CENTRAL BANK OF NIGERIA

NIGERIAN PAYMENTS SYSTEM

RISK AND INFORMATION SECURITY MANAGEMENT FRAMEWORK

TABLE OF CONTENTS

1. INTRODUCTION

The journey to the Payments System Vision 2020 (PSV 2020) started in 2007 with the objective of making the Nigeria Payments System ***internationally recognised and nationally utilised***. The phased implementation of the vision and other developments in the financial space including the pursuit of the Financial System Stability Vision 2020(FSS 2020) has stimulated an exponential growth in financial activities and hence in the volume and value of payment flows both within and across national borders.

The rapid growth in the volume and value of financial transactions represents an important source of revenue for the providers of payment services particularly banks and other stakeholders. Other benefits include: fostering safety and efficiency of payment, clearing, settlement, and recording systems, promotion of financial system stability, speed of service and transactions, development of new lifestyle products, financial inclusion, etc. The growth has also significantly altered the risks associated with the payment and settlement of these transactions. As a result, payment and settlement systems are important potential sources of systemic risks.

Furthermore, payments system may increase, shift, concentrate, or otherwise transform risks in unanticipated ways. The failure of one or more of the participants in a payment system to settle their payments or other financial transactions as expected, in turn, could create credit or liquidity problems for participants and their customers, the system operator, other financial institutions, and the financial markets the payment system serves. Such a failure may ultimately undermine public confidence in the nation's financial system.

It is therefore necessary to effectively manage the risks associated with payments system, as such systems which inherently create interdependencies among financial institutions can create systemic risks. A disruption may originate from any of the interdependent entities, including the system operator, participants in a payment system, or other systems, and spread quickly and widely across markets if the risks that arise among these parties are not adequately measured, monitored, and managed. For example, interdependencies are usually based on a series of complex and time sensitive transactions and payment flows which, in combination with a payment system's design, can lead to significant demands for intraday credit or liquidity, on either a regular or an extraordinary basis.

The Central Bank of Nigeria (CBN) as a settlement institution plays an important role in the Payments System. It is the primary provider of intraday balances and credit to foster the smooth operation and timely completion of settlement processes. To that extent, the CBN may face the risk of loss if such intraday credit is not repaid as planned.

Furthermore, mitigating the risks associated with payments system is important for the effective management of monetary policy and banking supervision. For example, the orderly settlement of Open Market Operations (OMO) and the efficient movement of funds throughout the financial system via the financial markets and the payments system that support those markets are critical to the effective implementation of monetary policy. Similarly, supervisory objectives must take into account the risks that payment systems pose to the financial system by participating directly or indirectly in, or providing settlement, custody, or credit services.

In the interconnected environment, the safety and efficiency of these systems may affect the stability and soundness of financial institutions and consequently the financial stability of the country. As a result, safeguarding the integrity of the payments system in Nigeria has acquired additional significance and calls for the upgrading of associated risk management procedures through concerted efforts by market participants and the relevant authorities, notably the CBN.

In light of the above, the CBN approved the Nigerian Payments System Risk and Information Security Management Framework (this Framework) to guide the management of risks associated with the payments system in Nigeria.

2. OBJECTIVES OF THE FRAMEWORK

The objectives of this framework include to:

a. identify and address sources of systemic risks within the Nigerian Payments System landscape;

b. establish sound governance arrangements to oversee the risk management framework by ensuring that risks are identified, monitored and treated;

c. establish clear and appropriate rules and procedures to carry out the risk-management objectives;

d. employ the resources necessary to achieve the payments system's risk management objectives; and

e. integrate risk management into the decision making processes of the Scheme Boards and Working Groups under PSV 2020.

3. SCOPE

This Framework is designed to guide the operators and users of the payment systems across Nigeria. These systems may be organized, located, or operated within Nigeria (domestic payments), outside Nigeria (offshore payments), or both (cross-border payments) and may involve currencies other than the Naira (non-

Naira systems and multi-currency systems). The scope of the Framework also includes any payment system based or operated in Nigeria that engages in the settlement of non-Naira transactions operating within Nigeria and those that operate across the Nigerian borders (cross border payment systems); along with their infrastructure providers and the Payment Service Providers (PSPs) that make up these systems.

