 20 business days' notice shall be given to the other participant(s)

iii. Where a disconnection is instant, due to fraud, abuse of services or by an instruction from the CBN, APs shall ensure that the AC is provided with a report justifying the disconnection within 2 business days.

9.0 DATA AND INFORMATION TREATMENT

9.1 DATA ETHICS

A Data Governance policy shall be approved by a Committee of the Board of Directors or at a minimum an Executive Management Committee of the AP/AC.

The policy shall ensure that all aspects of the data is well managed and fulfil legal and regulatory requirements.

The AP/AC shall incorporate the following into its Data governance policy, procedures and mechanisms:

i. Have a clear approach to collection, collation, analysis, sharing, storage and retrieval of customer data in line with extant Laws and Regulations;

ii. How the data interplays with the algorithmic system and models, regarding how data is weighted or attributed in the algorithmic system to produce the outcomes;

iii. Impact the combination of the data and the algorithmic system has on results;

iv. Intended outcomes of the data-driven service on customers and society; and

v. Unintended consequences of the service on customers and society.

9.1.1 DATA ETHICS FRAMEWORK

APs/ACs are required to have a data ethics framework in place.

The data ethics framework shall:

i. provide principles for the acquisition, collection, collation, analysis, use, and sharing of personal data;

ii. provide for a consistent process and document procedures to guide documentation, verification and decision making to ensure data processing activities:

    a. Comply with extant laws and regulations

    b. Generate fair and accurate reports for both the customers and society

9.2 DATA PRIVACY

APs/ACs shall comply with the Nigerian Data Protection Regulation or any CBN issued data protection regulation for FIs, to protect customer data.

9.3 INFORMATION SECURITY

To protect the confidentiality, integrity and availability of information and data in the open banking system, all participants shall implement Information Security controls in line with the Security Standards (Appendix III).

9.3.1 EFFECTIVE INFORMATION SECURITY MANAGEMENT

APs/ACs shall:

i. Develop, maintain, and implement an Information Security Policy, ensuring adequate resources, processes, technology, people and budget are allocated;

ii. Complete regular threat assessments;

iii. Allocate accountability to a nominated board member to oversee risks;

iv. Implement strong passwords and access management controls applying multi-factor authentication;

v. Routinely vet all staff, suppliers and service providers thoroughly;

vi. Establish a strong security awareness culture;

vii. Implement and run a dedicated security operations centre;

viii. Ensure strong IT systems controls;

ix. Ensure information security requirements are clearly stated in all contracts with suppliers;

x. Regularly undertake assurance of third-party providers; and

xi. Create and regularly test an incident response plan.

9.3.2 PROTECTING AGAINST DATA BREACH

APs/ACs shall:

i. Implement strong password and access controls;

ii. Ensure secret credentials remain secret at all times;

iii. Classify data assets appropriately according to risk, threat likelihood and sensitivity distinguishing between personal data and other classified/confidential data;

iv. Manage and monitor access to data, and review access quarterly;

v. Use strong authentication to manage access to data systems and role-based access for individual data sets;

vi. Train staff appropriately and frequently;

vii. Restrict the ability to download and store data via portable/removable media;

viii. Assess new applications, processes or services from a security perspective before implementation;

ix. Implement production level controls for production data used in non-production environment;

x. Ensure a secure break-glass process for emergency access to production data;

xi. Have a clear and documented data retention and destruction policy in line with extant laws and regulations; and

xii. Know your digital footprint and apply appropriate controls.

9.3.3 DATA BREACH POLICY

9.3.3.1 DATA BREACH POLICY DEVELOPMENT

APs/ACs shall create a data breach policy and operate as follows:

i. **Prevent:**

Operate regular risk assessment and risk monitoring in order to anticipate potential data threats, hazards and impacts.

ii. **Prepare:**

Ensure that the procedures for managing data incidents are clearly set out, together with clear roles and responsibilities, lines of escalation and communication for all parties involved in risk management procedures.

iii. **Assess:**

Assess each data incident according to its impact in order to determine a proportionate response and trigger the most appropriate command and control arrangements.

iv. **Contain:**

Activate the relevant processes and procedures to limit the impact of the incident.

v. **Communicate:**

Ensure that all relevant parties receive efficient, regular and timely communication in the event of a data incident.

vi. **Review:**

Conduct a robust analysis of the underlying cause of the incident, the efficacy of the incident response, the lessons learned, and the actions required to prevent future similar incidents.

vii. **Recover:**

Start the recovery process to ensure minimal disruption to service delivery.

viii. **Test:**

Regularly test adherence to the Incident Management Policy and associated Incident Management Procedures to ensure their adequacy and effectiveness.

9.3.3.2 TECHNICAL SECURITY

APs/ACs shall comply with the Technical Security Standards as provided in the Security Standards (Appendix III)

9.3.3.3 CYBERSECURITY

APs/ACs shall ensure the following:

i. Entrench an appropriate risk management regime;

ii. Have a secure configuration management system;

iii. Ensure network security for all connections;

iv. Ensure appropriate management of access rights and user privileges;

v. Conduct user education and awareness;

vi. Deploy malware prevention and detection tools;

vii. Implement system monitoring to detect actual or attempted attacks on systems and business services; and

viii. Restrict use of removable/portable storage media.

9.4 RENDITION OF RETURNS

ACs and APs shall render the following periodic returns to CBN using existing channels as specified by the Bank:

i. Volume of transactions

ii. Value of transactions

iii. Number of users

iv. Success rates

v. Failure rates

vi. Security incidents

vii. Fraud incidents

viii. Downtime reports

ix. Any other requirements as the CBN shall determine from time to time.

9.5 ANTI-MONEY LAUNDERING (AML) AND COMBATING THE FINANCING OF TERRORISM (CFT)

APs/ACs shall comply with the extant Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) in Banks and Other Financial Institutions in Nigeria Regulation.

9.6 TESTING

The Bank shall oversee testing procedures in the open banking ecosystem, while APs/ACs shall provide appropriate facilities for testing, both at initial launch and through subsequent changes.

9.7 BUSINESS CONTINUITY AND DISASTER RECOVERY

APs/ACs shall develop and implement Business Continuity Plan (BCP) and Disaster Recovery Plans (DRP). The plans shall be tested every six months.

9.7.1 BUSINESS CONTINUITY PLAN

The BCP shall:

i. identify a designated alternative site, critical roles, critical systems and access requirements, and a communication strategy for staff, external suppliers and other stakeholders;

ii. designate an alternate site with adequate facilities, or remote working arrangement, for individuals to perform their roles seamlessly; and

iii. specify protocol for call cascades, text messages or a simple call recording to notify staff to relocate to alternate site.

9.7.2 DISASTER RECOVERY

APs/ACs shall develop Disaster Recovery Plans, in the BCP or stand-alone.

