CENTRAL BANK OF NIGERIA
Central Business District
P.M.B. 0187,
Garki, Abuja.
+234 - 0946238445

BANKING AND PAYMENTS SYSTEM DEPARTMENT

BPS/PSV/SIG/CIR/01/001 **May 7th, 2018**

To: All Deposit Money Banks, Other financial Institutions, and Payment Service Providers, the General Public.

EXPOSURE DRAFT OF THE "NIGERIAN PAYMENTS SYSTEM RISK AND INFORMATION SECURITY MANAGEMENT FRAMEWORK"

The Central Bank of Nigeria(CBN), in furtherance of its mandate for the development of safe and secured electronic payments system in Nigeria, hereby issue the exposure draft of the Nigerian Payments System Risk and Information Security Management Framework for your review and comments (if any).

Kindly forward your comments, in hard copy to the Director, Banking & Payments System Department and the soft copy to scokojere@cbn.gov.ng and psv2020@cbn.gov.ng, on or before May 31st, 2018.

Thank you for your usual cooperation.

7/5/2018

'Dipo Fatokun
Director, Banking & Payments System Department

CENTRAL BANK OF NIGERIA

NIGERIAN PAYMENTS SYSTEM

RISK AND INFORMATION SECURITY MANAGEMENT FRAMEWORK

Document Ownership & Creation Record

	Designation	Name	Signature	Date
Policy Owner(s):				
Reviewed by:				
Document is owned and verified by:				
Authorized by:				
Approved by:				

REVISION	DESCRIPTION	DATE

METADATA	
Title	
Subject	
Policy Number	
Version	
Issuing Department	
Policy Status	
Approving Authority	
Date of Approval	
Date Last Amended	
Next Review Date	
Effective Date	
Date Created	
Category	
Description	
Size	
Key words	

TABLE OF CONTENTS

1. INTRODUCTION 5

2. OBJECTIVES OF THE FRAMEWORK 6

3. SCOPE 7

4. RISK MANAGEMENT GOVERNANCE STRUCTURE 7

5. ROLES AND RESPONSIBILITIES 8

5.1. CENTRAL BANK OF NIGERIA (CBN) 8

5.2. PAYMENT INITIATIVE COORDINATING COMMITTEE (PICC) 8

5.3. PAYMENTS SCHEME BOARD (PSB) 8

6. RISKS IN PAYMENTS SYSTEM 9

6.1. CREDIT RISK 9

6.2. LIQUIDITY RISK: 9

6.3. OPERATIONAL RISK 9

6.4. LEGAL AND REGULATORY RISK 9

6.5. SETTLEMENT RISK 10

6.6. INFORMATION SECURITY RISK 10

7. GENERAL POLICY EXPECTATIONS 10

7.1. PRINCIPLES FOR FINANCIAL MARKET INFRASTRUCTURES 10

7.2. RISK MANAGEMENT FRAMEWORK 10

7.2.1. IDENTIFY RISKS CLEARLY AND SET SOUND RISK-MANAGEMENT OBJECTIVES 11

7.2.1. ESTABLISH SOUND GOVERNANCE ARRANGEMENTS TO OVERSEE THE RISK MANAGEMENT FRAMEWORK 12

7.2.2. ESTABLISH CLEAR AND APPROPRIATE RULES AND PROCEDURES TO CARRY OUT THE RISK MANAGEMENT OBJECTIVES. 12

7.2.3. EMPLOY THE RESOURCES NECESSARY TO ACHIEVE THE SYSTEM'S RISK MANAGEMENT OBJECTIVES AND IMPLEMENT EFFECTIVELY ITS RULES AND PROCEDURES 13

7.2.4. BUILD RESILIENCE AND SECURITY ADEQUATE TO ENSURE THE CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF THE SYSTEM 13