This Framework does not apply to arrangements for the physical movement of cash or systems for settling securities nor apply to market infrastructures such as trading exchanges, trade-execution facilities, or multilateral trade-compression systems. It is also not intended to apply to bilateral payment, clearing, or settlement relationships, where a payment system is not involved, between financial institutions and their customers, such as traditional correspondent banking and government securities clearing services.

4. RISK MANAGEMENT GOVERNANCE STRUCTURE

The Payments System Management Department of the CBN is responsible for setting, applying and coordinating risk standards across the Nigeria Payments space. It is supported by the Payments Initiative Coordinating Committee and the four (4) Scheme Boards.

5. ROLES AND RESPONSIBILITIES

5.1. CENTRAL BANK OF NIGERIA (CBN)

The overall responsibility for the management of risk across the National Payments System rests with the CBN. The CBN is expected to drive the overall National Payments System Strategy, provide cross-scheme resource and arbitrate in cross-scheme decisions.

Its risk governance responsibilities include to:

a. provide risk oversight of the payments system and ensure adequate resources are allocated to risk management activities;

b. approve the risk strategy for the payments system;

c. set risk parameters and tolerances within which payment system activities would be conducted;

d. determine and periodically review payments system key policies and processes; and

e. review payments system risk reports and direct remedial and / or mitigating actions as appropriate.

5.2. PAYMENT INITIATIVE COORDINATING COMMITTEE (PICC)

The membership of PICC is composed of all the Chairpersons of the Payment Scheme Boards, Payments Initiative Working Groups, Special Interest Working Groups and Independent Director(s) representing the end-user community. The PICC is Chaired by the Director, Payments System Management Department

The PICC provides advisory services to the Bank on Payments System. It also serves as a forum where issues relating to risk affecting the various initiatives are discussed.

5.3. PAYMENTS SCHEME BOARD (PSB)

The PSBs are responsible for monitoring full conformance to the Principles of Financial Market Infrastructure and other best practices. The PSBs shall recommend initiatives, strategies and policies to the CBN with a view to close any gaps related to full conformance to agreed best practice. This ensures the resiliency and efficiency of the Nigerian Payments System.

Also, the PSBs provide advise to the CBN for the establishment of an appropriate general Risk Management Framework for their respective scheme.

6. RISKS IN PAYMENTS SYSTEM

The basic risks in payments system include systemic risk, credit risk, liquidity risk, operational risk, legal risk, settlement risk and information security risk. In the context of this Framework, these risks are defined as below.

6.1. SYSTEMIC RISK

The danger that problems in a single Payments System participant could disrupt the normal functioning of the entire payment system space leading to potential collapse of the financial system and or damage to the national economy.

6.2. CREDIT RISK

The risk that a counterparty, whether a participant or other entity, is unable to meet its financial obligations when they fall due, or at any time before or after the due date.

Participants within a payment system are obligated to meet their commitments. When one party is unable to fulfil such obligation, this creates a credit risk that might spread through the system (via a contingent effect and/or contagion). As with most financial systems, participants often rely on the fulfilment of prior obligation to meet future or immediate obligation. Therefore having a well-articulated, regulated and managed credit risk process is essential to the well-being of any payment system.

The Nigerian Payments System has rules and processes including a collateral management framework to maintain the associated credit risk at a level that is acceptable.

6.3. LIQUIDITY RISK:

The risk that a party in a payment flow, whether a participant or other entity, is unable to meet its financial obligations when due, even though it may be able to do so in the future. A payment system may bear or generate liquidity risk in one or more currencies in its payment or settlement process based on its design or operations. In this context, liquidity risk may arise between or among the payment system operators, participants and other entities (such as settlement banks, nostro agents, or liquidity providers).

6.4. OPERATIONAL RISK

The risk that inadequacies in internal processes, human errors, management failures, information technology systems or disruptions from external events will result in the reduction, deterioration, or breakdown of services provided by the payment system.