10.0 CHANGE AND COMMUNICATION MANAGEMENT

10.1 INTRODUCTION OF CHANGE

APs/ACs shall notify its respective ACs/APs prior to the introduction of changes or updates to any component of relevant systems or platforms, regardless of whether these are major, minor or patch updates. Emergency changes by APs/ACs may be allowed (e.g. for reported security issues) without any such notice.

a. All emergency changes shall be communicated to the respective APs/ACs within 24 hours of the change.

b. APs/ACs shall ensure that thorough and effective testing of changes, updates, or patches are done using the test facilities.

10.1.1 VERSIONING OF PUBLISHED API STANDARDS

Types of release and version numbering:

Release type	Description	Version numbering
Major	Significant breaking changes – which may require substantial implementation effort for APs/ACs and will cause existing applications to fail) until respective ACs/APs also implement changes.	v1.0.0, v2.0.0, etc
Minor	Minor breaking changes – may require some implementation effort for APs/ACs and will cause existing applications to fail until ACs/APs also implement change.	v1.1.0, v1.2.0, etc
Patch	Can include any non-breaking change, as well as errata and clarifications, which will not force ACs/APs to implement any changes.	v1.1.1, v1.1.2, etc
Release Candidate	Pre-release versions of any forthcoming patch, minor or major release. To enable the Bank (or designated entity) to publish regular updates based on review and feedback.	v1.0.0-rc1, v1.0.0-rc2, etc

11.0 SHARED INFORMATION FRAMEWORK

11.1 INFORMATION SHARING

APs shall only share information of a customer with an AC, upon presentation of a valid proof of consent by the customer, and shall authenticate such consent to ensure it emanates from its customer.

Authentication of end-users and the validation of information to be shared with the ACs shall be done directly by the AP using the prescribed authentication mechanism within the API Security and Risk Management Standards.

For consent obtained from a customer to be valid, the following information shall be presented to the customer by the AC:

i. Full and legal name of the AC;

ii. Shortened or brand name of the AC in situations where the AC operates under a different name from its legal registered name;

iii. The accreditation/registration number or other valid means of identification in the open banking registry;

iv. The business registration number of the AC with the Corporate Affairs Commission (CAC);

v. Compliance with access level to data by service category;

vi. Nature of request, which shall be explicit and describing the following:

   a. The type of access the AC shall have on the customer account in line with access level by data and service category;

   b. Duration/tenor of the consent or the date when the access shall be invalidated;

   c. Frequency of access to the customer information by the AC or if such access shall be one-off; and

   d. If the request includes the customer's consent to collect data for anonymous/de-identified data analysis;

vii. Information regarding the process for withdrawal of consent by the customer including the following;

   a. A statement that the customers can withdraw their consent at any point in time if so desired;

b. Detailed process for withdrawal of consent by the customer;

c. Information on the consequences of withdrawal of such consent to the customer, if any.

viii. Information about redundant data including the following touchpoints;

a. ACs general policy in relation to decision making on the deletion or de-identification of redundant data in accordance with extant laws and regulations;

b. An outline of the customer's rights to elect for deletion of their redundant data and information on how to exercise such rights.

11.1.1 INFORMATION SHARING WITH OTHER SERVICE PROVIDERS

If the customer's data will be disclosed to an outsourced service provider including non-Nigerian participants, the approval of the Bank shall be obtained, and the following additional information shall be required:

a. A statement indicating that the data would be used or disclosed in such manner;

b. Sufficient information about the data handling/privacy policy of the service provider; and

c. A guarantee that the customer can obtain further information about such disclosures from the policy or on request to the participant, if they so wish.

11.2 VERIFICATION OBLIGATION

When the AP receives customer's consent to provide customer's data to an AC, it shall verify that:

i. the consent emanated from its customer: This shall require Two Factor Authentication (2FA) of the customer to verify the consent.

ii. the request for customer's data contains the purpose of the request.

iii. the request contains the credentials of the requesting AC.

iv. the request contains a valid date and was made through appropriate channels.

11.3 DIGITAL SIGNATURES

i. Upon due verification, the AP shall create a token which shall reflect the details of the rights granted to the AC by the customer.

ii. The token shall be encrypted and securely exchanged with the AC.

iii. All responses of the AP shall be in real-time.

iv. For every API call made to read a customer's information or conduct transactions on the customer's account, the AP shall validate the token to ensure that it continues to meet the rights granted by the customer.

11.4 ENABLING DATA FLOWS

To enable these data flows, the APs shall:

i. Implement interfaces that will facilitate submission and authentication of consent information through encrypted mechanism;

ii. Adopt means to verify the consent in accordance with the verification obligations contained in this Guidelines, including digital signatures, contained in the consent information;

iii. Use certified electronic signature provider to authenticate the validity of the customers consent;

iv. Digitally sign the customers' financial information being shared; and

v. Maintain log of all information sharing requests and the actions performed pursuant to such requests and submit same to the customer.

11.5 RISK ASSESSMENT REPORTING FOR REGISTERED PARTICIPANTS

The following risk assessment reporting standard shall apply to registered participants:

i. A regular reporting mechanism shall be established, to ensure that APs and ACs provide the competent authorities, on a regular basis, with an updated assessment of security risks and the measures taken;

ii. Application for authorisation or accreditation of payment institutions shall be accompanied by a description of the procedure to monitor, handle and follow up on security incident and security-related customer complaints, including incident reporting mechanism;

iii. There shall be a risk management framework specifying:

   a. Technology risk management framework;

   b. System security, reliability, resiliency, and recoverability; and

   c. Strong authentication to protect access to customer data and systems.

11.6 RISK MANAGEMENT COMMITTEE

Participants shall have a risk management committee of at least three members of senior management cadre. The responsibility shall include;

i. Periodic consideration of factors such as reputation, customer protection, legal issues, controls, and security measures for computer systems, networks, data centres, operations and backup facilities

ii. Exercising oversight of technology risks and ensure that the organization's IT function is capable of supporting its business strategies and objectives

iii. Development of risk management reports.

11.7 CYBERSECURITY BREACH INCIDENT REPORTING

i. Participants shall:

   a. Implement appropriate security measures;

   b. Establish incident management procedures;

   c. Report major security incidents without undue delay to the competent authorities;

ii. The security incidents reporting obligations should be without prejudice to other incident reporting obligations laid down in other regulations including the CBN Risk-Based Cybersecurity Framework;

iii. In the case of a major operational or security incident, participants shall:

   a. Without undue delay, notify the CBN and other relevant stakeholders, of the incident and remediating measures; and

   b. Upon receipt of the notification, the CBN and other stakeholders shall assess the incident with respect to the ecosystem and where appropriate, take necessary measures to protect safety and stability of the financial system.

11.8 INCIDENT REPORTING PORTAL

i. An incident reporting portal shall be introduced to enable easy and fast reporting by participants in the ecosystem.

ii. Reportable incidents under this heading shall include incidents that;

   a. Affect participants, operations, and the systems; and

   b. Any other incident as may be determined by the CBN through relevant regulations and guidelines.