8. OTHER CONSIDERATIONS FOR A RISK MANAGEMENT FRAMEWORK 13

8.1. LEGAL AND REGULATORY 13

8.2. BUSINESS CONTINUITY 14

8.3. KNOW YOUR CUSTOMER / CLIENTS (KYC) 14

8.4. SCHEME OPERATIONS 15

8.5. SETTLEMENT RULES AND DEFAULT MANAGEMENT 16

8.6. INFORMATION SECURITY 16

8.7. OTHER REQUIREMENTS 16

9. SCHEME SPECIFIC REQUIREMENTS 17

9.1. CARD PAYMENT SCHEME BOARD'S RISK REQUIREMENTS 17

9.2. THE RTGS PAYMENT SCHEME BOARD'S RISK REQUIREMENTS 18

9.3. THE ACH, CHEQUE AND INSTANT PAYMENT SCHEME BOARD'S RISK REQUIREMENTS 18

9.4. MOBILE PAYMENT SCHEME BOARD'S RISK REQUIREMENTS 19

10. MONITORING 20

11. REPORTING 20

APPENDIX 1 21

1. INTRODUCTION

The journey to the Payment 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: foster 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. This has also significantly altered the risks associated with the payment and settlement of these transactions. As a result, payment and settlement systems are now more 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 owing to its disruptive impact on the financial markets.

Given the above, it is especially important to effectively manage the risks associated with payments system, as such systems which inherently create interdependencies among financial institutions can create systemic risks. In many cases, interdependencies are a normal part of a payment system's structure or operations. While this facilitates the safety and efficiency of such system's payment, clearing, settlement or recording processes and interdependencies; it is also an important transmission channel of systemic risk. Disruptions can originate from any of the interdependent entities, including the system operator, participants in the payment system, and other systems, and can 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 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 Central Bank 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 payments system pose to the financial system that participate directly or indirectly in, or provide settlement, custody, or credit services to, such systems.

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 Central Bank of Nigeria.

In light of the above, the Central Bank of Nigeria developed 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 payment system's risk management objectives.

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 payments 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 policy 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 payments system); 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 Nigerian Payments System Risk Governance Structure is closely aligned to the organisational structure of the Nigeria Payment System as captured in the PSV 2020 Strategy which is depicted in Figure 1 below.

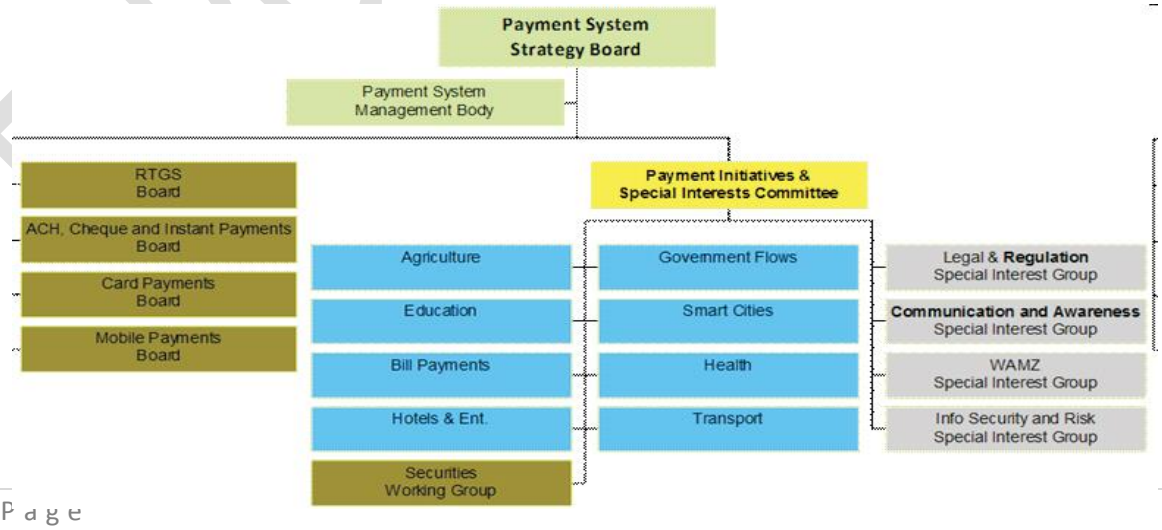

FIGURE 1 - RISK GOVERNANCE STRUCTURE

In line with the Bank's responsibility to ensure a credible, safe and reliable payment system in Nigeria, the Central Bank of Nigeria has set up a Payment System Strategy Board supported by four (4) Scheme Boards who are responsible for setting, applying and coordinating risk standards across the Nigeria Payments space.