6.5. COMPLIANCE, LEGAL AND REGULATORY RISK

The risk that arises from an unexpected or uncertain application of a law or regulation. These risks also arise between financial institutions as they clear, settle, and effect payments and other financial transactions and must be managed by institutions, both individually and collectively.

6.6. SETTLEMENT RISK

The general term used to designate the risk that settlement in a funds or securities transfer system will not take place as expected. This risk may comprise both credit and liquidity risks.

6.7. INFORMATION SECURITY RISK

The risk of loss resulting from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction of information assets and information systems.

Cyber security is a growing area of concern that deserves particular and continuous attention at the highest level.

7. GENERAL POLICY EXPECTATIONS

7.1. PRINCIPLES FOR FINANCIAL MARKET INFRASTRUCTURES

The Principles for Financial Market Infrastructures (PFMI) issued by the Committee on Payment and Settlement Systems (CPSS) and the Technical Committee of the International Organization of Securities Commissions (IOSCO)

establish minimum standards for addressing risk associated with Payments System that are systemically important.

The standards captured in the PFMI have been widely recognized, supported, and endorsed by the CBN. The implementation of the PFMI by the payments system will promote safety, efficiency and stability of the financial system. Accordingly, the CBN has incorporated into this Framework PSR policy principles 1 through 24 from the PFMI. In applying part I of this policy, the CBN and the Scheme Boards shall be guided by the key considerations and explanatory notes from the PFMI.

7.2. RISK MANAGEMENT FRAMEWORK

Scheme Boards shall maintain a general Risk Management Framework for their scheme and shall require all payment systems within the scheme to implement a risk-management framework appropriate for the risks the payment system poses to the scheme and the broader financial system.

At a minimum, the risk management framework shall include to:

a. establish sound governance arrangements to oversee the risk management framework;

b. set sound risk management objectives and establish processes for identifying the key risks associated with the payment scheme;

c. establish clear and appropriate rules and procedures to pursue the stated objectives;

d. employ the resources necessary to achieve the system's risk-management objectives and implement effectively its rules and procedures; and

e. build resilience and security adequate to ensure the confidentiality, integrity and availability of the system.

IDENTIFY RISKS AND SET RISK-MANAGEMENT OBJECTIVES

Appropriate risk identification and assessment is the foundation of a sound risk-management framework. Scheme Boards and Payment System Operators shall take adequate steps to clearly identify and assess all risks that may result from or arise in any part of the payment system including the system's settlement process as well as the parties posing and bearing each risk.

In particular, system operators should:

a. identify the risks posed to and borne by the system participants, and other key parties such as a system's settlement banks, custody banks, and third-party service providers;

b. analyse whether risks might be imposed on other external parties and the financial system more broadly;

c. analyse how risk is transformed or concentrated by the settlement process;

d. consider the possibility that attempts to limit one type of risk that could lead to an increase in another type of risk;

e. be aware of risks that might be unique to certain instruments, participants, or market practices;

f. where payment systems have inter-relationships with or dependencies on other Financial Market Infrastructures (FMIs), system operators should analyse whether and to what extent any cross-system risks exist and who bears them;

g. set risk management objectives that clearly allocate acceptable risks among the relevant parties and set out strategies to manage these risks;

h. establish the risk tolerance of the system, including the levels of risk exposure that are acceptable to the system operator, system participants, and other relevant parties; and

i. re-evaluate their risks in conjunction with any major changes in the settlement process or operations, the transactions settled by the system's rules or procedures, or the relevant legal and market environments.

Risk management objectives should be consistent with the objectives of this Framework, the system's business purposes, and the type of payment instruments and markets for which the system clears and settles. Risk-management objectives should also be communicated to and understood by both the system operator's staff and system participants. System operators shall review the risk management objectives regularly to ensure that:

i. they are appropriate for the risks posed by the system;

ii. they continue to be aligned with the system's purposes;

iii. they remain consistent with this Framework; and

iv. they are being effectively adhered to by the system operator and participants.

ESTABLISH SOUND GOVERNANCE ARRANGEMENTS TO OVERSEE THE RISK MANAGEMENT FRAMEWORK

Each payment system shall have sound governance arrangements to implement and oversee their risk management frameworks. The responsibility for sound

governance rests with a system operator's board of directors or similar body and with the system operator's senior management.