11.9 DATA BREACH POLICY AND PROCEDURE

i. APs/ACs shall develop and implement a data breach policy and procedure as part of information security management system to;

   a. Carry out regular risk assessment and monitoring;

b. Ensure that the procedures for managing data incidents are clearly set out;

c. Assess the impact of each data incident;

d. Activate the relevant processes and procedures to limit the impact of the incident;

e. Adopt a three-line defence model into its business standard policies and procedure for risk management and compliance;

f. Ensure that all relevant parties receive efficient, regular, and timely communication in the event of a data incident;

g. Start the recovery process promptly to ensure minimal disruption to service delivery;

h. Conduct a robust analysis of the underlying cause of the incident, the efficacy of the incident response, the lessons learned, and the actions required to prevent future similar incidents; and

i. Regularly test adherence to the incident management policy and associated incident management procedures to ensure their adequacy and effectiveness.

11.10 DATA INCIDENT MANAGEMENT PROCEDURE

i. APs/ACs and other registered participants shall develop an Incident Management Procedure that includes Data Incidents which shall be adhered to in all case.

ii. The Data Incident Management Procedure must apply to and shall be followed by all workers, in any capacity, including employees, contractors, directors, external consultants, third party representatives, business partners, etc.

iii. The Data Incident Management Procedure shall run concurrently as follows:

a. Identification/logging of the data incident including initial alert, triggering a potential incident etc.

b. Management team including Legal, privacy compliance officer and other management executives are made aware and convened

c. Management team conduct impact assessment and commence mitigating actions for resolution

d. Incident resolution

e. Closure and return to business as usual

f. Post incident review.

11.11 REVALIDATION OF AGREEMENTS

Participants shall be required to revalidate their SLAs as stated in the agreement.

11.12 INTELLECTUAL PROPERTY PRESERVATION

11.12.1 INTELLECTUAL PROPERTY RIGHTS

Participants' intellectual property in proprietary and protectable software source and object codes, aggregate data, and aggregate services among other protectable information shall be protected under the applicable laws in Nigeria.

11.12.2 TRANSFER OF INTELLECTUAL PROPERTY RIGHTS

No Party shall unlawfully acquire any proprietary rights, title, or interest in or to any Intellectual Property Rights of another Party or any other Participant pursuant to the participation in Open Banking in Nigeria.

11.12.3 OWNERSHIP AND USE OF OPEN DATA AND OTHER INFORMATION

All ownership rights in any open data or other information shall at all times remain with the Party or Participant from which such open data or other information originated whether the open data or other information is in human or machine-readable form.

11.12.4 LICENSED USE OF DATA

Participants shall be allowed to grant royalty free license for their intellectual property in aggregated data, subject to the satisfaction of the consent requirement, for use by other participants to such extent as may be required for Open Banking in Nigeria.

12.0 DISPUTE RESOLUTION

For Open Banking arrangement, the financial industry dispute resolution process shall be applicable.

Participants shall abide by the dispute resolution mechanism laid down under "Liability Management, Customer Complaint and Redress Management" of the Customer Experience Standards (Appendix IV) as well as the CBN Consumer Protection Framework.

The Bank shall approve appropriate liability models and redress mechanisms, (such as insurance, collateral requirements, pool industry funds etc.) for participants.

APPENDIX 1 – API STANDARDS

1.0 Identification and Categorization of APIs

Microsoft Excel Worksheet

Click on link to access the information: API Identification: Categorisation and Risk Matrix

2.0 Voluntary/Involuntary API Implementation

Microsoft Excel Worksheet

Click on link to access the information: API Identification: Voluntary and Involuntary Implementations

3.0 Technical Considerations

Standard Areas	Sub Items
Protocol	• Protocol: SSL, HTTPS, OAuth2.0
Messaging	• Architectural Style: REST • Messaging: JSON, ISO 20022
Security	• Throttling/Rate Limiting • Message Signing & Encryption • Token Format and Expiry: JWT • METHOD Access and Control • Global Runtime Policies
Integrity	• Idempotency • Non-Repudiation
Experience	• Headers • Status Codes • HTTP Status Codes • Pagination • Resource URI Convention • Developer Onboarding
Data	• Archiving • Analytics

3.1 Consent Management

Consent Management is to provide guidelines on managing and sharing customer data in respect to the customer consent, data access control, data classification and Technical API operations.

3.2 Consent Management Stages

Consent management shall be divided into the following:

i. **Consent Stage**

a. The customer shall be informed of type and purpose of data requested, terms and conditions applicable, in concise and easy to understand manner

b. The consent shall be explicit

c. The customer shall be presented with the option to accept or decline onboarding into the Open Banking arrangement

d. In the consent stage, customer shall be shown the requested information and purpose

e. The consent provided shall be time-bound, not in perpetuity

f. A customer shall be allowed to explicitly opt-out, which shall be provided to customer periodically in line with the provisions of this guideline

g. A customer after providing consent, shall be accurately informed of the time-bound permission provided.

ii. **Authentication Stage**

a. Authentication shall provide a mechanism to verify user identity to the APs.

b. APs shall provide authentication mechanisms in acceptable form that conform in principle and architecture to the following requirements for authentication:

i. **Authentication must happen over pre-authorized channels** (such as email, phone numbers, devices, applications, biometrics etc)

ii. **User endpoint should be verified prior to use for authentication** (emails, phone numbers or other user endpoints shall be verified using control information such as OTP verification prior to being used as a platform for Open Banking consent).

c. Appropriate customer authentication methods such as multi-factor authentication shall be established to reduce the chance of identity theft or fraud.

Following consent by customers, APs/ACs shall activate authentication mechanisms to ensure the security of the customer's data.

iii. **Authorisation Stage**

a. Authorisation shall be the process by which customers consent is obtained for ACs to access their data with APs;

b. The following are guidelines for authorisation:

i. ACs shall provide mechanisms for customer to **immediately** enable or revoke permissions to different particulars of each account;

ii. Each change in the user's selection shall be proceeded with the generation of a new OAuth token to capture the change in scope;

iii. When prompting users for consent on the application, details shall be grouped for ease of presentation;

iv. Sufficient information in the confirmation screen shall capture or make available the details involved;

v. Details shall be presented in friendly and easily understandable language that embodies the object, action, initiator (user or auto) and periodicity;

vi. Notifications shall be provided, using agreed channels, to customers indicating any changes to permissions requested against AP for the user's keepsake;

vii. The customer shall be presented with the details about the consent required on the AC-user interface;

viii. The customer is presented with the options to allow or deny the request from participants to access the shown data;

ix. The response from the end-user is then sent to the AP, and the data must be recorded accordingly;

x. Participant shall provide a minimum of two (2) channels by which the end-user can view, consent, decline or revoke permission requests;

xi. When consent is given by the end-user for specific permissions, the records of such consent shall be recorded along with a timestamp, an audit record capturing a transcript of the change in permissions scope and the point of initiation;

xii. Revocations shall be captured with a timestamp, an audit record capturing a transcript of the change in permissions scope and the point of initiation;

xiii. Consented scopes shall be updated within the AP's API-directory;

xiv. Subsequent token requests by the ACs on behalf of the user shall include consented scopes; and

xv. The AP may provide additional services to notify the AC of the approved scopes so the AC can proactively enable those functions within the customer's profile instead of waiting for the next sign-on event.