5. ROLES AND RESPONSIBILITIES

5.1. CENTRAL BANK OF NIGERIA (CBN)

The overall responsibility for the national payment 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 payment system.

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

d. Determine and periodically reviews payment system key policies and processes.

e. Review payment system risk reports and direct remedial and / or mitigating actions as appropriate.

5.2. PAYMENT INITIATIVE COORDINATING COMMITTEE (PICC)

The PICC drives the various initiatives and oversee the Working Groups focused on specific initiatives. The Chairpersons of the various working groups are members of this committee.

Its risk governance responsibilities would be to serve as a forum where issues relating to risk affecting the various initiatives are discussed.

5.3. PAYMENTS SCHEME BOARD (PSB)

The role of the PSBs is to formulate rules, guidelines and frameworks governing the business, operation and risk management activities of the payment infrastructure and the other stakeholders that participate in their scheme. While nurturing volume growth in the segment, each Scheme Board shall give adequate attention to developing an appropriate level of overall governance of the segment and tracking conformance of stakeholders to the PFMI (Principles of Financial Markets Infrastructure).

6. RISKS IN PAYMENTS SYSTEM

The basic risks in payments system include credit risk, liquidity risk, operational risk, information security risk and legal risk. In the context of this framework, these risks are defined as follows:

6.1. CREDIT RISK

The risk that a counterparty, whether a participant or other entity, is unable to meet fully 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 (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.

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

6.2. LIQUIDITY RISK:

The risk that a party in a payment, whether a participant or other entity, will be unable to meet fully its financial obligations when due, although 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).

6.3. 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.

6.4. LEGAL AND REGULATORY RISK

The risk that arises from the 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.

6.5. 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 risk.

6.6. 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.

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 Technical Committee of the International Organization of Securities Commissions (IOSCO) establishes minimum standards for addressing risk associated with PAYMENTS SYSTEM that are systemically important.

The standards captured in the PFMI has been widely recognized, supported, and endorsed by the CBN. The Bank believes that the implementation of the PFMI by the payments system within the scope of this section will help 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, as set forth in the appendix 1. 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 PAYMENTS SYSTEM 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 the following:

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 & 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.

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

7.2.1. IDENTIFY RISKS CLEARLY AND SET SOUND RISK-MANAGEMENT OBJECTIVES

Appropriate risk identification and assessment is the foundation of a sound risk-management framework. Scheme Boards and Payment System Operators should 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 payments system have inter-relationships with or dependencies on other 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.

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

Risk-management objectives should be consistent with the objectives of this policy, 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 should 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 policy,
iv. They are being effectively adhered to by the system operator and participants.

7.2.1. ESTABLISH SOUND GOVERNANCE ARRANGEMENTS TO OVERSEE THE RISK MANAGEMENT FRAMEWORK

Each payment system should 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.

Governance structures and processes should be transparent; enable the establishment of clear risk management objectives; set and enforce clear lines of responsibility and accountability for achieving these objectives; ensure that there is appropriate oversight of the risk management process; and 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 should 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.

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

Systems should 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 should specify the respective responsibilities of the system operator, system participants, and other relevant parties. Rules and procedures should 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.

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

System operators should 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 should have the appropriate skills, information, and tools to apply the system's rules & procedures and achieve the system's risk management objectives. System operators should also ensure that their facilities and contingency arrangements, including any information system resources, are sufficient to meet their risk-management objectives.

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

The Scheme Boards shall ensure that Operators 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 current 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 must include daily comprehensive data back-up; fully resourced alternate site(s) for IT and other operational activities as well detailed procedure for responding to material disruptions. To ensure the completeness and continued effectiveness of the disaster recovery program, the program should be tested at least once year.