Such governance structures and processes shall:

i. be transparent;
ii. enable the establishment of clear risk management objectives;
iii. set and enforce clear lines of responsibility and accountability for achieving these objectives;
iv. ensure that there is appropriate oversight of the risk management process; and
v. enable the effective use of information reported by the system operator's management, internal auditors, and external auditors to monitor the performance of the risk management process.

Individuals responsible for governance shall be qualified for their positions, understand their responsibilities, and understand their system's risk management framework. Governance arrangements should also ensure that risk management information is shared in forms, and at times, that allow individuals responsible for governance to fulfil their duties effectively. Risk reports should be presented to the Board of Directors of payment system operators at least quarterly

ESTABLISH CLEAR AND APPROPRIATE RULES AND PROCEDURES TO CARRY OUT THE RISK MANAGEMENT OBJECTIVES.

Payment systems shall have rules and procedures that are appropriate and sufficient to carry out the system's risk-management objectives and that are consistent with its legal framework. Such rules and procedures shall specify the respective responsibilities of the system operator, system participants, and other relevant parties. Rules and procedures shall establish the key features of a system's settlement and risk-management design and specify clear and transparent crisis management procedures and settlement failure procedures, if applicable.

EMPLOY THE RESOURCES NECESSARY TO ACHIEVE THE SYSTEM'S RISK MANAGEMENT OBJECTIVES AND IMPLEMENT EFFECTIVELY ITS RULES AND PROCEDURES

System operators shall ensure that the appropriate resources and processes are in place to allow the system to achieve its risk management objectives and implement effectively its rules and procedures. In particular, the system operator's staff shall have the requisite skills, information, and tools to apply the system's rules and procedures to achieve the system's risk management

objectives. System operators shall also ensure that their facilities and contingency arrangements, including any information system resources, are sufficient to meet their risk management objectives.

BUILD RESILIENCE AND SECURITY ADEQUATE TO ENSURE THE CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF THE SYSTEM

The Scheme Boards should ensure that Operators build and implement adequate resilience into their infrastructure and operations to limit the potential for disruptions (operational failures) resulting from single points of failure. In addition, Operators shall ensure that critical data including customer information are encrypted to the standard specified in the extant CBN guidelines.

Furthermore, Operators shall implement appropriate back-up and disaster recovery programs to limit the impact of prolonged disruption including denial of service attacks. Such a program shall include daily comprehensive data back-up; adequately resourced alternate site(s) for IT and other operational activities as well as detailed procedures for responding to material disruptions. The disaster recovery programme shall be tested at least once a year to ensure its continued effectiveness and completeness.

8. OTHER CONSIDERATIONS FOR A RISK MANAGEMENT FRAMEWORK

Payment systems differ widely in form, function, scale, and scope of activities. These characteristics result in differing combinations and levels of risks. Thus, the exact features of a system's risk management framework should be tailored to the risks of that system. Where appropriate, the following should be covered:

8.1. LEGAL AND REGULATORY

i. Each Scheme Board shall recommend a set of rules for the registration of scheme participants. Aspiring members shall be required to comply with the requirements set by the appropriate scheme board.
ii. Participants operating in the Nigerian payment space shall be licensed and regulated by the CBN.
iii. Participants operating in the Nigerian payment space shall ensure they comply with all appropriate CBN Guidelines.
iv. Participants and Payment Service Providers (PSPs) shall maintain a Compliance Matrix or other appropriate cross referencing tool to ensure and provide proof of compliance with key regulatory requirements.
v. All participants should have a legal and regulatory risk management policy.
vi. Participants shall establish an appropriate compliance function within their organisation that provides regular reports to their Board of Directors.