3.3 Data Classification

3.3.1 Customer-Biodata/ BVN Data

Customers personal data shall include at the minimum, the following:

Data	**Description**
FirstName	User first name
Middle Name	User middle name (other names)
Last Name	User last name (Surname)
Contact Address	User contact address
Date of birth	User date of birth
State of Residence	User's state of residence
NIN	User National Identity Number
BVN	User's Bank Verification Number
Email Address	User's email address
Phone Number	User's mobile phone number

3.3.2 Account Details

Customer's account or wallet data shall include at the minimum, the following:

Data	Description
Account Number	Account identification
Currency	Bank account currency
Status	Account status e.g., dormant, active, etc.
Created Date	Date account was created
Account Name	Account name on the bank account
Account Type	Type of account e.g., Savings, Current, etc.
Balance*	Account balance
BVN	Bank verification number
Bank of Name	Account holder's bank, e.g., FirstBank, Zenith

3.3.3 Transaction-History

This shall be the transaction history of a particular customers' account based on date range.

3.3.4 Debit-Mandate

This shall be a mandate signed by the customer physically or electronically to participate in open banking.

4.0 API Operations

i. Request Consent

Request Attributes	Response Attributes
TPP-Id Consent-Type Expiry-Date Customer-Id Data-Source-Id	Consent-Id Response-Code Response-Message

The Consent-Id is expected to be part of the request payload to retrieve consent.
Consent types: Biodata, Transaction History, Debit mandate, Account details

ii. Retrieve Consent

Request Attributes	Response Attributes
TPP-Id Consent-Id Data-Source-Id	Consent-Type Expiry-Date Customer-Id Data-Source-Id Response-Code Response-Message Consent-Id

iii. Cancel-Consent.

Request Attributes	Response Attributes
TPP-Id Consent-Id Data-Source-Id	Response-Code Response-Message

iv. Create-Debit-mandate

Request Attributes	Response Attributes
TPP-Id Customer-Name BVN Bank-Code Account-No Description Duration Mandate-Type	ResponseCode ResponseMessage Mandate-Id

v. Retrieve-Mandate

Request Attributes	Response Attributes
TPP-Id Mandate-Id	TPP-Id Mandate-Id Customer-Name BVN Bank-Code Account-No Description Duration Mandate-Type ResponseCode ResponseMessage

vi. Delete-Mandate

Request Attributes	Response Attributes
TPP-Id Mandate-Id Data-Source-Id	Response-Code Response-Message

5.0 Conclusion on Consent Management

Participants in open banking shall strictly adhere to Appendix III (Security Standards) of this Guidelines or as may be updated from time to time.

APPENDIX II – RISK MANAGEMENT

1.0 Introduction

Open banking promotes innovations and broadens financial products and services, which involves sharing of customer data and inter-connectivity of systems, therefore, exposing the participants to risks such as cybersecurity, money laundering, regulatory and compliance, contract management, product management, etc. Open banking offers great benefits and opportunities to the financial sector but is accompanied with risks that could undermine the objectives if not properly managed.

It is important that these risks are properly identified and managed for the safety of the participants and soundness of the financial system.

This Guidelines provides for the management of risks associated with open banking in Nigeria.

2.0 Risks Associated with Open Banking

The basic risks in open banking include cybersecurity, data privacy and integrity, contract management, product management, money laundering, regulatory and compliance.

At the minimum, participants shall address all identified risks, by developing and implementing effective risk management frameworks, policies and procedures for open banking, approved by the Board of Directors, as well as institute a culture of sound corporate governance.

2.1 Cyber-Security Risk

Cybersecurity risks arise from the use of APIs for interconnectivity between participants. APIs potentially expose the financial system to more vulnerabilities due to sharing of data and connections.

i. Participants shall comply with the extant Risk-Based Cyber-Security Framework and Guidelines for Deposit Money Banks and Payments Service Providers, as well as Cyber-Security Framework and Guidelines for Other Financial Institutions.

These Guidelines established minimum standards for managing cyber-security risks

ii. Participants shall comply with the requirements of ISO 27001 standard (Information Security Management Standard)

iii. Participants shall comply with other standards and requirements determined by the Bank.

2.2 Third Party Risk

Third Party risk is associated with possible losses arising from the non-fulfilment of the terms of contract or the contract performing poorly. Participants shall have a duly executed Service Level Agreements for all third-party contracts.

i. Participants shall, at the minimum:

   a. Adopt/implement a regulatory risk framework;

   b. Adopt comprehensive internal controls, including adequate policies, procedures, and limits;

   c. Acquire insurance policy to cover losses;

   d. Ensure that all third parties are registered with stipulated risk control requirements related to customers consent to access data and use of the data; and

   e. Ensure that contractual agreements are established between participants before accessing customer permissioned data.

2.3 Money Laundering Risk

This is the likelihood or probability that a participant will knowingly or unwittingly engage in money laundering or financing of terrorism. Money laundering is the act of directly or indirectly concealing or disguising any fund or property that is derived from the proceeds of an unlawful activity, with the aim of making the illicit funds seem to have been proceeds of legitimate activities.

Open APIs creates new areas of vulnerability for participants as a result of interconnectivity, giving rise to a large number of financial players and eases cross-border transactions, which makes the monitoring of transactions more complex.

i. Participants shall, at the minimum:

   a. Implement an effective Know Your Customer/Continuous Due Diligence policy (KYC/CDD);

b. Adopt AML/CFT due diligence; and

c. Adopt sound risk management practices.

2.4 Regulatory and Compliance Risk

Regulatory and Compliance risk is the risk arising from violations of laws, rules or regulations, or from non-compliance with internal policies or procedures or with the participant's business standards. This risk exists when the products or services of a third party are inconsistent with governing laws, rules, regulations, policies or ethical standards.

i. Participants shall comply with all CBN regulations relating to open banking and ensure that third-party service providers also comply.

ii. Participants, shall at the minimum:

   a. Adopt/implement a regulatory risk framework;

   b. Adopt comprehensive internal controls, including adequate policies, procedures, and limits;

   c. Insurance policy to cover losses;

   d. Have a dedicated compliance officer; and

   e. Develop compliance policy/manual.