8. OTHER CONSIDERATIONS FOR A RISK MANAGEMENT FRAMEWORK

Payments system 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 Bank.
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 shall have a Legal and regulatory risk management policy.
vi. Participants shall establish a compliance function within their organisation headed by a senior officer that reports to the board.

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 & subsequent standards and its successors.
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 that are routinely tested and available for audit.
v. Scheme Boards shall encourage improved collaboration among participants e.g. the use of shared services.
vi. Each participant shall maintain a 'Living Will' to allow for an orderly wind-down procedure should the need arise.

8.3. KNOW YOUR CUSTOMER / CLIENTS (KYC)

i. Scheme participants shall conduct appropriate continuous KYC (including BVN validation) on all merchants 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's main business lines (Know Your Customer's Business (KYCB)) to ensure effective transaction monitoring.

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

ii. Each Scheme Board shall set appropriate enhanced monitoring scheme for watch-listed merchants. This shall include setting appropriate transaction limits in terms of volume and value for watch-listed merchants. If a bank decides to remove the limit placed, the bank must indemnify the system against this risk.

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

8.4. SCHEME OPERATIONS

Each Scheme Board shall:-

i. Set clear and detailed procedures to govern the day to day operations of the scheme.

ii. Establish minimum capital requirement for participants. Each scheme shall define and document 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 recommendation to the CBN.

iii. Establish a process for approving new products within the scheme space. Such reviews shall include a detailed risk assessment that identifies the key risks associated with the product and mitigates 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 and fines

vii. Take adequate steps to retain public confidence in the operations of the scheme. These steps 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
   e. Develop strategies for crisis management including assigning specific roles and responsibilities.

8.5. SETTLEMENT RULES AND DEFAULT MANAGEMENT

Each Scheme Board shall:-

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

ii. Establish 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. Establish well defined procedure for the management of default. Such procedure shall be in line with existing BIS 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.

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 its successors.

   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 define 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 ongoing issues.

8.7. OTHER REQUIREMENTS

i. Each scheme board shall set 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 BOARD'S RISK REQUIREMENTS

i. Card must be produced in accordance to 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 must be in accordance with 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. The CBN shall regularly monitor and sanction erring organizations and provide appropriate information on compliance issues and sanctions to scheme board.

iv. Acquirers shall ensure that merchants with turnover greater than N10Million/month screen their employees against BVN Watch-list at least once a year.

v. 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.

vi. Acquirers shall screen directors and signatories of each merchant against the BVN watch-list before on-boarding by acquirers

vii. Card Scheme Board shall agree and set the Industry limit on card transactions.

viii. All Card Not Present (CNP) transactions on Nigerian issued Cards from a Nigerian acquired merchant MUST use a minimum of 2 Factor authentication. Except for card on file transactions where the initial transaction must have used 2 factor authentication.

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

x. Participants shall comply with CBN guideline on set up of Anti-Fraud desk and fraud management system.

xi. 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. THE RTGS PAYMENT SCHEME BOARD'S RISK REQUIREMENTS

i. The scheme board shall set 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 guide to this.

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 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 omission to support early detection of fraud.

ix. Participants shall comply with CBN guideline on set up of Anti-Fraud desk and fraud management system.

x. 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. THE ACH, CHEQUE AND INSTANT PAYMENT SCHEME BOARD'S RISK REQUIREMENTS

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

ii. The Scheme Board 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 scheme participants to actively participate in industry wide fraud management and information sharing initiatives.

iv. Participants shall comply with CBN guideline on set up of Anti-Fraud desk and fraud management system.

9.4. MOBILE PAYMENT SCHEME BOARD'S RISK REQUIREMENTS

The Scheme board shall:

i. Encourage operators to conduct continuous customer education to minimize the occurrence of identity theft and other frauds.

ii. Ensure a minimum of two-factor authentication shall be applied to all mobile money transactions to reduce the risk of identity theft.

iii. Ensure licensed agents use visible branding/logos at all agent locations.

iv. Operators have an automated transaction alerting system with updated balance and it's built into the platform to ensure users are notified on completed or truncated transactions.

v. Ensure Operators fee structure is made public and visible at agent location.

vi. 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. 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, Mobile device will 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 comply with CBN guideline on set up of Anti-Fraud desk and fraud management system.

xiv. Operators shall ensure that all alerts containing Unique Account Identifier are masked

xv. Operators shall ensure compliance with subsisting AML /CFT guidelines.