8.2. BUSINESS CONTINUITY

i. Participants shall build adequate redundancies into their operational infrastructures to reduce the risks associated with single points of failure to an acceptable level.

ii. Participants shall have a robust Operational Risk Management Policy that includes a Business Continuity Strategy and show evidence of compliance with ISO 22301 standards and subsequent standards.

iii. Participants shall ensure that appropriate business continuity plans covering all critical services are in place and routinely tested. This should include services in the area of networking and good succession plan for critical personnel.

iv. Scheme Boards and participants shall ensure that all PSPs and other key suppliers have appropriate business continuity plans, covering all critical services, which are routinely tested and available for audit.

v. Scheme Boards shall encourage improved collaboration among participants e.g. the use of shared services.

vi. Systemically Important Payment Systems (as defined by the appropriate scheme boards) shall maintain a 'Living Will' to allow for an orderly wind-down procedure should the need arise.

8.3. KNOW YOUR CUSTOMER / CLIENT (KYC)

i. Scheme participants shall conduct appropriate continuous KYC on all Merchant customers/clients before on-boarding and throughout the life of the relationship.

   a. As a minimum, the KYC check shall include checks against the appropriate sanction lists including the BVN Watch list.

   b. KYC shall include adequate understanding and documentation of the Merchant customer's main business lines (Know Your Customer's Business (KYCB) to ensure effective transaction monitoring.

   c. A Merchant customer/client with any of its directors on the BVN Watch-list database shall be subject to enhanced monitoring.

ii. Each Scheme Board shall recommend appropriate enhanced monitoring schemes for watch-listed customers/clients Merchant. This shall include setting appropriate transaction limits in terms of volume and value for watch-listed customers/clients Merchant.

iii. A customer/client/ Merchant shall only be removed from the BVN Watch-list, in line with the BVN Watch-List Framework.

iv. An Acquirer shall not on-board a Merchant where the Acquirer is aware or reasonably suspects that a Merchant is involved in illegal or illicit business

v. Operators shall comply with CBN guidelines on the set up of Anti-Fraud desk and fraud management system.

8.4. SCHEME OPERATIONS

Each Scheme Board shall:

i. recommend clear and detailed procedures to govern the day to day operations of the scheme;
ii. recommend minimum capital requirement for participants. Each scheme shall define clear rules regarding actions to be taken in the event that a participant is unable to meet the prescribed minimum capital requirement and make appropriate recommendations to the CBN;
iii. recommend a process for reviewing new products within the scheme space. Such reviews shall include a detailed risk assessment that identifies the key risks associated with the product and controls built into the product design;
iv. conduct an annual risk review of existing products in the scheme space;
v. agree a unified risk based collateral requirement for participation in the payment space;
vi. release reports that make the following information public:
    a. standards to be adopted;
    b. data on volume and value of transactions;
    c. emerging risks and trends;
    d. projections for the industry;
    e. penalties;
vii. take adequate steps to retain public confidence in the operations of the scheme, which shall include but not limited to:
    a. ensuring the availability and reliability of the platform;
    b. security of transactions;
    c. transparency of rules and related charges;
    d. effective communication and strong relationship with key stakeholders; and
    e. develop strategies for crisis management including assigning specific roles and responsibilities.

8.5. SETTLEMENT RULES AND DEFAULT MANAGEMENT

Each Scheme Board shall:-

i. recommend clear rules with regards to the irrevocability of transactions, finality of payment and settlement;

ii. recommend and communicate settlement procedures to all participants; furthermore, each participant shall ensure full compliance with settlement rules as it applies to the scheme and take adequate steps to mitigate its exposure to liquidity and credit risks that may impact on the scheme settlement;

iii. recommend well defined procedure for the management of default. Such procedure shall be in line with existing PFMI; where appropriate, the scheme board shall define who bears any losses that may result from a default, what actions are taken against the defaulting party and any other steps required to ensure the continuity of the scheme;

iv. develop appropriate credit risk management practices to limit the risk associated with counter party and settlement failure; and

v. agree a unified risk based collateral requirement for participation in the payment space.

8.6. INFORMATION SECURITY

i. System operators, Participants and PSPs shall:
   a. establish and implement Information Security policies that are in line with ISO 27001 standards or subsequent standards; and
   b. ensure the confidentiality, integrity and availability of all information, systems and networks that are critical to the success of the scheme. The owners of such information, systems and networks shall be responsible for deploying the required resources.

ii. Scheme Boards shall recommend where appropriate a minimum information security protocol such as PCIDSS for Card Payment System, to ensure the security of transactions and information transmission across the scheme.

iii. Participants and PSPs shall conduct annual Information Security assessment including penetration and vulnerability tests to ensure it is aware and is taking adequate steps to address current and on-going issues.