2.5 Data Integrity Risk

This is the risk that data stored and processed by information technology systems are incomplete, inaccurate or inconsistent across different IT systems. Participants shall put measures in place to guarantee integrity and availability of data.

i. Participants, shall at the minimum:

a) Implement full audit trail of all transactions

b) Implement access rules, approvals, revocations and review procedures

c) Data shall follow standards such as the 9 ALCOA+ principle of Attributable, Legible, Contemporaneous, Original, and Accurate, Complete, Consistent, Enduring, and Available.

2.6 Data Privacy Risk

This is the risk of unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.

i. Participants shall put measures in place to guarantee confidentiality of data and comply with extant laws and regulations on data protection and privacy;

ii. Participants, shall at the minimum, implement:

   a. A robust ISMS to ensure sensitive data are systematically managed;

   b. A Data loss prevention (DLP) procedure;

   c. Encryption and pseudonymization procedure;

   d. Identity and access management (IDAM) procedure;

   e. The creation of a dispute resolution mechanism/body specific to open banking including customer liability framework;

   f. Know your data;

   g. Separation of duties within participants on access to customer data. 2 level accessibility to customer data;

   h. An adherence to information security standards and data protection regulations; and

   i. Development of technology standards for participants in open banking ecosystem.

2.7 Product Management Risk

Open Banking creates the potential for proliferation of innovative products and services which may increase the complexity of financial services delivery, thus, making it difficult to control operational risk, information security, money laundering etc.

i. Participants shall ensure that:

   a. all products are approved by the regulator;

   b. risks associated with the products are identified and risk mitigants are put in place; and

   c. the benefits to the customers are known.

3.0 Risk Management Requirements

Risk Management requirements for participants shall depend on their risk management maturity (RM) level as stipulated in Section 5.1 of the Regulatory Framework for Open Banking in Nigeria.

i. Tier 0 (Product Information Service Touchpoint - PIST)

Sponsors shall ensure that Tier 0 participants, at the minimum, have competence and capacity to carry out the activity, and provide evidence of good risk management practices.

ii. Tier 1 (Market Insight Transactions - MIT)

Sponsors shall ensure that Tier 0 participants, at the minimum have competence and capacity to carry out the activity. The sponsor shall also ensure that Tier 1 participants have adequate corporate governance, risk management policies and procedures to ensure that risks that can potentially affect the services provided are adequately and effectively managed.

iii. Tier 2 (Personal Information and Financial Transaction (PIFT)

Tier 2 participants, shall at the minimum, ensure:

a. Adequate corporate governance, risk management policies and procedures to ensure that risks that can potentially affect the services provided are adequately and effectively managed. These shall cover, but are not limited to; customer consent, data protection audit, cyber-defence, data protection impact assessment, privacy policy notices, data protection trainings etc;

b. Operational competence and professional experience of key personnel;

c. Adequate internal control environment and insurance coverage;

d. Procedures and processes for communicating and consulting with its stakeholders on key issues that can affect its service delivery are in place;

e. Policies, procedures and governance arrangements for technology planning to ensure that technologies that can affect the delivery of service are properly managed;

f. Processes and evidence of periodic background checks on its employees and vendors, particularly those that would have access to the participants applications/systems are in place;

g. Information security framework, policies and processes to ensure the confidentiality, integrity and availability of the participants' information assets. These shall include, but not limited to; identity and access management, encryption and pseudonymization, data loss prevention, etc; and

h. Business continuity management and disaster recovery policies, procedures and plans are in place.

iv. Tier 3 Profile, Analytics and Scoring Transaction (PAST)

Tier 3 participants shall, at the minimum, ensure:

a. The establishment of corporate governance as well as risk management policies and procedures to ensure that risks that can affect the services provided are adequately and effectively managed. These shall include, but not limited to; customer consent, data protection audit, cyber-defence, data protection impact assessment, privacy policy notices, data protection trainings etc;

b. Information security framework, policies and processes to ensure the confidentiality, integrity and availability of the participants information assets. These shall include, but not limited to; identity and access management, encryption & pseudonymization, data loss prevention, etc;

c. Business continuity management and disaster recovery policies, procedures and plans;

d. Policies, procedures and governance arrangements for technology planning to ensure that technologies that can affect the participants' service delivery are properly managed;

e. Procedures and processes for communicating and consulting with stakeholders on key issues that can affect service delivery;

f. Operational competence and professional experience of key personnel;

g. Adequate internal control environment and insurance coverage; and

h. Processes and evidence of periodic background checks on employees and vendors, particularly those that would have access to the participants applications/systems.

APPENDIX III – SECURITY STANDARDS

1.0 Introduction

This section defines the minimum-security requirements for open banking operation in Nigeria covering information security and privacy controls.

2.0 Principles

Participants shall comply with minimum security principles such as are encapsulated in the US NIST CSRC.

a. **Layered security** is a principle that security controls are layered to reduce the security risk.

b. **Separation of duties** is a principle that no user should be given enough privileges to misuse the system on their own.

c. **Least privilege** is a principle that restricts the access privileges of authorized personnel (e.g., program execution privileges, file modification privileges) to the minimum necessary to perform their jobs.

d. **Zero trust** is a principle that security design that assumes asset compromise to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services.

e. **Dual control** is a principle that uses two or more separate entities operating in concert to protect sensitive functions or information.

f. **Need to know** is a principle that ensures that only authorised recipients are provided access to specific classified information to perform or assist in a lawful and authorized function.

g. **Privacy** is a principle of the right of a party to maintain control and confidentiality of information about itself.

3.0 Administrative Security Specifications

i. Governance

Participants shall:

a. Ensure compliance with the provisions of the extant CBN Risk-based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers and CBN Risk-based Cybersecurity Framework and Guidelines for Other Financial Institutions (OFIs).

b. Develop, maintain, and implement security policies that ensure authorised and secure connection and disconnection of APIs.

ii. Risk Management

Participants shall adopt practices as defined in Appendix II (Risk Management).

iii. Compliance and Audit

All compliance requirements shall be identified, assessed, documented, and monitored. At a minimum, this shall cover the following: data flow, data privacy, internal controls, reporting, regulations, intellectual property, health, and safety.