10. MONITORING

Risk is dynamic and as such should be closely and regularly monitored. On-going monitoring of risks inherent in the payment system initiatives shall be conducted. Each scheme board shall 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.

11. REPORTING

Risk reports shall be provided to the PICC and other bodies 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	PICC	Quarterly
2.	Scheme Risk Reports	Highlights major risk events faced by each scheme board	SCHEME BOARDS	ISRM SIWG	Quarterly
S/N	**REPORT NAME**	**DESCRIPTION**	**RESPONSIBILITY**	**DISTRIBUTION**	**FREQ'NCY**
3.	New Initiative Risk Report	Provides key changes and risks to new initiatives	ISRM SIWG	PICC	On need basis
4.	Emerging Risk Report	Highlight emerging risks due to changes in the payment landscape	ISRM SIWG	PICC	Quarterly

APPENDIX 1

DEFINITION OF TERMS

S. No.	TERM	DEFINITION
1	PAYMENTS SYSTEM	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.
2	RETAIL PAYMENT SYSTEM	A funds transfer system that typically handles a large volume of relatively low-value payments in such forms as cheques, electronic transfers, direct debits, card payment transactions and any other payment token.
3	LARGE-VALUE PAYMENT SYSTEM (LVPS)	A funds transfer system that typically handles large-value and high-priority payments. Many LVPSs are operated by central banks, using an RTGS or equivalent mechanism.
4	DEFERRED NET SETTLEMENT (DNS)	A net settlement mechanism which settles on a net basis at the end of a predefined settlement cycle.
5	REAL-TIME GROSS SETTLEMENT (RTGS)	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.
6	PAYMENTS SYSTEM	Various hardware, software, secure telecommunications

	INFRASTRUCTURE	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.
7	INTERBANK PAYMENTS SYSTEM	Enable payments to be made between people using their accounts with Payment Service Providers (PSP) (e.g. their bank accounts).
8	ELECTRONIC COMMERCE	Also known as e-commerce or eCommerce, or e-business consists of the buying and selling of products or services over electronic systems such as the Internet and other computer networks.
9	PAYMENT SYSTEM OPERATORS	Payments system are managed by payment system operators and underpin the delivery of payment services.
10	Bank Verification Number (BVN)	A biometric identification system implemented by the Central Bank of Nigeria to curb or reduce illegal banking transactions in Nigeria.
11	PAYMENT SERVICE PROVIDERS (PSPs)	Offer payment services to individuals, businesses and other organisations including government - which is the largest user of payments system by volume of transactions. Types of PSPs include credit institutions (banks, building societies and credit unions), electronic money and payments institutions.
12	PAYMENT SYSTEM STRATEGY BOARD (PSSB)	Drive the overall National Payments System Strategy; provide cross-scheme resource and arbitrate in cross-scheme decisions
13	PAYMENT SCHEME BOARDS (PSB)	Oversee the activities of the various scheme boards. The board will ensure that there is transparency and efficiency in the payment system.

14	PAYMENT INITIATIVE COORDINATING COMMITTEE (PICC)	Drive the various initiatives and oversee the Working Groups focused on specific initiatives.
15	CARD PAYMENT BOARD	Formulate 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.
16	RTGS PAYMENT SCHEME BOARD	Ensure that there is adequate measurement and management of liquidity, credit and operational risk management
17	ACH CHEQUE AND INSTANT PAYMENT SCHEME BOARD	Ensue that NIBSS as a systemically important payment system provider is robust and have adequate business continuity arrangements.
18	MOBILE PAYMENT SCHEME BOARD	Formulate 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.
19	PAYMENT MESSAGE/ INSTRUCTION	An order or message to transfer funds (in the form of a monetary claim on a party) to the order of the beneficiary. The order may relate either to a credit transfer or to a debit transfer. See also credit transfer, debit transfer system, payment.
20	ACQUIRER	A bank or any other legal person concluding contracts with merchants concerning acceptance of payment by means of an electronic payment token.
21	AUTOMATED CLEARING HOUSE	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.
22	AUTOMATED TELLER MACHINE	An electromechanical device that permits authorised users, typically using machine-readable plastic cards, to withdraw cash from their accounts and/or access other services, such as balance enquiries, transfer of funds or acceptance of deposits. ATMs may be operated either online with real-time access to an authorisation database