8.7. OTHER REQUIREMENTS

i. Each Scheme Board shall recommend minimum fraud prevention requirements for participants in its scheme.

ii. Participants shall designate an officer who will be responsible for managing risks relating to payment system.

iii. Participants shall ensure that adequate risk management practices and processes are implemented across activities that may impact on the Payments System.

9. SCHEME SPECIFIC REQUIREMENTS

9.1. CARD PAYMENT SCHEME RISK REQUIREMENTS

i. Cards shall be produced in accordance with CBN "Guidelines on Card Issuance and Usage in Nigeria" and the Payment Card Industry (PCI) card production security standards; where applicable.

ii. The handling of cards through the Card Life Cycle shall be in accordance with the minimum standards as defined by PCI Data Security Standards (DSS) and CBN "Guidelines on Card Issuance and Usage in Nigeria" or as may be reviewed from time to time.

iii. Acquirers shall ensure that Merchants with turnover greater than N10Million/month (with the Acquirer), or as maybe prescribed by the CBN from time to time, screen their employees against the BVN Watch-list at least once a year.

iv. Once an Acquirer identifies a Merchant or an employee(s) of a Merchant as the source or a participant in fraudulent transactions and related activities; the Acquirer shall propose the Merchant or employee for Watch-listing.

v. Acquirers shall screen directors and signatories of each Merchant against the BVN watch-list before on-boarding by Acquirers

vi. Card Payments Scheme Board shall agree and recommend the industry limit on card transactions.

vii. All Card Not Present (CNP) transactions on Nigerian issued Cards from a Nigerian acquired Merchant shall use a minimum of 2 Factor authentication; with the exception of card on file transactions where the initial transaction must have used 2 factor authentication.

viii. Participants shall make appropriate investments in IT infrastructure to aid automation and straight through processing, data loss prevention and fraud management.

ix. Participants shall conduct annual capacity assessment to ensure that adequate infrastructure, skilled personnel, and processes exist to support expected growth in transaction volume and value for the next 12 months.

9.2. RTGS PAYMENT SCHEME RISK REQUIREMENTS

i. The Scheme Board shall recommend risk parameters and tolerances within which RTGS related payment activities will be conducted.

ii. Participants shall maintain sufficient funds to effect settlement of payment obligations.

iii. For payments related to clearing sessions, the Board shall ensure that rules and appropriate arrangements exist to allow for immediate settlement of all clearing related obligations under a wide range of potential stress scenarios.

iv. The Scheme Board shall take steps to ensure that settlement of payments between multiple banks or participants are conducted in a safe, reliable and repeatable manner to eliminate the need for banks to settle transactions bilaterally.

v. Participants shall have appropriate business continuity plan in place. Compliance with ISO 22301 shall be a minimum requirement.

vi. The scheme Board in collaboration with CBN shall ensure that annual stress tests, quarterly vulnerability assessment and annual penetration tests of the RTGS system is conducted.

vii. The Scheme Board in collaboration with CBN shall ensure that access to RTGS platform is subject to a role based privileges and multi-factor authentication to provide secure access and non-repudiation of transactions.

viii. Participants shall ensure sufficient transaction controls and monitoring processes are implemented to prevent errors and omissions to support early detection of fraud.

ix. In the event that a participant is unable to settle its obligation, the scheme shall lock the participant's account from all forms of debit transaction (debit freeze) except from clearing. Participation in clearing is subject to clearing rules and regulations.

9.3. ACH, CHEQUE AND INSTANT PAYMENT SCHEME RISK REQUIREMENTS

i. The Scheme Board in collaboration with CBN shall ensure that each participant provides annual attestation on self-assessment and continuous compliance with regulatory requirements.

ii. The Scheme Board in collaboration with CBN shall ensure that Settlement Banks conduct appropriate due diligence on associated non-settlement financial institutions. In addition, settlement banks shall ensure KYC and AML /CFT monitoring on their transactions.

iii. The Scheme Board shall encourage participants to actively participate in industry wide fraud management and information sharing initiatives.