Participants shall:

a) Regularly evaluate organizational policies, standards, procedures, and methodologies in all functions to ensure compliance with relevant legal and regulatory requirements

b) Implement performance metrics to enable review and monitoring of both the detailed status of changes and the overall state (for example, age analysis of change requests)

c) Ensure that status reports form an audit trail, so that changes can subsequently be tracked from inception to eventual disposition

d) Obtain objective third-party assessments, audit reports, quality assurance reviews and risk profile

e) Review identified gaps and remediate open banking security-related loss exposures.

iv. System Acquisition, Development and Maintenance

Participants shall ensure that procurement of open banking infrastructure comply with extant laws.

v. Supplier Management

Participants shall:

a) Be responsible for data protection shared and owned by third-party providers.

b) Enforce ownership for the protection of Personal Information and Financial Transaction (PIFT) and Profile, Analytics and Scoring Transaction (PAST) information through clearly documented contracts with service providers such as outsourced business processing, infrastructure, application development, shared services, etc.

c) Ensure change management processes with suppliers do not violate information security policies using contractual terms and Service Level Agreements (SLAs).

d) Ensure that each supplier directly and/or indirectly interacting with PIFT and PAST have documented evidence of implementing information security standards such as, ISO 27001 standard requirements or approved Information Security Management System (ISMS) accreditation.

vi. Personnel Security

Participants shall ensure that staff and other service providers pass periodic security checks.

vii. User Awareness

Participants shall:

a. Develop and maintain strong security awareness culture within and outside the organisation to include staff, customers and third parties.

b. Conduct periodic security awareness and simulations that tests employees and other service providers responses to relevant cyber threats.

4.0 Technical Security Specifications

i. Access Control

Participants shall implement zero-trust architecture.

ii. Roles and Responsibilities

Participants shall:

a) Maintain minimal user access rights in accordance with business function, process requirements and security policies.

b) Align the management of identities and access rights to the defined roles and responsibilities, based on least-privilege, need-to-have and need-to-know principles.

c) Ensure that access authentication to information assets shall be based on the individual's role or business rules.

d) Coordinate with business units that manage authentication within applications used in business processes to ensure that authentication controls have been properly administered.

iii. Identification

a. The Biometric Verification Number (BVN), National Identity Number (NIN) and Tax Identification Number and other such unique identifiers, shall be stored in independent identity systems.

b. Each endpoint accessing an open banking product and service shall be uniquely identified and its attributes examined for compliance of information security policies.

iv. Authentication

a. The process through which an end user authenticates itself to its service provider shall be designed to minimize digital friction.

b. Participants shall use strong authentication which includes Multi-Factor Authentication (MFA) to manage access to API systems and implement role-based access control for PIFT and PAST.

c. Participants shall adopt authentication protocols at the minimum, OAuth 2.0 in conjunction with OpenID Connect. Higher authentication protocols shall be implemented as required.

d. Mutual authentication over Transport Layer Security (mTLS) shall be implemented for authentication between client and server machines or any approved authentication standard.

v. Authorisation

Participants shall:

a. Implement open banking security profiles in compliance with the Financial-grade API (FAPI) specifications.

b. Implement digital tokens that ensures third party is acting within the bounds of the permissions granted.

c. Provide evidence that their third-party service is entitled to use an authorisation token such as providing client identity and client secret to provider.

d. Be responsible for identity token management and ensure that third-party providers are in possession of legitimate tokens.

e. Ensure that access granted to third-party providers are defined in terms of specific permissions to data and/or functionality.

f. Note that all malicious misuse of permissions is prohibited.

g. Document and implement the following:

    i. Customer revocation rights.

    ii. A mechanism through which users can review and cancel their permissions.

    iii. Assignment of risk levels to permissions.

    iv. Allow for prohibitions on granting permissions.

    v. Placement of contextual limits on permissions where appropriate (e.g., payment limits).

    vi. Subject permissions to time/duration limits.

    vii. Refresh and challenge permission token validity at specific intervals.

h. Define roles with appropriate permissions and be defined in a standardized nomenclature for future work.

vi. Identity propagation

Participants shall secure identities propagated across all channels and storage systems.

vii. Fraud

Participants shall:

a. Implement anti-fraud and counter terrorism financing controls and capabilities.

b. Ensure that the API provides supports out-of-band (OOB) authentication, where necessary;

c. Be required to notify the user asynchronously/OOB when significant actions have occurred such as, a change to a payee etc;

d. Ensure that the API responses inform the third-party and customer that an OOB process is underway so that, where appropriate; and

e. Ensure that fraud-relevant information, such as IP addresses and traffic information, in the API return messages are stored and investigated for research and development purposes.

5.0 Operations Security

Participants shall assign roles and responsibilities for identifying and monitoring any changes in legal, regulatory, and other external contractual requirements relevant to the use of IT resources and the processing of open banking information within the business and IT operations.

5.1 Malware Protection

All participants shall implement updated anti-malware and anti-ransomware solutions automatically or at least semi-automatically.

5.2 Data Loss Prevention

Participants shall:

a. Apply data classification and labelling techniques to protect sensitive data and information assets at rest, in motion and in use;

b. Protect personal and transactional data against data loss, theft and breach in line with regulations such as the Nigeria Data Protection Regulation (NDPR) and/or any data protection regulation issued by the Bank; and

c. Have and implement clearly defined data retention and destruction policy(ies) in line with CBN regulations, the Nigerian Data Protection Regulations, etc.

5.3 Information Security Incident Management

5.3.1 Incident management

Participants shall:

a. Integrate the planning, design, implementation and monitoring of information security and privacy procedures and other controls capable of enabling prompt detection, prevention of security events, and response to security incidents;

b. Ensure that cyber risks are thoroughly investigated, and root causes communicated with additional risk response requirements and process improvements to appropriate decision makers;

c. Implement corrective actions based on root causes such as problems with business process, application system development and maintenance, development and test environments, documentation and manuals, and data integrity;

d. Establish Cyber-Threat Intelligence (CTI) capability to detect, prevent, and respond to potential cyber-threats and risks, as well as develop relevant CTI policies; and

e. Report and share cyber security intelligence and threat feeds to the CBN Security Operation Centre or any such centre as may be required by the CBN.

5.3.2 Forensics

Participants shall implement digital forensics capabilities for open banking operations.

5.3.3 Communications Security

a. Participants shall implement network security controls to proactively detect, prevent and respond to network threats that can affect the confidentiality, integrity and availability of open banking information and assets;

b. Participants shall adequately and securely configure open banking gateways to minimize integration friction and enable seamless information flow; and

c. Participants shall implement Transport Layer Security (TLS) for network communication channels for open banking platforms with extended validation certificates.

5.3.4 Vulnerability Management and Penetration Testing

Participants shall:

a. Conduct periodic vulnerability scanning and penetration testing of system security to determine adequacy of system protection against cyber risks.

b. Remediate identified vulnerabilities in tandem to the severity of the open banking assets.

5.3.5 Operational Software Integrity

5.3.5.1 Secure change control

Participants shall ensure that:

a. Changes to open banking product and services are made in a secured, structured manner and controlled environment;

b. Change controls include impact analysis on business process, infrastructure, systems and applications, business continuity plans (BCPs) and service providers to ensure that all affected components have been identified;

c. All emergency changes are monitored, verified, and post-implementation reviews conducted involving all concerned parties. The review shall consider and initiate corrective actions based on root causes such as problems with business process, application system development and maintenance, development and test environments, documentation and manuals, and data integrity; and

d. Change status reports with performance metrics are implemented to enable management review and monitoring of both the detailed status of changes and the overall state such as age analysis of change requests, which shall form audit trail.