		or offline.
23	AVAILABILITY	The ability of services and information to be accessed by users when requested.
24	BILATERAL NET SETTLEMENT SYSTEM	A settlement system in which participants' bilateral net settlement positions are settled between every bilateral combination of participants. See also net credit (or debit) position.
25	CASH CARD	Card for use only in ATMs or cash dispensers (other cards often have a cash function that permits the holder to withdraw cash).
26	CASH CLEARING	A method for clearing futures contracts in which positions are periodically marked to market and resulting obligations are satisfied by cash payments, known as variation margin.
27	PAYMENT INSTRUMENT	Any instrument enabling the holder/user to transfer funds.
28	PAYMENT	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.
29	PAYMENT LAG	The time lag between the initiation of the payment order and its final settlement.
30	PAYMENT NETTING	Settling payments due on the same date and in the same currency on a net basis.
31	PAYMENT ORDER	An order or message requesting the transfer of funds (in the form of a monetary claim on a party) to the order of the payee. The order may relate either to a credit transfer or to a debit transfer. Also called payment instruction.
32	PAYMENT VERSUS PAYMENT	A mechanism in a foreign exchange settlement system which ensures that a final transfer of one currency occurs if and only if a final transfer of the other currency or currencies takes place.
33	POINT OF SALE	This term refers to the use of payment cards at a retail location (point of sale). The payment information is captured either by paper vouchers or by electronic

		terminals, which in some cases are designed also to transmit the information. Where this is so, the arrangement may be referred to as "electronic funds transfer at the point of sale"
34	SECURITIES SETTLEMENT SYSTEM	The full set of institutional arrangements for confirmation, clearance and settlement of securities trades and safekeeping of securities.
35	SECURITY INTEREST	A form of interest in property which provides that the property may be sold on default in order to satisfy the obligation covered by the security interest.
36	COLLATERAL POOL	Assets owned by members of a payment system that are collectively available to the system as collateral to enable it to obtain funds in circumstances specified in its rules.
37	COLLATERAL	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
38	CRYPTOGRAPHY	The application of mathematical theory to develop techniques and algorithms that can be applied to data to ensure goals such as confidentiality, data integrity and/or authentication.
39	BATCH (BULK PAYMENTS)	A group of orders (payment orders and/or securities transfer orders) to be processed together
40	CHEQUE	A written order from one party (the drawer) to another (the drawee; normally a credit institution) requiring the drawee to pay a specified sum on demand to the drawer or a third party specified by the drawer.
41	CREDIT LIMIT (CREDIT CAP):	A limit on the credit exposure which a payment system participant incurs either vis-à-vis another participant (a "bilateral credit limit") or vis-à-vis all other participants (a "multilateral credit limit") as a result of receiving payments which have not yet been settled.
42	CARD NOT PRESENT TRANSACTION	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.
43	CROSS-BORDER PAYMENT	A payment where the financial institutions of the payer and the payee are located in different countries.
44	CROSS-BORDER SETTLEMENT	Settlement that takes place in a country (or currency area) in which one or both parties to the transaction are not located.
45	INFORMATION SECURITY AND RISK MANAGEMENT SPECIAL INTEREST WORKING GROUP (ISRM SIWG)	Responsible for effectively managing the risks associated with Nigerian Payments System.
46	INTEROPERABILITY	The set of arrangements/procedures that allows participants in different systems to conduct and settle payments or securities transactions across systems while continuing to operate only in their own respective systems.