9.4. MOBILE PAYMENT SCHEME RISK REQUIREMENTS

i. The Scheme Board shall encourage operators to conduct continuous customer education to minimize the occurrence of identity theft and other frauds.

ii. The Scheme Board in collaboration with CBN shall ensure a minimum of two-factor authentication shall be applied to all mobile money transactions to reduce the risk of identity theft.
iii. The Scheme Board in collaboration with CBN shall ensure licensed agents use visible branding/logos at all agent locations.
iv. Operators have an automated transaction alerting system with updated balance and it is built into the platform to ensure users are notified on completed or truncated transactions.
v. The Scheme Board in collaboration with CBN shall ensure Operators fee structure is made public and visible at agent location.
vi. The Scheme Board in collaboration with CBN shall ensure MMOs have a backup pathway for completing transactions when the primary path is unavailable. Back up paths shall be tested on a regular basis.
vii. The Scheme Board in collaboration with CBN shall ensure data transmitted is adequately secured.
viii. Participants shall ensure a maximum time allotted for a session. When sessions timeout, transactions shall be rolled back.
ix. When sessions are terminated, an immediate alert shall be sent indicating termination. During session time, the mobile device shall not be allowed to send same transaction i.e. same amount to the same beneficiary.
x. Operators shall implement adequate security measures to prevent denial of service on its platform.
xi. Operators shall conduct due diligence before on boarding and engaging agents.
xii. Operators shall adhere to the guidelines on Agency Banking.
xiii. Operators shall ensure that all alerts containing Unique Account Identifier are masked.

10. DISPUTE RESOLUTION

Each scheme shall establish its dispute resolution mechanism to serve as an additional dispute resolution mechanism that will help participants resolve disputes in a timely and cost effective manner.

Disputes that arise between or across schemes may be referred through the Director, Payments System Management Department of the CBN to the PICC for resolution

11. RISK MONITORING

Risk is dynamic and as such should be closely and regularly monitored. The respective Scheme Boards and Initiative Working Groups shall conduct on-going monitoring of risks inherent in the payment system, and communicate significant risk events to the Information Security and Risk Management Special Interest Working Group (ISRM SIWG) for aggregation and recommendation of remedial actions.

The following methodologies shall be employed for risk monitoring activities;

I. Questionnaires,

II. Risk reports from various scheme boards and

III. Independent control assessment.

12. RISK REPORTING

Risk reports shall be provided to the CBN and PICC as appropriate. The reports shall contain key risk and remedial actions.

The following reports shall be periodically prepared and circulated:

S/N	REPORT NAME	DESCRIPTION	RESPONSIBILITY	DISTRIBUTION	FREQUENCY
1.	Independent Risk Assessment of the Payment System Initiatives	Provide independent assessment of the various payment system initiatives	ISRM SIWG	CBN PICC	Quarterly
2.	Scheme Risk Reports	Highlights major risk events faced by each scheme board	SCHEME BOARDS	ISRM SIWG	Quarterly
3.	New Initiative Risk Report	Provides key changes and risks to new initiatives	ISRM SIWG	CBN PICC	On need basis
4.	Emerging Risk Report	Highlight emerging risks due to changes in the payment landscape	ISRM SIWG	CBN PICC	Quarterly

13. CBN OVERSIGHT

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

14. DEFINITION OF TERMS

The terms below shall have the following meaning for the purpose of this Framework.