5.4 Configuration management

Participants shall:

a. Ensure a documented inventory of configuration items that relate to open banking operations which include applications, devices, endpoints, platforms, staff, personnel, data etc;

b. Document and regularly review all configuration changes on open banking infrastructure;

c. Ensure documentation of configuration item changes using standardised version control formats such as Semantic Versioning 2.0.0; and

d. Enforce continuous patching, including documenting and archiving dates to all technology and have individual accountability for patching specific software and equipment.

6.0 Business Continuity Management and Disaster Recovery

Participants shall:

a. Implement and regularly review Disaster Recovery (DR) and Business Continuity (BC) policies, procedures, and controls to ensure resilience of open banking operations.

b. Implement backup controls and regularly restore to reduce service unavailability.

c. Implement controls such as Distributed Denial of Service (DDoS) controls on open banking environment, to ensure resilience and 99.99 per cent availability.

d. Participants shall ensure that open banking data are retained for reference for a minimum of ten years.

7.0 Logging and Monitoring

Participants shall implement:

a. Controls that audit all activities and generate tamper-proof digital logs that can used as court evidence and non-disputable audit trail for effective problem resolution and forensics examination;

b. Monitoring controls to detect, prevent and respond to anomalous activities on open banking IT operations; and

c. Threat monitoring, alerting systems and intelligence to review and refine threats and implement mitigating actions regularly for continuous improvement.

8.0 Application Security

Participants shall:

a. Implement security controls into the Software Development Lifecyle (SDLC) for all open banking APIs;

b. Embed information security from planning, designing to implementation of all open banking software products;

c. Ensure strong IT systems controls (access and role management etc.) covering Software Development Lifecycle (SDLC), continuous integration, and continuous deployment (CI/CD) pipelines; and

d. Secure APIs and web application security risks in line with recommendations of the OWASP API Security project and OWASP Top Ten Web Application Security Risks respectively.

e. Ensure that practices considered inimical to the open banking ecosystem, are not carried out. Such practices include screen scraping, shotting, copying, snipping and others as may be determined by the Bank from time to time.

9.0 Data Privacy and Interoperability

Participants shall:

a. Access data and service category information according to the Regulatory Framework for Open Banking in Nigeria, provided customer's explicit consent have been obtained, and enable the customer to exercise their right to data portability;

b. Not use, access, or store any data for purposes other than the service explicitly requested by the end user; and

c. Safeguard their customers' data in line with NDPR and/or any CBN regulation on data privacy and protection and enforce the requirements with their third parties.

10.0 Encryption

Participants shall ensure message timestamps comply with ISO-8601 date formats or any other up-to-date standard/format. For example, 2020-07-10 15:00:00.000, represents the 10th of July 2020 at 3 p.m. (in local time as there is no time zone offset specified—more on that below)

Participants shall:

a. Ensure that Message Signing require TLS 1.2 Mutual Authentication RFC 8705 for non-repudiation, or any other up-to-date standard/format;

b. Ensure Message encryption is implemented through JSON Web Encryption (JWE) RFC 7516, or any other up-to-date standard/format;

c. Implement JSON Web Signature (JWS) RFC 7515 signed using an algorithm that supports asymmetric keys, or any other up-to-date standard/format; and

d. Implement asymmetric algorithms, (or any other up-to-date standard/format) RFC 7518 such as:

   i. TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
   ii. TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
   iii. TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
   iv. TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

e. Use a trust anchor that is defined by the CBN which is responsible for providing an issue, management and store of public keys and certificates; and

f. Retrieve public keys to verify messages from the trust anchor.

11.0 Physical Security Specifications

Participants shall:

a. Restrict physical access to critical areas in line with Open Banking Industry Data Security Standard physical security controls;

b. Restrict and monitor access to sensitive open banking premises by establishing perimeter restrictions, such as fences, walls, and security devices on interior and exterior doors; and

c. Log and monitor all entry points to open banking premises and register all visitors, including contractors and vendors, to the site.

APPENDIX IV – CUSTOMER EXPERIENCE STANDARDS

1.0 Introduction

This section defines the minimum customer experience requirements for open banking operation in Nigeria and addresses customer experience principles, journey and protection measures.

2.0 Customer Experience Principles

i. Control

Participants shall ensure that customers shall be provided with the right tools and clarity of information at the right time that will enable them to make informed decision. This includes but not limited to; knowing the account balance at the point of payment or knowing that they can view and cancel consents given when they feel it is appropriate to do so.

ii. Speed

Participants shall ensure that each interaction has appropriate speed, clarity and efficiency, without compromising security and control.

iii. Transparency

Participants shall:

a. Provide progressive levels of information in plain language that inform and support customer decisions.

b. Ensure clarity on information required from customers, the reason, purpose and what the consequences could be.

iv. Security

Participants shall provide explicit clarity and reassurance in relation to data definition, use, security and protection.

3.0 Customer Journey

Participants shall ensure the clarity of information that is presented and described in a manner that ensures that each API Standard Customer journey is easy to understand.

4.0 Customer Protection Measures

Participants shall ensure that the following measures are put in place to ensure customer protection when implementing open banking.

Customers shall be provided, at a minimum, information on procedures to exit, revoke consent and access rights at the time of onboarding and authorising data access.

4.1 Data Protection and Retention

Participants shall:

a. Establish clear data protection and retention policies with protocols for safeguarding information;

b. Ensure that data obtained for the purposes of open banking is retained for a minimum period of seven (7) years, except when legally bound;

c. Enable customer exercise right to revoke consent;

d. Ensure that the use access or storage of customer data for any purpose is as provided in the Regulatory Framework on Open Banking in Nigeria;

e. Ensure that third parties storing customer data shall be equipped with well-defined capabilities to manage data acquired through Open Banking APIs, including capabilities to handle token-based authentication, consent management and data privacy; and

f. Inform the customer on the process for handling redundant data and right to revoke consent, as part of the withdrawal process.

4.2 Customer Consent

a. Customers shall provide explicit consent for the use of their data;

b. Customers' consent shall be obtained in the same form the agreement was presented and a copy of the consent of the customer shall be made available to the customer and preserved by the participant;

c. The consent of the customer shall be re-validated annually and/or where the AC had not used the service for 180 days;

d. The participant shall ensure that the connection is configured to terminate upon expiration of the consent;

e. Appropriate customer authentication methods such as multi-factor authentication shall be established to reduce the chance of identity theft or fraud;

f. Customers shall always have control over their data and be able to access, manage or withdraw their consent at any point in time; and

g. Participants shall develop and agree on a consent management mechanism which includes a clear set of policies and procedures.

4.3 Disclosure and Transparency

Participants shall:

a. Disclose to customers the implications of data sharing before authorising and agree to the terms and conditions of consent; and

b. Notify the customer of security updates regularly in his/her preferred form and language.

4.4 Liability Management, Customer Complaint and Redress Management

4.4.1 Liability Management

Participants shall establish:

a. Procedures for handling customer complaints and resolving disputes; and

b. Appropriate liability models and redress mechanisms as approved by the Bank.

4.4.2 Customer Complaint

Participants shall:

a. Develop customer complaint resolution mechanisms with clearly defined roles and responsibilities and have sufficient channels available to customers for lodging complaints, including both physical and digital channels.

b. Provide:

i. Multiple dedicated channels to receive and handle customer complaints;

ii. Complaints channels that are effective, functional, efficient and easily accessible;

iii. Complaints channels that generate a unique identification number and acknowledge complaints within 24 hours of lodgment, including transcription of verbal complaints; and

iv. Emergency channels for reporting time-sensitive issues especially fraud-related complaints at all times.

4.4.3 Redress Mechanism/Dispute Resolution

Participants shall provide adequate redress mechanism and dispute resolution process as approved by the Bank.

The customer at onboarding shall be provided information on how to lodge complaints and available dispute resolution mechanisms.

a) Upon receipt of a complaint, the participant shall communicate to the customer within 24 hours, an acknowledgment containing:
   i. Unique identification or tracking number,
   ii. Contact details of the complaints desk,
   iii. Expected resolution timeline,
   iv. Escalation options; and
   v. An assurance that the complaint is being addressed.

b) Complaints shall be resolved within 48 hours of the receipt of the complaints.

i. Dispute Resolution between Participants

a. Participants shall detail in Service Level Agreements (SLA), comprehensive dispute resolution processes including timelines for resolution
b. Where dispute arise among participants, the dispute shall be resolved by the participants within the timelines agreed in their SLA
c. Where the SLA is breached without resolution, or a Participant is dissatisfied with the resolution, the aggrieved participant shall escalate the issue to the CBN for resolution
d. Participants shall cooperate with the CBN in resolving the dispute.

5.0 Dispute Resolution at the CBN

i. Customers shall escalate complaints to the Consumer Protection Department of CBN.

ii. Such complaints shall only be escalated:

a. If the complainant has exhausted the Participant's Internal Dispute Resolution (IDR) process.
b. If a participant fails to satisfactorily resolve the complaint within 14 days.

c. If it is not undergoing the process of resolution or already considered and resolved by a recognised ADR channel.
d. If it is not under litigation or already adjudicated upon by a court of law, except where the aspect before the court is distinct from the matter brought to the CBN or where the court is dealing with the criminal aspect of the matter.

APPENDIX V – OPERATIONAL READINESS CHECKLIST

#	Category	Requirement	Mandatory	Recommended
1.	**Master agreements**	1. Data Access Agreement 2. Service Level Agreement	AP	
2.	**Customer charters**	1. Customer bill of rights 2. Data privacy agreements which must be in compliance with the NDPR 3. Terms and conditions written in clear and accessible language	AP, AC	
3.	**Onboarding and partnerships**	1. Know your customer checklist (KYC) 2. Know your partner checklist (KYP) 3. Risk assessment report evaluation criteria	AP, AC	
4.	**Risk management**	1. Risk control matrix 2. Risk management metrics	AP	AC

#	Category	Requirement	Mandatory	Recommended
5.	**Key performance indicators**	1. System performance KPIs 2. Onboarding KPIs 3. Dispute resolution KPIs 4. Risk KPIs 5. KPI Warning Thresholds	AP	AC
6.	**Communication**	1. Design communication plan for all incident types. Include plan in service level agreements 2. Implement real-time interface for incident management with Audio, Video and Text capabilities. 3. Implement ticket management systems / processes 4. Onboard partners on TMS and communications platforms.	AP	
7.	**Monitoring**	1. Design KPI gathering and storage architecture 2. Implement performance and availability gathering mechanisms, plug into reporting module, publish over APIs if feasible. 3. Setup visual aids and triggers for alerts	AP, AC	

#	Category	Requirement	Mandatory	Recommended
8.	**Incident Management**	1. Document incident management plan with clear operational processes to meet SLAs, align with communication plan. 2. Keep an open register of incidents and categorize per type, log each occurrence. 3. Track and report incident and resolution occurrences 4. Escalate recurring incidents to problem management 5. Keep lessons learnt and knowledge base repositories	AP, AC	
9.	**Business Continuity Plan**	1. Document business continuity plans, detailing processes, responsibilities and redundancies provided. Ensure detailed steps are enumerated and design to meet SLAs. 2. Schedule review and failover activities for the year 3. Track results and problems	AP, AC	
10.	**Problem Management**	1. Inaugurate a problem register detailing issue type, date, symptoms,	AP	AC

#	Category	Requirement	Mandatory	Recommended
		stop-gap, resolution plan and dates		
11.	**Change Management**	1. Institute change register maintenance and change management process and owned by appointed Change Advisory Board members 2. Ensure change notification schedules are implemented as recommended and employ technology tools where possible.	AP	
12.	**Reporting**	1. Design reporting templates and systems, and plug-in to data sources. Note recommended report data 2. Ensure reports are segmented per participant 3. Automate reporting where possible.	AP	AC
13.	**Accounting & Financial Management**	1. Capture billing arrangements within business/service contracts. 2. Design and document accounting procedures to provide clarity between operations, accounting and	AP	AC

#	Category	Requirement	Mandatory	Recommended
		business management personnel. 3. Create process for updating this process with new products/services		
14.	**Settlement**	1. Adhere to guidelines regarding switching operations. 2. Ensure inter-participant settlement operations are clearly defined to amounts, timing, defaults, overdrafts etc.	AP, AC	
15.	**Dispute Resolution**	1. Implement systems to track & maintain required SLA 2. Implement consumer interfaces for raising and communicating updates on disputes 3. Design and operationalize inter-participant dispute management processes. 4. Train operational personnel for Open Banking related disputes and procedure handbook to guide action.	AP, AC	
16.	**Fraud and Liabilities**	1. Design, and operationalize fraud management processes 2. Establish legal and business framework for treating liabilities	AP, AC	

#	Category	Requirement	Mandatory	Recommended
		3. Implement controls to ensure compliance at all levels		
17.	a. Notes b. **Mandatory**: These are requirements that shall be implemented to meet regulatory conformance. The CBN shall request evidence of conformance. c. **Recommended**: These are requirements that the CBN strongly encourage for implementation for Operational Guidelines to achieve its objectives. The CBN *WILL NOT* request evidence of conformance d. **API Provider (AP):** This refers to a participant that uses API to avail data or service to another participant. An API Provider can be a licensed financial institution/service provider, a Fast-Moving Consumer Goods (FMCG) Company or other retailers, Payroll Service Bureau etc. e. **API Consumer (AC):** This refers to a participant that uses API released by the (API) providers to access data or service. An API Consumer can be licensed financial institution/service provider, an FMCG or other retailers, Payroll Service Bureau etc		