1. *ACH Cheque & Instant Payment Scheme Board* means the body that **e**nsures that NIBSS, as a systemically important payment system provider, is robust and has adequate business continuity arrangements.
2. *Acquirer* means bank or any other legal person concluding contracts with Merchants concerning acceptance of payment by means of an electronic payment token.
3. *Arbitration* means resolution of disputes outside the courts.
4. *Automated Clearing House* means an electronic clearing system in which payment orders are exchanged among financial institutions, primarily via magnetic media or telecommunications networks, and handled by a data processing centre.
5. *Availability means* the ability of services and information to be accessed by users when requested.
6. B*ank Verification Number (BVN)* means a biometric identification system implemented by the Central Bank of Nigeria to curb or reduce illegal banking transactions in Nigeria.
7. Card Life cycle is the period from the production, storage, issuance, maintenance to the disposal of a payment card.
8. *Card Not Present Transaction* means a payment card transaction made where the cardholder does not or cannot physically present the card for a Merchant's visual examination at the time that an order is given and payment effected, such as for mail-order transactions by mail or fax, or over the telephone or Internet.
9. *Card Payment Scheme Board* refers to the Board that formulates rules, guidelines and frameworks governing the Card Payment Infrastructure with regard to the business, operational and risk management activities of the various stakeholders operating in Nigeria.
10. Collateral means an asset that is delivered by the collateral provider to secure an obligation to the collateral taker. Collateral arrangements may take different legal forms; collateral may be obtained using the method of title transfer or pledge.
11. Critical Data is information that is vital to the operation of a business

12. Customer/Client: refers to an individual/entity in account relationship with the regulated institution

13. Information Security and Risk Management Special Interest Working Group (ISRM SIWG) refers to the SIWG that is responsible for effectively managing the risks associated with Nigerian Payments System.

14. Living Will means a detailed plan stipulating in advance how a systematically important payment system should be liquidated in the event of a collapse to prevent a panic and disorderly disposal of its assets. This is to ensure that the failure of a SIPS does not result in the failure of National Payment System or the whole economy. The contents of living will shall be as stipulated by the Central Bank of Nigeria from time to time.

15. Mobile Payment Scheme Board refers to the Board that formulates rules, guidelines and frameworks governing the Mobile Payment Infrastructure with regard to the business, operational and risk management activities of the various stakeholders operating in Nigeria.

16. Participant means a party that participates in the Nigerian payment system and which are bound by all the rules governing the payment system.

17. Payment means the payer's transfer of a monetary claim on a party acceptable to the payee. Typically, claims take the form of banknotes or deposit balances held at a financial institution or at a central bank.

18. Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes.

19. Payment Initiative Coordinating Committee (PICC) refers to the body responsible for driving and overseeing the various payments system initiatives.

20. Payment Scheme Board (PSB) or Scheme Board refers to the body that oversees the activities of the various scheme boards. The board will ensure that there is transparency and efficiency in the payment system.

21. Payment Service Provider (PSPs) refers to CBN licensed companies that employ the infrastructure of the scheme operator to provide services to end users.

22. Payment System Operator, System Operator, or Operator is an entity licensed by the CBN to engage in the operation and/or delivery of payment services within the National Payments System.

23. Payments System is a set of instruments, procedures, and rules for the transfer of funds between or among participants; the system includes the participants and the entity

operating the arrangement. Payments system are typically based on an agreement between or among participants and the operator of the arrangement, and the transfer of funds is effected using an agreed-upon operational infrastructure.

24. Payments System Infrastructure refers to various hardware, software, secure telecommunications network and operating environments that are used to manage and operate payments system. This infrastructure supports the clearing and/or settlement of a payment or funds transfer request after it has been initiated.

25. PCI DSS stands for Payment Card Industry Data Security Standard. It was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. (See www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf)

26. Real-Time Gross Settlement (RTGS) is a payment system in which processing and settlement of high value funds occur on real time (that is without deferral) and gross (i.e. transaction by transaction) among participants. The core feature is that payment instructions are settled only on funded accounts at the Central Bank of Nigeria and settlements are final and irrevocable.

27. RTGS Payment Scheme Board refers to the body responsible for ensuring that there is adequate measurement and management of liquidity, credit and operational risk management in the payment system

28. Systemically Important Payment System (SIPS) are major real time clearing, settlement and other payment systems that share the characteristic that a failure of one or more of these systems could endanger the operation of the National payment system or the whole economy. Each Scheme Board shall with the approval of the CBN determine from time to time the list of SIPS within their scheme

29. Systemic Risk is the failure of one or more participants to settle their payments obligation leading to credit or liquidity problems for other participants.